At all Jurgen
Neukirch

Algebraic Number Theory

Translated from the German
by Norbert Schappacher

With 16 figures

Springer

Jurgen Neukircht

Translator:

Norbert Schappacher

U:F.R. de Mathematique et d'Informatique
UniversiteLouis Pasteur
7, rue Rene Descartes
F"67084 Strasbourg, France
e-mail: sch�ppa@math.u-strasbg.fr

The original German edition was published in 199-2 under the title
Algebraische Zahlentheorie
ISBN 3-540-54273--6 Springer-Ve.lag Berlin Heidelb:erg New York

Library of Congress Cataloging-in-Publication Data

Neukirch, Jurgen, 1937-. [Algehraische 1'.ahlentheorie. En:glis-h] Algebraic number theory/ Jurgen Neukirch; translated from the German by Norbert Schappacher.
p. cm. - (Grundlehren der mathematischen Wissensch-aften; 322
fndudes bibliographical references and index.
lS.BN 3-540-65399-6 (he.: alk. paper)
!.-Algebraic number theory. I. Title II. Series.
QA247.N;517.13 1999 512'.74-dc21 99-21030 £JP

Mathematics Subject Classification (1991): 11-XX, 14-XX

ISSN 0072-7830
ISBN 3-540J65399-6 Springer-Verlag Berlin Heidelberg New York

Cover design: MetaDesign plus GmbH, Berlin
Photo<:omposed from fue translator's L'"TEX files after editing and reformatting by Raymond Seroul, Strasbourg
SPIN: 10425040 41/3143-5 4 3 21 o Printed on acid-free paper

Foreword

-It is a very sad moment for me to write this "Geleitwort" lo the English translation-ofJtirgen Neukirch's book on Algebraic Number Theory. It would have been so much better, if he could -have done this himself.

But it is also very difficult for me to write this "Geteitwort": The book contains NeU:kirch's Preface to the German edition.There he himself speaks about his intentions, the content.of the book arrd his personal view of the subject. What else can be said?

It becomes dear from his Preface that Number Theory was Neukirch's favorite subjectin mathematics. He was enthusiastic about it, and he was also able to implant this enthusiasm into the minds of his students.

He attracted them, they gathered around him in Regensburg. He told them thatthe subject and its beauty justified the-highest effort and so they were always eager and motivated to discuss and tolearn the newest developments in number theory and arithmetic algebraic geometry. I remember very well the many occasions when this equipe showed up in the meetings of the '!Oberwolfach Arbeitsgemeinschaft" and demonstrated their strength (mathematically and on the soccer field).

During the meetings of the "Oberwolfach Arbeitsgemeinschaft" people come together to learn a subject which is not necessarily their own speciality. Always at the end, when the most difficult talks had to be delivered, the Regensburg crew took over. In the meantime many members of this team teach at German universities.

We.find this charismaofJi.irgen Neukirch,in the book.It will be a motivating source for young students to study Algebraic Number Theory, and I am sure �hat it will attract many of them.

At Neukirch's funeral his daughter-Christiane recited the poem which she often heard ,from her father: *Herr van Ribbeck au/ Ribbeck im Havellandby* Theodor'Fontane. It tells the story of a nobleman who always generously gives away the pears from his garden to the children. When he dies he ·asks fora pear to be put in his grave, so that later the children can pick the pears from the growing tree.

This is -I believe - a good way ofthinking of Neukirch's book: There are seeds in it for a tree to grow from which the "children" can pick fruits in the time :to come.

G.Harder

Translator's Note

When I first accepted Jurgen Neukiroh's request to translate *hisAlgebraische Zahlentheorie*, back in 1991, no-.one imagined thathewould-not live.to seethe English edition. He did see the raw version of the translation -(I gave him the last chapters in the Fall of 1996), and he still had time to go carefully through the first four chapters of it.

The bulk of the text consists of .detailed technical mathematical prose and was thus straightforward to translate, even though the author's desire to integrate involved arguments and displayed formulae into comprehensive sentences could not simply be copied into English. However, JtirgenNeukirch had peppered his book with more meditative paragraphs which make rather serious use of the German language. When I started to work on the translation, he warned me that in every one of these passages, he was not seeking poetic beauty,-but orily the precisely adequate expression of anidea.It isfor the reader to judge whether 1 managed to render his ideas faithfully.

There i,sone neologism that I propose in this translation, with Jiirgen Neukirch's blessing: I call *replete* divisor, ideal, etc., what is :usually called Arakelov divisor, etc. (aterminology that Neukirchhadavoided in the German edition). Time will deliver its verdict.

lammuch indebted to Frazer Jarvis for goingthroughmy entire manuscript, thus saving the English language from various infractions. But needless to say, I alone am responsible for all deficiencies that remain.

After Ji.irgen Neukirch's untimely death early in 1997, -**it** was Ms Eva-Maria Strobel whotook it upon herself to finish as best she could what Ji.irgen Netikirch had to leave undone. She had already applied her infinite care and patience to the original :German book, and she had assistedJtirgen Neukirch in proofreading the first fom chapters of the translation. Without'her knowledge, responsibility, and energy, this bodk would not be what it ;is.1n particular, a fair number of small corrections and modifications of the German original that had been accumulated thanks to.attentive readers, were taken .into account for this English edition. Kay Wingberg graciously helped to chedka-few of them. We sincerely hope that the book published here would have made its author happy.

Heartythanks goto RaymondSeroul, Strasbourg, for applying-his wonderful expertise of TEX to the final preparation of the camera-ready manuscript.

Thanks go to the Springer staff for seeing this project through until it was finally completed. Among them I wantto thank especially Joachim Heinze for interfering rarely, but effectively, over the years, with the rea:Iization of this translation.

Strasbourg, March 1999 *Norbert Schappacher*

Preface to the German Edition

Number Theory, among the mathematical disciplines, occupies an idealized position, similar to the one that mathematics holds among the sciences. Under no obligation to serve needs that do not originate within its-elf, it is essentially autonomous in setting its goals, and thus manages to protect its undisturbed harmony. The possibility of formulating its basic problems simply, the peculiar clarity of its statements, the arcane touch in its laws, be they discovered or undiscovered, merely divined; last but not least, the charm of its particularly satisfactory ways ·of reasoning - all these features have at all times attracted to number theory a community of dedicated followers.

But different·number theorists may dedicate themselves differently·to·their science. Some will push thetheoretical development only as far as is necessary for the concrete result they desire. Others will strive for a more universal, conceptual clarity, never tiring of searching for the deep-lying reasons behind the apparent variety ,of arithmetic phenomena. Both attitudes are justified, and they grow particularly effective through the mutual inspirational influence they exert on one another. Several beautifui textbooks illustrate the success of the first attitude, which is oriented towards specific problems. Among them, let us pick out in particular *Number Theory* by *S.I.* BoREV!CZ and *J.R.* SAFAREVIC [J 4]: a book which is extremely rich in content, yet easy to read, and which we especially recommend to the reader.

The present book was conceived with a different objective in mind. It does provide the student with an essentially self-contained introduction to the theory of algebraic number fields, presupposing only basic algebra (it starts with the equation $2 = 1 + 1$). But unlike the textbooks alluded to above, it progressively emphasizes theoretical aspects that rely on modern concepts. Still, in doing so, a special effort is made to limit the amount of abstraction used, in order that the reader should not lose sight of the concrete goals of number theory proper. The desire to present number theory as much as possible from a unified theoretical point of view seems imperative today, as a result of the r.evolutionary development that number theory has undergone in the last decades in conjunction with 'arithmetic algebraic geometry'. The immense success that this new geometric ,perspective has brought about - for instance, in the context of the Weil conjectures, the Mordell conjecture, of problems related to the conjectures of Birch and Swinnerton-Dyer - is largely based on the unconditional and universal application of the conceptual approach.

It i-s true that those impressive :resuhs can hardly be touched upon in this book because they require higher dimensional theories, whereas the book deliberately confines itself to the theory of algebraic number fields, Le., to the 1-dimensional case. But I thought it necessary to present the theory in a way which takes these developments into account, taking them as the distant focus, borrowing emphases and arguments from the higher point of view, thus integrating the theory of algebraic number fields 'into the higher dimensional theory - or at least avoiding any obstruction to such an integration. This is why I preferred, whenever it was feasible, the functorial point of view and the more far-reaching argument to the devertrick, and made a particular effort to place geometric interpretation tothefore, in the spirit of the theory of algebraic curves.

Let me forego the usual habit of describing the content of each individual chapter in this foreword; simply turning pages will yield the same information in a more entertaining manner. *l* would however like to emphasize a few basic principles that have guided me while writing the book. The first chapter lays down the foundations of the global theory and the second of the local theory of algebraic number fields. These foundations are finaUy summed up in the first three sections of chapter Ill, the aimof which isto present the perfect analogy of the classical notions and results with thetheory of algebraic curves and the idea of the Riemann-Roch theorem. The presentation is dominated by ".Arakelov's point of view", which has acquired much importance in recent years. It is probably the first time that this approach, with all its intricate normalizations, has received an ex-tensive treatment in a textbook. But I finally decided not to employ the term "Arakelov divisor" although it is now widely used. This would have entailed attaching the name of *Arakelov* to many other concepts, introducing too heavy a terminology for this elementary material. My decision seemed all the more justified as *ARAKELOV* himself introduced his divisors only for arithmetic surfaces. The corresponding idea in the number field case goes back to *HASSE,* and is clearly highlighted for instance in *S. LANc's* textbook [94].

It was not without hesitation that l decided to include *Class Field Theory* in chapters IV-VI. Since my book [107] on this subject had been published-no.t long before, another treatment of this theory posed obvious questions. Butin the end, after long consideration, there was simply no other choice. A sourcebook on algebraic number fields withoutthe crowning conclusion of class field theory with its important consequences for the theory of L-series would have appeared like a torso, suffering from an unacceptable lack of completeness. This also gave me the opportunity to modify and emend my earlier treatment, to enrich that somewhat dry presentation with quite a few examples, to refer ahead with some remarks, and to add beneficial exercises.

A lotof work went intothe last chapteron zetafunctions and £..:series. These functions :haYe gained central importance in recent decades, but textbooks do not pay sufficient attention to1hem. -Idid not, however, include *TATE'S* approach to Hecke L-series, which is based on harmonic analysis, althoughjt would have suited the more conceptual orientation of the book perfectly well. In fact, the darity of *TATE's* own presentation could hardly be improved upon, and it has also been sufficiently repeated in other places. Instead I have preferred to turn back to.*HECKE's* approach, which is not easy to understand in the original version, but for all its various advantages cried-out for a modern treatment. This having been done, there was the obvious opportunity of givinga thorough-presentation of *ARTIN's* L-series with their functional equation - which surprisingly has not been undertaken in any exi-sting textbook.

It was a difficult decision to exclude *lwasawa Theory*, a relatively recent theory totally germane to algebraic number fields, the subject of this book.Since it mirrors important geometric properties .of algebraic curves, 'it would have been a par.ticularly beautiful vindication of our oft-repeated thesis .that number theory ,is geometry. Ldo believe, however, thatin this case the geometric aspect becomes truly convincing only if on-euses *etale cohomology* - which can neither-be assumed nor reasonably .developed here. Perhaps the dissatisfaction with this exclusion will be strong enough to bring about a sequel tothe present volume, devoted to the cohomology of algebraic number fields.

,from the very starNhe book was.not just intended as·a modern sourcebook on algebraic number theory, but also as a convenient textbook for a course. This intention was increasingly jeopardized by the unexpected growth of the material which had to be covered in view of the intrinsic necessities of the theory. Yet I think that the bookhas.not lost that character. In fact, it has passed a first test inthis respect. With a bit of careful planning, the basic content of the first three .chapters can easily be presented in one academic year (if :possible including infinite Galois theory). The following term wi11 then provide scarce, yet sufficient room for the class field theory ofchapters IV-VI.

Sections 11-14 of chapter I may most]y be dropped from an introductory .course. Although the results of section 12 on *orders* are irrelevant for the sequel, lconsiderits insertion in the bookparticularly important. For onething, orders -constitute the rings of multipliers.., which play an eminent role in many diophantine problems. But most importantly, they represent the analogues of *singular* algebraic curves.. As cohomology theory becomes .increasingly important for algebraic number fields, and since this is even more true of *algebraic K-theory*, which cannot be constructed without singular schemes, ·the time has come to give orders- an adequate treatment.

In chapter II, the special treatment of henselian fields in s.ection 6 may be restricted to complete valued fields, and thus joined with section 4. ff pressed for time,.section 10 on higher ramification may be omitted completely.

The firsnhree sections of chapter III should be presented inthe lectures since they highlight a new approach to classical results of algebraic number theory. The subsequent theory concerning the theorem of Grothendieck-Riemann-Roch is a nice subject for a student seminar rather than for an -introductory course.

Final!:)', in presenting class field theory, it saV'es considerable time if the students are already familiar with profi-nite groups and infinite Galois theory. Sections 4_:_7 ofchapter V, on formal groups, Lubin-Tate theory and the theory of higher ramification maybe omitted. Cutting out even more, chapter V, 3, on the Hilbert symbol, and VI, 7 and 8, still leaves a fully-fledged theory, which is however unsatisfactory because it remains in the abstract realm, and is never linked to classical problems.

A word on the exercises at the end of the sections. Some .of them are not so much exercises, but additionalremarks which did not fit well into the main text. The reader is encouraged to prove his versati'lity in looking up the literature. I should also point out that I have not actually done all the exercises myself, so that there might be occasional mistakes in the way they are posed. If such a case arises, it is for the reader to find the correct formulation. May the reader's reaction to such a possible slip of the author be mitigated by Goethe's distich:

"Irttum verlaHt uns nie, doch ziehet ein hoher Bediirfnis
lmmerden streberrden Geist leise zur Wahrheit hinan." *

During the writing of this book I have been helped in many ways. I thank the Springer Verlag for considering my wishes with generosity. My students /. *KAusz,B. KocK, P. KoiczE, TH. MosER, M.*SnEsshavecritically examined larger or smaller parts, which led to numerous improvements and made it possible to avoid mistakes and ambiguities. To my friends *W.-D.GEYER, G. TAMME,* and *K. W1NGBERG* I owe much valuable advice :from which the book has profited, and it was C. *DENINGER* and *U.JANNSEN* who suggested that I give a new treatment ofHecke's theory of theta series and L-series. I owe a great debt of gratitude to Mrs. *EvA-MAR!A. STROBEL.* She drew the .pictures and helped me with the proofreading and the formatting of the text, never tiring of going into the minutest detail. Let me heartily thank ail those who assisted me, and also those who are not named here. Tremendous thanks are due to Mrs. *MARTINA HERTL* who didthetypesetting of the manuscript in TpC Thatthe book can appear·is

* Error is ever with us. Yet some angelic need
Gently coaxes our striving mind upwards, towards truth.
(Translation suggested by *BARRY MAZUR.)*

essentially due to her competence, to the unfailing and kind willingness with which she worked through the long handwritten manuscript, and through the many modifications, additions, and corrections, always prepared to give her best.

Regensburg, February 1992 *Jiirgen Neukirch*

Table of Contents

Chapter I

Algebraic Integers

§ 1. The Gaussian Integers

The equations

$$2 = 1 + 1,\ 5 = 1 + 4,\ 13 = 4 + 9,\ 17 = 1 + 16,\ 29 = 4 + 25,\ 37 = 1 + 36$$

show the first prime numbers that can be represented as a sum of two squares. Except for 2, they are all $=$ 1 mod 4, and it is true in general that any odd prime number of the form $p = a^2 + b^2$ satisfies $p = 1 \bmod 4$, because perfect squares are $= 0$ or $= 1$ mod 4. This is obvious. What is not obvious is the remarkable fact that the converse also holds:

(1.1) Theorem. *For aJJprime numbers* $p \# 2$, one *has:*

$$p = a^2+b^2 \quad "(a, b \in Z) \quad \{=::> \quad p = 1 \bmod 4.$$

The natural explanation of this arithmetic law concerning the ring Z of rational integers is found in the larger domain of the **gaussian integers**

$$Z[i]=\{a+bi \,|\, a,b \in Z\},\quad i = ?-$$

In this ring, the equation $p = x^2 + y^2$ turns into the product decomposition

$$p = (x + iy)(x - iy),$$

so that the problem is now when and how a prime number $p \in Z$ factors in Z[i]. The answer to this question is based on the following result about unique factorization in $Z[i]$.

(1.2) Proposition. *The ring* Z[i] *is euclidean,* therefore *in particular factorial.*

Proof: We show that Z[i] is euclidean with respect to the funciion Z[i] -+ f:J U {O}, $a \mapsto |a|^2$. So, for $a, /3 \in Z[i]$, $J3 =J 0$, one has to verify the existence of gaussian integers y, p such that

$$a = yf3 + p \quad \text{and} \quad |P|^2 < |/3|^2.$$

It clearly suffices to find $y \in Z[i]$ such that $/ j - y / < 1$. Now, the gaussian integers form a **lattice** in the complex plane (C (the points with integer coordinates with respect to the basis 1, i). The complex number j lies in some mesh of the lattice and its distance from the nearest lattice point is not .greater than half the length of the diagonal of the mesh, i,e. 1-v12. Therefore there exists an element *y* E Z[iJ with J.� - *y* j ::: ½.J2 < 1. □

Based on this result about the ring Z[i], theorem (LI) now follows like this: it is sufficient to show that a prime number p = 1 mod 4 of Z does not remain a prime element in the ring Z{i). Indeed, if this is proved, then there exists a decomposition

$$p=a\bullet f3$$

into two non-units *a*, *f3* of *Z[i].* The **norm** of $z = x + iy$ is defined by

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y2,$$

i.e., by N(z) = lzl2. It is multiplicative, so that one has

$$p^2 = N(a) \cdot N(/3).$$

Since *a* and *f3* are not units, it follows that *N(a)*, N({J) ¥ 1 (see exercise 1), and therefore $p = N(a) = a^2 + b^2$, where we put *a* = *a* + *bi.*

Finally, in order to prove that a rational prime of the form $p = 1 + 4n$ .cannot be a prime element in *Z[i],* we note thatthe congruence

$$-1 = x^2 \bmod p$$

admits a solution, namely $x = (2n)!$. Indeed, since $-1 = (p - 1)! \bmod p$ by Wilson's theorem, one has

$$-1 = (p - 1)! =:[1 \cdot 2 \cdots (2n)]l[(p - 1)(p - 2) \cdots (p - 2n)]$$

$$= [(2n)!][(-L\}^2n(2n)!] = [(2n)!]^2 \bmod p.$$

Thus we have $p \mid x^2 + 1 = (x + i)(x - i)$. But since $\frac{x}{p} \pm \frac{i}{p} \notin$ Z[i), p does not divide any of the factors $x+i$, $x-i$, and is therefore not a prime element in the factorial ring Z[*i].*

The example of the equation $p = x^2+y2$ shows that even quite elementary questions about rational integers may lead to the consideration of higher domains of integers. But it was not so much for this equation that we .have introduced the ring Z[*i],* but rather in order to preface the general theory of algebraic integers with a .concrete example. For the same reason we will now look at this ring a bit more closely.

When developing the theory of divisibility for a ring, two basic problems are most prominent: on the one hand, to detemiine the **units** of the ring in question, on the other, its **prime elements.** The answer to the first question in the present case is particularly easy. A number $a = a + bi$ E Z[i] is a unit if .and only if its norm is 1:

$$N(a) := (a + ib)(a - ib) = a^2 + b^2 = \mathrm{I}$$

(exercise 1), i.e., if either $a^2 = 1$, $b^2 = 0$, or $a^2 = 0$, $b^2 = 1$. We thus obtain the

(l.3) Proposition. *The group of units of the ring* Z[i] *consists oftb-e fourth roots of unity,*

$$Z[i]^* = \{1, -1, i, -i\}.$$

In order to answer the question for primes, i.e., irreducible elements of the ring Z[*i],* we first recall that two elements *a,* f3- in a ring are called **associated,** symbolically *a* ~ *f3,* if they differ only by a unit factor, and that every element associated to an irreducible element JT is also irreducible. Using theorem (1.1) we obtain the following precise list of all prime numbers of *Z[i].*

(1.4) Theor-em. *The prime* elements *n* of *Z[i], up to associated* elements, *are given as faJJows.*

(1) rr $= 1 + i$,

(2) rr $= a + bi$ with $a^2 + b^2 = p$, $p \equiv 1 \bmod 4$, $a > |b| > 0$,

(3) rr $= p$, $p \equiv 3 \bmod 4$.

Here, *p* denotes *aprimenumberof* Z.

Proof: Numbers as in (l) or (2) are prime because a decomposition rr $= a \cdot$ f3 in Z[*i]* implies an equation

$$p = N(n) = N(a) \cdot N(f3),$$

with some prime number *p.* Hence either $N(a) = 1$ or $N(/3) =$ L, so that either *a* OT *f3* is a unit.

Numbers rr $= p$, where $p \equiv 3 \bmod 4$, are prime in Z[i], because a decomposition $p = a \cdot$ f3 into non-units *a,* f3 would imply that $p^2 = N(a) \cdot N(,B)$, so .that $p = N\{a) = N(a + bi) = a^2 + b^2$, which according to (LI) would yield $p \equiv$ I mod 4.

This being said, we have to check that an arbitrary prime element *Tl* of *Z[i]* is associated to one of those listed. First of all, the decomposition

$$\mathrm{N}(rr) = n \cdot if = Pl \cdots Pr,$$

with rational primes *Pi,* shows that *-ir IP* for some *.p* = *Pi.* This gives *N(n)IN(p)* = p^2, so that either N(rr) = *p* or N(rr) = p^2. In the case *N* (rr) = *p* we get rr = *a+ bi* with $a^2 + b^2 = p$, so rr is of type (2) or, if *p* = 2, it is associated to 1 + *i.* On the other hand, if *N* (rr) = p^2, then rr is associated to *p* since *p* / *Tl* is an ·integer with norm one and thus a unit. Moreover, *p* = 3 mod 4 has to hold in this case because otherwise we would have *p* = 2 or *p* = I mod 4 and because of (1. I) *p* = $a^2 + b^2$ = (a + *bi}(a - bi)* could not be prime. This completes the

�� D

The proposition also settles completely the question of how prime numbers *p* E *Z* decompose in Z[i]. The prime 2 = (1 +i)(l *-i)* is associated to the square of the prime element 1+*i.* Indeed, the identity 1- *i* = -i{I+i) shows that 2 ~ $(1 + i)^2$. The prime numbers *p* ·= 1 mod 4 split into two conjugate .prime factors

$$p = (a + b\text{-}i)(a - bi),$$

and the .prime numbers *p* = 3 mod 4 remain prime in Z[*i].*

The gaussian :integers play the ,same role in the field

$$\mathrm{Q}(i) = \{a + bi \mid a,b \in \mathrm{ilJ}\}$$

as the rational integers do in the field Q. So they should be viewed as the "integers" in <Q(i). This notion of=integrality is relative to the coordinates of the basis 1, i. However, we also have the following characterization of the gaussian integers, which is independent of a choice of basis.

(1.5) Proposition. Z[i] *consists precisely* of those *elements* of *the* extension *field* Q(i) ofQ *which satisfya manic polynomial equation*

$$x^2 + ax + b = 0$$

with coeflicients *a, b* E Z.

Proof: An element *a* = *c* +*id* E Q(i) is a zer-oof the polynomial

$$x^2 + ax + b \in (\mathrm{Q}:[x] \quad \text{with} \quad a = -2c,\ h = c^2 + d^2.$$

If *c* and *d* are rational integers, then so are *a* and *b.* Conversely, if *a* and *b* are integers, then so are 2c and *2d.* From (2c)2 + (2d)2 = *4b* = 0 mod 4 it follows that (2c)2 = $(2d)^2$ = 0 mod 4, since square-s are always = 0 or = l. Hence *c* and *d* are integers. □

The last proposition leads us to the general notion of an algebraic integer as being an element satisfying a monic polynomial equation with rational integer coefficients. For the domain of the gaussian integers we have obtained in this section a complete answer to the question of the units, the question of prime elements, and to the question of unique factorization.

These questions indicate already the fundamental problems in the general theory of algebraic integers. But the answers we found in the special case $\mathbb{Z}[i]$ are not typical. Novel features will present themselves instead.

Exercise 1. $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.

Exercise 2. Show that, in the ring $\mathbb{Z}[i]$, the relation $\alpha\beta = \varepsilon\gamma^n$, for α, β relatively prime numbers and ε a unit, implies $\alpha = \varepsilon'\xi^n$ and $\beta = \varepsilon''\eta^n$, with $\varepsilon', \varepsilon''$ units.

Exercise 3. Show that the integer solutions of the equation

$$x^2 + y^2 = z^2$$

such that $x, y, z > 0$ and $(x, y, z) = 1$ ("pythagorean triples") are all given, up to possible permutation of x and y, by the formula:

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $(u, v) = 1$, u, v not both odd.

Hint: Use exercise 2 to show that necessarily $x + iy = \varepsilon\alpha^2$ with a unit ε and with $\alpha = u + iv \in \mathbb{Z}[i]$.

Exercise 4. Show that the ring $\mathbb{Z}[i]$ cannot be ordered.

Exercise 5. Show that the only units of the ring $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$, for any rational integer $d > 1$, are ± 1.

Exercise 6. Show that the ring $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, for any squarefree rational integer $d > 1$, has infinitely many units.

Exercise 7. Show that the ring $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is euclidean. Show furthermore that its units are given by $\pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$, and determine its prime elements.

§ 2. Integrality

An **algebraic number field** is a finite field extension K of $\mathbb{Q}$. The elements of K are called **algebraic numbers.** An algebraic number is called **integral,** or an **algebraic integer,** if it is a zero of a monic polynomial $f(x) \in \mathbb{Z}[x]$. This notion of integrality applies not only to algebraic numbers, but occurs in many different contexts and therefore has to be treated in full generality.

In what follows, -rings are always understood to be commutative rings with .1.

(2.1) Definition. Let *A* -� *B be an extension .of rings. An* element b E *B is called* **integral** *over* A, if *it satisfies a monic equation*

$$xn-+a_1xn-l+\cdots+an-=0, \qquad n::::1,$$

•• *with coefflcients-a;* EA. *The ring B is called* **integral** *over A ifall elements* b E *B* are *integral over A.*

It is desirable, but strangely enough not immediately obvious, that the sum and the product of two elements which are integral over *A* are again integral. This wjlJ be a consequence of the following abstract reinterpretation of the notion of integrality.

{**2.2) Proposition.** *Finitely many* elements b1, ... , *bn* E *B are all integral* over *A if and only ifthe ring A[b1, ... , bn] viewed as an A-module is finitely* generated.

To prove this we make use ofthe following result of linear algebra.

(2.3) Proposition (Row-Column Expansion). *Let A* = *(a;_;) be an (r* x *r)-matrix with entries in an arbitrary ring, and let A** = *(a;1)* be *the adjoint matrix,* i.e., *a0*= (-I)i+J det(A;j), *where the matrix AiJ* is *obtained* from *A by deleting the* i -'*th column and* the *j -th row. Then one has*

$$AA^*= A^*A= \det(A)E,$$

where *E denotes the unit matrix* of *rank r. For any vector x* = *(x1, ... , xr), this yields the implication*

$$Ax= 0 \implies (\det A)x = 0.$$

Proof of proposition (2.2): LeLb E *B* be integral over *A* and *f(x)* E *A[xJ* a monic polynomial of degree *n* :::: 1 such that f(b) = 0. For an arbitrary polynomial *g(x)* E A[x] we may then write

$$g(x) = q(x)f(x) + r(x),$$

with q(x), *r(x)* E *A[x]* and deg(r(x)) < *n_*, so that one has

$$g(b) = r(b) = a_0 + a_1b + \cdots + a_{n-1}b^{n-1}.$$

Thus *A_[b]* is generated as A-module=b_y I ,*b*, ... , *hn-l.*

More generally, if $b_1, \dots, b_n \in B$ are integral over A, then the fact that $A[b_1, \dots, b_n]$ is of finite type over A follows by induction on n. Indeed, since b_n is integral over $R = A[b_1, \dots, b_{n-1}]$, what we have just shown implies that $R[b_n] = A[b_1, \dots, b_n]$ is finitely generated over R, hence also over A, if we assume, by induction, that R is an A-module of finite type.

Conversely, assume that the A-module $A[b_1, \dots, b_n]$ is finitely generated and that $w_1, \dots, w_r$ is a system of generators. Then, for any element $b \in A[b_1, \dots, b_n]$, one finds that

$$b w_i = \sum_{j=1}^{r} a_{ij} w_j, \quad i = 1, \dots, r, \quad a_{ij} \in A.$$

From (2.3) we see that $\det(bE - (a_{ij}))w_i = 0$, $i = 1, \dots, r$ (here E is the unit matrix of rank r), and since 1 can be written $1 = c_1 w_1 + \dots + c_r w_r$, the identity $\det(bE - (a_{ij})) = 0$ gives us a monic equation for b with coefficients in A. This shows that b is indeed integral over A. □

According to this proposition, if $b_1, \dots, b_n \in B$ are integral over A, then so is *any* element b of $A[b_1, \dots, b_n]$, because $A[b_1, \dots, b_n, b] = A[b_1, \dots, b_n]$ is a finitely generated A-module. In particular, given two integral elements $b_1, b_2 \in B$, then $b_1 + b_2$ and $b_1 b_2$ are also integral over A. At the same time we obtain the

(2.4) Proposition. Let $A \subset B \subset C$ *be two ring extensions. If C is integral over B and B is integral over A, then C is integral over* A.

Proof: Take $c \in C$, and let $c^n + b_1 c^{n-1} + \dots + b_n = 0$ be an equation with coefficients in B. Write $R = A[b_1, \dots, b_n]$. Then $R[c]$ is a finitely generated R-module. If B is integral over A, then $R[c]$ is even finitely generated over A, since R is finitely generated over A. Thus c is integral over A. □

From what we have proven, the set of all elements

$$\bar{A} = \{ b \in B \mid b \text{ integral over } A \}$$

in a ring extension $A \subset B$ forms a ring. It is called the **integral closure** of A in B. A is said to be **integrally closed** in B if $A = \bar{A}$. It is immediate from (2.4) that the integral closure $\bar{A}$ is itself integrally closed in B. If A is an integral domain with field of fractions K, then the integral closure $\bar{A}$ of A in K is called the **normalization** of A, and A is simply called integrally closed if $A = \bar{A}$. For instance, every **factorial** ring is integrally closed.

In fact, if a/ b E K (a, b E A) is integral over A, i.e.,

$$(a/b)^{n} + a1\,(a/h)^{n-1} + \cdots + an = 0,$$

with ai E A, then

$$a^n + a_1 b a^{n-1} + \cdots + a_n b^n = 0 .$$

Therefore each prime element n which divides b also divides a. Assuming a/b to be reduced, this implies a/b E A.

We now tum to a more specialized situation. Let A be an integral domain which is integrally closed, K its field of fractions, Ll K a finite field .extension, and B the integral closure of A in L According to (2.4), B is automatically integrally dosed. Each element $f3$ E L is of the form

$$f3 = \frac{b}{a}, \quad bEB, aEA,$$

because if

$$an\,fr + \cdots + a_1\,f3 + ao = 0, \qquad Gi \text{ E } A,\ an \neq 0,$$

then $h = an\,f3$ ·is integral over A, an integral equation

$$(anf3t + \cdots + a;(an/3) + ab = 0, \quad .a; \text{ E } A,$$

being obtained from the equation for $f3$ by multiplication by ai^{-1}. Furthermore, the 'fact-that A is integrally closed has the effect that an element $f3$ E L is inte_gral-over A if and only if its **minimal polynomial** $p(x)$ takes its coefficients in A. In fact, let $f3$ be a.zero of the monic polynomial $g(x)$ E $A[x]$. Then $p(x)$ divides $g(x)$ in K[x], so that all zeroes /h, ..., $f3n$ of $p(x)$ are integral over A, hence 1Ire same holds for all the coefficients, m other words $p(x)$ E A[x}.

The trace and the norm in the .field extension LJK furnish important tools for the Study of the integral elements in L. We recall the

(.2.5) "Definition. *The* **trace** *and* **norm** *of an* element x E L *are* defined *to be* the *trace and* determinant, *respectively,,of the endomorphism*

$$T_x : L \to L, \quad T_x(\alpha) = x\alpha,$$

,of *the* K-vector *space L:*

$$Tr_{L|K}(x) = Tr(T_x), \quad N_{L|K}(x) = \det(T_x).$$

In the characteristic polynomial

$$f_x(t) = \det(t\,\mathrm{id} - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t]$$

of T_x, $n = [L:K]$, we recognize the trace and the norm as

$$a_1 = Tr_{L|K}(x) \quad \text{and} \quad a_n = N_{L|K}(x).$$

Since $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \circ T_y$, we obtain homomorphisms

$$Tr_{L|K} : L \to K \quad \text{and} \quad N_{L|K} : L^* \to K^*.$$

In the case where the extension $L|K$ is separable, the trace and norm admit the following Galois-theoretic interpretation.

(2.6) Proposition. *If $L|K$ is a separable extension and $\sigma : L \to \bar{K}$ varies over the different K-embeddings of L into an algebraic closure $\bar{K}$ of K, then we have*

(i) $f_x(t) = \prod_\sigma (t - \sigma x)$,

(ii) $Tr_{L|K}(x) = \sum_\sigma \sigma x$,

(iii) $N_{L|K}(x) = \prod_\sigma \sigma x$.

Proof: The characteristic polynomial $f_x(t)$ is a power

$$f_x(t) = p_x(t)^d, \quad d = [L : K(x)],$$

of the minimal polynomial

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m, \qquad m = [K(x) : K],$$

of x. In fact, $1, x, \ldots, x^{m-1}$ is a basis of $K(x)|K$, and if $\alpha_1, \ldots, \alpha_d$ is a basis of $L|K(x)$, then

$$\alpha_1, \alpha_1 x, \ldots, \alpha_1 x^{m-1}; \;\ldots;\; \alpha_d, \alpha_d x, \ldots, \alpha_d x^{m-1}$$

is a basis of $L|K$. The matrix of the linear transformation $T_x : y \mapsto xy$ with respect to this basis has obviously only blocks along the diagonal, each of them equal to

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}.$$

The corresponding characteristic polynomial is easily checked to be

$$t^m + c_1 t^{m-1} + \cdots + c_m = p_x(t),$$

so that finally $f_x(t) = p_x(t)^d$.

The set $\operatorname{Hom}_K(L, \bar K)$ of all K-embeddings of L is partitioned by the equivalence relation

$$\sigma \sim \tau \iff \sigma x = \tau x$$

into m equivalence classes of d elements each. If $\sigma_1, \ldots, \sigma_m$ is a system of representatives, then we find

$$p_x(t) = \prod_{i=1}^{m} (t - \sigma_i x),$$

and $f_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)^d = \prod_{i=1}^{m} \prod_{\sigma \sim \sigma_i} (t - \sigma x) = \prod_{\sigma} (t - \sigma x)$. This proves (i), and therefore also (ii) and (iii), after Vieta. □

(2.7) **Corollary.** *In a tower of finite field extensions $K \subseteq L \subseteq M$, one has*

$$Tr_{L|K} \circ Tr_{M|L} = Tr_{M|K}, \quad N_{L|K} \circ N_{M|L} = N_{M|K}.$$

Proof: We assume that $M|K$ is separable. The set $\operatorname{Hom}_K(M, \bar K)$ of K-embeddings of M is partitioned by the relation

$$\sigma \sim \tau \iff \sigma|_L = \tau|_L$$

into $m = [L:K]$ equivalence classes. If $\sigma_1, \ldots, \sigma_m$ is a system of representatives, then $\operatorname{Hom}_K(L, \bar K) = \{\sigma_i|_L \mid i = 1, \ldots, m\}$, and we find

$$Tr_{M|K}(x) = \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma x = \sum_{i=1}^{m} Tr_{\sigma_i M|\sigma_i L}(\sigma_i x) = \sum_{i=1}^{m} \sigma_i Tr_{M|L}(x)$$
$$= Tr_{L|K}\big(Tr_{M|L}(x)\big).$$

Likewise for the norm.

We will not need the inseparable case for the sequel. However it follows easily from what we have shown above, by passing to the maximal separable subextension $M_s|K$. Indeed, for the inseparable degree $[M:K]_i = [M:M_s]$ one has $[M:K]_i = [M:L]_i[L:K]_i$ and

$$Tr_{M|K}(x) = [M:K]_i \, Tr_{M_s|K}(x), \qquad N_{M|K}(x) = N_{M_s|K}(x)^{[M:K]_i}$$

(see [143], vol. I, chap. II, § 10). □

The **discriminant** of a basis $\alpha_1, \dots, \alpha_n$ of a separable extension $L|K$ is defined by

$$d(\alpha_1, \dots, \alpha_n) = \det((\sigma_i\alpha_j))^2,$$

where σ_i, $i = 1, \dots, n$, varies over the K-embeddings $L \to \bar{K}$. Because of the relation

$$Tr_{L|K}(\alpha_i\alpha_j) = \sum_k (\sigma_k\alpha_i)(\sigma_k\alpha_j),$$

the matrix $(Tr_{L|K}(\alpha_i\alpha_j))$ is the product of the matrices $(\sigma_k\alpha_i)^t$ and $(\sigma_k\alpha_j)$. Thus one may also write

$$d(\alpha_1, \dots, \alpha_n) = \det(Tr_{L|K}(\alpha_i\alpha_j)).$$

In the special case of a basis of type $1, \theta, \dots, \theta^{n-1}$ one gets

$$d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2,$$

where $\theta_i = \sigma_i\theta$. This is seen by successively multiplying each of the first $(n-1)$ columns in the **Vandermonde matrix**

$$\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix}$$

by θ_1 and subtracting it from the following.

(2.8) Proposition. *If $L|K$ is separable and $\alpha_1, \dots, \alpha_n$ is a basis, then the discriminant*

$$d(\alpha_1, \dots, \alpha_n) \neq 0,$$

and

$$(x, y) = Tr_{L|K}(xy)$$

is a nondegenerate bilinear form on the K-vector space L.

Proof: We first show that the bilinear form $(x, y) = Tr(xy)$ is nondegenerate. Let θ be a primitive element for $L|K$, i.e., $L = K(\theta)$. Then $1, \theta, \dots, \theta^{n-1}$ is a basis with respect to which the form (x, y) is given by the matrix $M = (Tr_{L|K}(\theta^{i-1}\theta^{j-1}))_{i,j=1,\dots,n}$. It is nondegenerate because, for $\theta_i = \sigma_i\theta$, we have

$$\det(M) = d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0.$$

If $\alpha_1, \dots, \alpha_n$ is an arbitrary basis of $L|K$, then the bilinear form (x, y) with respect to this basis is given by the matrix $M = (Tr_{L|K}(\alpha_i\alpha_j))$. From the above it follows that $d(\alpha_1, \dots, \alpha_n) = \det(M) \neq 0$. □

After this review from .the theory of fields, we return to the integrally dosed integral domain A with field of fractions K, .and to its integral closure B in ihe finite separable extension $L|K$. If $x \in B$ is an integral element of L, then all of its conjugate.s σx are also integral. Taking into account that A is integrally closed, i.e., $A = B \cap K$, (2:6) implies that

$$Tr_{L|K}(x), \quad N_{L|K}(x) \in A.$$

Furthermore, for the group o-funits of B over A, we obtain the relation

$$x \in B^* \iff N_{L|K}(x) \in A^*.$$

For ifaNL1dx) $= 1$, $a \in A$, then $1 = a^{-1} \prod \sigma x = yx$ for some $y \in B$. The discriminant is often u.seful because -of the following

(2.9) Lemma. Let $\alpha_1, \dots, \alpha_n$ *be a basis of* $L|K$ *which is contained in* B, *of discriminant* $d = d(\alpha_1, \dots, \alpha_n)$. *Then one has*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Proof: If $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$, $a_j \in K$, then the a_j are a solution of the .system of linear equations

$$Tr_{L|K}(\alpha_i\alpha) = \sum_j Tr_{L|K}(\alpha_i\alpha_j)a_j,$$

and, as $Tr_{L|K}(\alpha_i\alpha) \in A$, they are given as the quotient of an element of A by the determinant $\det(Tr_{L|K}(\alpha_i\alpha_j)) = d$. Therefore $da_j \in A$, and thus

$$d\alpha \in A\alpha_1 + \cdots + A\alpha_n.$$

A system of elements $\omega_1, \dots, \omega_n \in B$ such that each $b \in B$ can be written uniquely as a linear combination

$$b = a_1\omega_1 + \cdots + a_n\omega_n$$

with coefficients $a_i \in A$, is called an **integral basis** of B over A (or: an A-basis of B). Since such an inte.gral basis is automatically a basis of $L|K$, .its length n always .equals the degree $[L:K]$ of the field extension. The existence of an integral basis signifies that B is a **free A-module** of rank $n = [L:K]$. In general, such an integral basis does not exist. If, however, A is a principal ideal domain, then one has the following more general

(2.10) Proposition. *If* $L|K$ *is separable and* A *is a principal ideal domain, then every finitely generated* B*-submodule* $M \neq 0$ *of* L *is a free* A*-module of rank* $[L:K]$. *In particular,* B *admits an integral basis over* A.

Proof: Let *M* -=*ft* O be a finitely generated B--submodule of Land *a1,* , *an* a basis of LI*K.* Multiplying by an element of A, we may arrange for the *ai* to fie in *B.* By (2.9), we then .have *dB* S; *Aa1* + • • • + *Aan,* in particular, rank(B):::; *[L: K],* and since a system of.generators of the A-module Bis also a system of generators of the *K*-module *L,* we have rank(B) = •*[L : K].* Let *μ,*1, ... , *μr* E *M* be a system of generators of the *B*-module *M.* There exists an *a* EA, *a#* 0, such that *aμ,i* E *B,.i* = 1, ... , *r,* so that *aM* •S; *B.* Then

adM -S; *dB* S; *Aa1* +···· + *Aan* =Mo.

According to the main theorem on finitely generated modules over principal ideal domains, since *Mo* is a free A-module, so is *ad M,* and hence also ***M.*** Finally,

*[L : **K]*** = rank(B) :::; rank(M) = rank(ad*M)* :::; rank(Mo) = *[L :**K],***

hence rank(M) = *[L : **K].*** □

It is **in** general a difficult problem to produce integral ba<;es. **In** concrete situations it can also be an important one. This is why the following proposition is interesting. Instead of integral bases ·of the integral closure *B* of *A* in *L,* we will now simply speak of integral bases of the extension LI *K.*

('.l.11) Proposition. *Let L* IK *and L'IK be two Galois* extensions of degree *n, resp. n', such that* L n *L'* = *K. Let w1, ... , wn, resp.* di, ... , *w�,,* be *an integral basis of L* I *K, resp. L'* IK, *with discriminant d,* resp. *d'. Suppose that d and d' are relatively prime in* the sense *that xd* + *x'd'* = 1, for *suitable x, x'* E *A. Then wi w1 is an integral basis of LL',-of discriminant dn'drn.*

Proof: As *L* n *L'* = *K,* we have *[LL'* : *K]* = *nn',* so the *nn'* products *w;w1* do form a basis of *LL'* IK. Now 1et *a* be an integral element of *LL',* and write

$$a = La;; \; wi \; w1, \quad a;; \in K.$$
$$\text{i, } j$$

We have to show that *a;J* E *A.* Put */3;* = *LiaiJ Wi,*Let *G(LL'IL')* {a1, ... , *an}* and *G(LL'IL)* = {o:{, ... , *u�,}.* Thus

$$G(LL'|K) = \{\sigma_k\sigma'_\ell \mid k = 1, \ldots, n, \ \ell = 1, \ldots, n'\}.$$

Putting

$$T = (\sigma'_\ell\omega'_j), \quad a = (\sigma'_1\alpha, \ldots, \sigma'_{n'}\alpha)^t, \quad b = (/J,' \ldots ' \; fJn')I'$$

one finds det{T)2 = d' and

$$a = Tb.$$

Write T^* for the adjoint matrix of T. Then row-column expansion (2.3) gives

$$\det(T)b = T^*a.$$

Since T^* and a have integral entries in LL', the multiple $d'h$ has integral entries in L, namely $d'f3J = Lid'aiJ\, Wi$. Thus $d'aiJ$ E A. Swapping the roles of (w;) and (w1), one checks in the same manner that $daiJ$ E A, so that

$$aiJ = xdaiJ + x'd'au \text{ E } A\,.$$

Therefore w; w1 is indeed an integral basis of $LL'IK$. We compute the discriminant $L1$ of this integral basis. Since $G(LL'IK)$ = {oJc'.T� I k = I, ... , n, £ = 1, ... , nil, it is the square of the determinant of the (nn' x nn')·matrix

$$M = (crka; WjWj) = (akWi\, a;wj).$$

This matrix is itself an (n' x n')-matrix with entries (n x n)�matrices of which the (£, })-entry is the matrix $Qo:$�w1 where $Q = (akw;)$. In other words,

$$M = \begin{pmatrix} Q & & 0 \\ & \ddots & \\ 0 & & Q \end{pmatrix} \begin{pmatrix} E\sigma_1'\omega_1' & \cdots & E\sigma_{n'}'\omega_1' \\ \vdots & & \vdots \\ E\sigma_1'\omega_{n'}' & \cdots & E\sigma_{n'}'\omega_{n'}' \end{pmatrix}.$$

Here E denotes the (n x n)•unit matrix. By changing indices the second matrix may be transformed to look like the first one. This yields

$$\Delta = \det(M)^2 = \det(Q)^{2n'} \det\big((\sigma_\ell'\omega_j')\big)^{2n} = d^{n'} d'^{n}\,. \qquad \square$$

Remark: It follows from the proof thatthe proposition is valid for arbitrary separable extensions (not necessarily Galois), if one assumes instead of $L \cap L' = K$ that L and L' are Jinearly disjoint.

The chief application of our considerations on integrality will .concern the integral closure OK s; K of Z � (Ql in an algebraic number field K. By ·proposition (2.10), every finitely generated OK-suomodule a of K admits a Z-basis $a,$, ... , Ctn,

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n\,.$$

The discriminant

$$d(et1, \ldots, an) = \det((a;a;))^2$$

is independent of the choice of a $\mathbb{Z}$-basis; if $\alpha_1', \dots, \alpha_n'$ is another basis, then the base change matrix $T = (a_{ij})$, $\alpha_i' = \sum_j a_{ij}\alpha_j$, as well as its inverse, has integral entries. It therefore has determinant ± 1, so that indeed

$$d(\alpha_1', \dots, \alpha_n') = (\det T)^2\, d(\alpha_1, \dots, \alpha_n) = d(\alpha_1, \dots, \alpha_n).$$

We may therefore write

$$d(\mathfrak{a}) = d(\alpha_1, \dots, \alpha_n).$$

In the special case of an integral basis $\omega_1, \dots, \omega_n$ of $\mathcal{O}_K$ we obtain the **discriminant of the algebraic number field** K,

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \dots, \omega_n).$$

In general, one has the

(2.12) Proposition. *If $\mathfrak{a} \subseteq \mathfrak{a}'$ are two nonzero finitely generated $\mathcal{O}_K$-submodules of K, then the index $(\mathfrak{a}' : \mathfrak{a})$ is finite and satisfies*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2\, d(\mathfrak{a}').$$

All we have to show is that the index $(\mathfrak{a}' : \mathfrak{a})$ equals the absolute value of the determinant of the base change matrix passing from a $\mathbb{Z}$-basis of $\mathfrak{a}$ to a $\mathbb{Z}$-basis of $\mathfrak{a}'$. This proof is part of the well-known theory of finitely generated $\mathbb{Z}$-modules.

Exercise 1. Is $\frac{3+2\sqrt[4]{6}}{1-\sqrt{6}}$ an algebraic integer?

Exercise 2. Show that, if the integral domain A is integrally closed, then so is the polynomial ring $A[t]$.

Exercise 3. In the polynomial ring $A = \mathbb{Q}[X, Y]$, consider the principal ideal $\mathfrak{p} = (X^2 - Y^3)$. Show that $\mathfrak{p}$ is a prime ideal, but $A/\mathfrak{p}$ is not integrally closed.

Exercise 4. Let D be a squarefree rational integer $\neq 0, 1$ and d the discriminant of the quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Show that

$$d = D, \qquad \text{if } D \equiv 1 \bmod 4,$$

$$d = 4D, \qquad \text{if } D \equiv 2 \text{ or } 3 \bmod 4,$$

and that an integral basis of K is given by $\{1, \sqrt{D}\}$ in the second case, by $\{1, \frac{1}{2}(1 + \sqrt{D})\}$ in the first case, and by $\{1, \frac{1}{2}(d + \sqrt{d})\}$ in both cases.

Exercise 5. Show that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{2})$.

Exercise 6. Show that $\{1, \theta, \frac{1}{2}(\theta + \theta^2)\}$ is an integral basis of $\mathbb{Q}(\theta)$, $\theta^3 - \theta - 4 = 0$.

Exercise 7. The discriminant d_K of an algebraic number field K is always $\equiv 0 \bmod 4$ or $\equiv 1 \bmod 4$ *(Stickelberger's discriminant relation).*

Hint: The determinant $\det(\sigma_i\omega_j)$ of an integral basis ω_j is a sum of terms, each prefixed by a positive or a negative sign. Writing P, resp. N, for the sum of the positive, resp. negative terms, one finds $d_K = (P - N)^2 = (P + N)^2 - 4PN$.

§ 3. Ideals

Being a generalization of the ring Z s::; Q, the ring *o K* of integers of an algebraic number field *K* is at the center of an our considerations. As in Z, every ,non-unit *a* # 0 can be factored in *o K* into a product of irreducible elements. For if *a* is not itself irreducible, then it can be written as a product of two non-units *a* = *f3y*. Then by,§2, one has

$$1 < \left|N_{K|\mathbb{Q}}(\beta)\right| < \left|N_{K|\mathbb{Q}}(\alpha)\right|, \quad 1 < \left|N_{K|\mathbb{Q}}(\gamma)\right| < \left|N_{K|\mathbb{Q}}(\alpha)\right|,$$

and the prime decomposition of *a* follows by inducfion from those of *f3* and *'Y*. However, contrary to what happens in the rings Z and ,;;z[,i], the uniqueness of prime factorization does not hold in general.

Example: The ring of integers of the field *K* = Q(H) ,is given by §2, exercise 4, as *OK* = *;;z,* + ZH. In this ring, the rational integer 21 can be decomposed in two ways,

21 = 3. 7 = O + 2J=s). O -2✓-'s).

All factors occurring here are irreducible in *o K.* For •if one had, for instance, 3 = *af3,* with *a, f3* non-units, then 9 = *NKrQ(a)N* KIQ(/3) would imply *N*Ki!Ql(a) = ±3. But the equation

NK1Q(X + yN) = x^2 + sy2 = ±3

has no solutions in Z. In the same way it is seen that 7, I + 2,J=s, and **1** - 2,J=s are irreducible. As the fractions

$$\frac{1 \pm 2R}{3} \qquad \frac{1 \pm 2,J=s}{7}$$

do not belong to *OK,* the numbers 3 and 7 are not associated to 1 + *2H* or 1 - 2H. The two prime factorizations of 21 are therefore essentially different.

Realizing the failure of unique factorization in general has led to one ohhe grand events in the history of number theory, the discovery of ideal theory by *EouMw KUMMER.* Inspired by the discovery of complex numbers, Kummer's idea was that fhe integers of *K* would have to aamit an embedding into a bigger ,domain of "ideal numbers" where **unique** factorization into "ideal prime numbers" would hold. For :instance, in the example of

$$21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5}),$$

the factors on ,the .right would be composed of ideal -Prime numbers $\mathfrak{p}_1, \mathfrak{p}_2$, $\mathfrak{p}_3, \mathfrak{p}_4$, subject to the rules

$$3 = \mathfrak{p}_1\mathfrak{p}_2, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1+2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \quad 1-2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4.$$

This would resolve the above non-uniqueness into the wonderfully unique factorization

$$21 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4).$$

Kummer's concept of "ideal numbers" was iater replaced by that of **ideals** of the ring $\mathcal{O}_K$. The reason for this is easify seen: whatever an ideal number $\mathfrak{a}$ should be defined to be, it ought to be linked to certain numbers $a \in \mathcal{O}_K$ by a divisibility relation $\mathfrak{a} \mid a$ satisfying the following rules, for $a, b, \lambda \in \mathcal{O}_K$,

$$\mathfrak{a}\mid a \text{ and } \mathfrak{a}\mid b \Longrightarrow \mathfrak{a}\mid a\pm b; \qquad \mathfrak{a}\mid a \Longrightarrow \mathfrak{a}\mid \lambda a.$$

And an ideal number $\mathfrak{a}$ should be determined by the totality of its divisors in $\mathcal{O}_K$

$$\mathfrak{a} = \{a \in \mathcal{O}_K \mid \mathfrak{a}\mid a\}.$$

But in view of the rules for divisibility, this s.et is an ideal of $\mathcal{O}_K$.

This is the reason why *RICHARD DEDEKIND* re-introduced Kummer's "ideal numbers" as being the ideals of $\mathcal{O}_K$. Once this is done, the divisibility relation $\mathfrak{a} \mid a$ can simply be defined by the inclusion $a \in \mathfrak{a}$, and more generally the divisibility relation $\mathfrak{a} \mid \mathfrak{b}$ between two ideals by $\mathfrak{b} \subseteq \mathfrak{a}$. In what follows, we will .study .this notion of divisibility more closely. The basic theorem here is the following.

(3.1) Theorem. *The ring $\mathcal{O}_K$ is noetherian, integrally closed, and every prime ideal $\mathfrak{p} \neq 0$ is a maximal ideal.*

Proof: $\mathcal{O}_K$ is noetherian because every ideal $\mathfrak{a}$ is a finitely generated $\mathbb{Z}$-module by (2.10), and therefore *a fortiori* a finitely generated $\mathcal{O}_K$-module. By §2, $\mathcal{O}_K$ is also integrally closed, being the integral closure of $\mathbb{Z}$ in K. It thus remains to show that each prime ideal $\mathfrak{p} \neq 0$ is maximal. Now, $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal (p) in $\mathbb{Z}$: the primality is clear, and if $y \in \mathfrak{p}$, $y \neq 0$, and

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0$$

is an equation for y with $a_i \in \mathbb{Z}$, $a_n \neq 0$, then $a_n \in \mathfrak{p} \cap \mathbb{Z}$. The integral domain $\bar{\mathcal{O}} = \mathcal{O}_K/\mathfrak{p}$ arises from $\kappa = \mathbb{Z}/p\mathbb{Z}$ by adjoining algebraic elements and is therefore again a field (recall the fact that $\kappa[a] = \kappa(a)$, if a is algebraic). Therefore $\mathfrak{p}$ is a maximal ideal. □

The three properties of the ring o_K which we have just proven lay the foundation of the whole theory of divisibility of its ideals. This theory was developed by Dedekind, which suggested the following

(3.2) **Definition.** *A noetherian, integrally closed integral domain in which every nonzero* prime *ide::11* is maximal is *called* a **Dedekind domain.**

Just as the rings of the fonn o_K may be viewed as generalizations of the ring Z, the Dedekind domains may be viewed as generalized principal ideal domains. Indeed, if A is a principal ideal domain with field of fractions K, and LI K is a finite field extension, then the integral closure B of A in L is, in general, not a principal ideal domain, but always a Dedekind domain, as we shall show further on.

Instead of the ring o_K we will now consider an arbitrary Dedekind domain o, and we denote by K the field of fractions of o. Given two ideals a and b of o (or more generally of an arbitrary ring), the divisibility relation alb is defined by b c;;:; a, and the sum of the ideals by

$$a+b = \{a+b \mid a \in a, b \in b\}.$$

This is the smallest ideal containing a as well as b, in other words, il is the greatest common divisor gcd(n, b) of n and b. By the same token the intersection n $\cap$ b is the 1cm (least common multiple) of a and b. We define the **prnduct** of n and b by

$$ab = \{\textstyle\sum a_i b_i \mid a_i \in a, b_i \in b\}.$$

With respect to this multiplication the ideals of o will grant us what the elements alone may refuse to provide: the **unique prime factorization.**

(3.3) **Theorem.** Every *ideal* a of o *different* from (0) and (I) *admit!>* a *factorization*

$$a = P_1 \cdots P_r$$

into nonzero prime ideals P_i *of* o *which is unique up to the order of the factor.*

This theorem is of course perfectly in line with the invention of "ideal numbers". Still, the fact that it holds is remarkable because its proof is far from straightforward, and unveils a deeper principle governing the arithmetic in o. We prepare the proof proper by two lemmas.

(3.4) Lemma. *For every ideal* $\mathfrak{a} \neq 0$ *of* $\mathcal{O}$ *there exist nonzero prime ideals* $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ *such that*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r .$$

Proof: Suppose the set $\mathfrak{M}$ of those ideals which do not fulfill this condition is nonempty. As $\mathcal{O}$ is noetherian, every ascending chain of ideals becomes stationary. Therefore $\mathfrak{M}$ is inductively ordered with respect to inclusion and thus admits a maximal element $\mathfrak{a}$. This cannot be a prime ideal, so there exist elements $b_1, b_2 \in \mathcal{O}$ such that $b_1 b_2 \in \mathfrak{a}$, but $b_1, b_2 \notin \mathfrak{a}$. Put $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$. Then $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$ and $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. By the maximality of $\mathfrak{a}$, both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ contain a product of prime ideals, and the product of these products is contained in $\mathfrak{a}$, a contradiction. □

(3.5) Lemma. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathcal{O}$ *and define*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\}.$$

Then one has $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a},\ x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$, *for every ideal* $\mathfrak{a} \neq 0$.

Proof: Let $a \in \mathfrak{p}$, $a \neq 0$, and $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, with r as small as possible. Then one of the $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$, and so $\mathfrak{p}_1 = \mathfrak{p}$ because $\mathfrak{p}_1$ is a maximal ideal. (Indeed, if none of the $\mathfrak{p}_i$ were contained in $\mathfrak{p}$, then for every i there would exist $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ such that $a_1 \cdots a_r \in \mathfrak{p}$. But $\mathfrak{p}$ is prime.) Since $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$, there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin a\mathcal{O}$, i.e., $a^{-1}b \notin \mathcal{O}$. On the other hand we have $b\mathfrak{p} \subseteq (a)$, i.e., $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, and thus $a^{-1}b \in \mathfrak{p}^{-1}$. It follows that $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Now let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}$ and $\alpha_1, \dots, \alpha_n$ a system of generators. Let us assume that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Then for every $x \in \mathfrak{p}^{-1}$

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in \mathcal{O}.$$

Writing A for the matrix $(x\delta_{ij} - a_{ij})$ we obtain $A(\alpha_1, \dots, \alpha_n)^t = 0$. By (2.3), the determinant $d = \det(A)$ satisfies $d\alpha_1 = \dots = d\alpha_n = 0$ and thus $d = 0$. It follows that x is integral over $\mathcal{O}$, being a zero of the monic polynomial $f(X) = \det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$. Therefore $x \in \mathcal{O}$. This means that $\mathfrak{p}^{-1} = \mathcal{O}$, a contradiction. □

Proof of (3.3): I. Existence of the prime ideal factorization. Let $\mathfrak{M}$ be the set of all ideals different from (0) and (1) which do not admit a prime ideal decomposition. If $\mathfrak{M}$ is nonempty, then we argue as for (3.4) that there exists a maximal element $\mathfrak{a}$ in $\mathfrak{M}$. It is contained in a maximal ideal $\mathfrak{p}$, and the inclusion $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ gives us

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}.$$

By (3.5), one has $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$. Since $\mathfrak{p}$ is a maximal ideal, it follows that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. In view of the maximality of $\mathfrak{a}$ in $\mathfrak{M}$ and since $\mathfrak{a} \neq \mathfrak{p}$, i.e., $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, the ideal $\mathfrak{a}\mathfrak{p}^{-1}$ admits a prime ideal decomposition $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, and so does $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, a contradiction.

II. Uniqueness of the prime ideal factorization. For a prime ideal $\mathfrak{p}$ one has: $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$, i.e., $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. Let

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

be two prime ideal factorizations of $\mathfrak{a}$. Then $\mathfrak{p}_1$ divides a factor $\mathfrak{q}_i$, say $\mathfrak{q}_1$, and being maximal equals $\mathfrak{q}_1$. We multiply by $\mathfrak{p}_1^{-1}$ and obtain, in view of $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$, that

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Continuing like this we see that $r = s$ and, possibly after renumbering, $\mathfrak{p}_i = \mathfrak{q}_i$, for all $i = 1, \ldots, r$. □

Grouping together the occurrences of the same prime ideals in the prime ideal factorization of an ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}$ gives a product representation

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}, \quad \nu_i > 0.$$

In the sequel such an identity will be automatically understood to signify that the $\mathfrak{p}_i$ are pairwise distinct. If in particular $\mathfrak{a}$ is a principal ideal (a), then – following the tradition which tends to attribute to the ideals the rôle of "ideal numbers" – we will write with a slight abuse of notation

$$a = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}.$$

Similarly, the notation $\mathfrak{a} \mid a$ is often used instead of $\mathfrak{a} \mid (a)$ and $(\mathfrak{a}, \mathfrak{b}) = 1$ is written for two relatively prime ideals, instead of the correct formula $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \mathcal{O}$. For a product $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ of relatively prime ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, one has an analogue of the well-known "Chinese Remainder Theorem" from elementary number theory. We may formulate this result for an arbitrary ring taking into account that

Indeed, since $\mathfrak{a}_i \mid \mathfrak{a}$, $i = 1, \ldots, n$, we find on the one hand that $\mathfrak{a} \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$, and for $a \in \bigcap_i \mathfrak{a}_i$ we find that $\mathfrak{a}_i \mid a$ and therefore, the factors being relatively prime, we get $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n \mid a$, i.e., $a \in \mathfrak{a}$.

(3.6) Chinese Remainder Theorem. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ *be ideals in a ring* $\mathcal{o}$ *such that* $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{o}$ *for* $i \neq j$. *Then, if* $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{a}_i$, *one has*

$$\mathcal{o}/\mathfrak{a} \cong \bigoplus_{i=1}^n \mathcal{o}/\mathfrak{a}_i .$$

Proof: The canonical homomorphism

$$\mathcal{o} \to \bigoplus_{i=1}^n \mathcal{o}/\mathfrak{a}_i, \quad a \mapsto \bigoplus_{i=1}^n a \bmod \mathfrak{a}_i,$$

has kernel $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$. It therefore suffices to show that it is surjective. For this, let $x_i \bmod \mathfrak{a}_i \in \mathcal{o}/\mathfrak{a}_i$, $i = 1, \dots, n$, be given. If $n = 2$, we may write $1 = a_1 + a_2$, $a_i \in \mathfrak{a}_i$, and putting $x = x_2 a_1 + x_1 a_2$ we get $x \equiv x_i \bmod \mathfrak{a}_i$, $i = 1, 2$.

If $n > 2$, we may find as before an element $y_1 \in \mathcal{o}$ such that

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \bigcap_{i=2}^n \mathfrak{a}_i,$$

and, by the same token, elements $y_2, \dots, y_n$ such that

$$y_i \equiv 1 \bmod \mathfrak{a}_i, \quad y_i \equiv 0 \bmod \mathfrak{a}_j \quad \text{for } i \neq j.$$

Putting $x = x_1 y_1 + \dots + x_n y_n$ we find $x \equiv x_i \bmod \mathfrak{a}_i$, $i = 1, \dots, n$. This proves the surjectivity. □

Now let $\mathcal{o}$ be again a Dedekind domain. Just as for nonzero numbers, we may obtain **inverses** for the nonzero ideals of $\mathcal{o}$ by introducing the notion of fractional ideal in the field of fractions K.

(3.7) Definition. *A* **fractional ideal** *of* K *is a finitely generated* $\mathcal{o}$*-submodule* $\mathfrak{a} \neq 0$ *of* K.

For instance, an element $a \in K^*$ defines the fractional "principal ideal" $(a) = a\mathcal{o}$. Obviously, since $\mathcal{o}$ is noetherian, an $\mathcal{o}$-submodule $\mathfrak{a} \neq 0$ of K is a fractional ideal if and only if there exists $c \in \mathcal{o}$, $c \neq 0$, such that $c\mathfrak{a} \subseteq \mathcal{o}$ is an ideal of the ring $\mathcal{o}$. Fractional ideals are multiplied in the same way as ideals in $\mathcal{o}$. For distinction the latter may henceforth be called **integral ideals** of K.

(3.8) Proposition. *The fractional ideals form an abelian group, the* **ideal group** J_K *of* K. *The identity element is* $(1) = \mathcal{o}$, *and the inverse of* $\mathfrak{a}$ *is* a-¹=lxEKjxas;o)

Proof: One obviously has associativity, commutativity and $\mathfrak{a}(1) = \mathfrak{a}$. For a prime ideal $\mathfrak{p}$, (3.5) says that $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$ and therefore $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ because $\mathfrak{p}$ is maximal. Consequently, if $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ is an integral ideal, then $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$ is an inverse. $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ implies that $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Conversely, if $x\mathfrak{a} \subseteq \mathcal{O}$, then $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, so $x \in \mathfrak{b}$ because $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Thus we have $\mathfrak{b} = \mathfrak{a}^{-1}$. Finally, if $\mathfrak{a}$ is an arbitrary fractional ideal and $c \in \mathcal{O}$, $c \neq 0$, is such that $c\mathfrak{a} \subseteq \mathcal{O}$, then $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ is the inverse of $c\mathfrak{a}$, so $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

(3.9) Corollary. *Every fractional ideal $\mathfrak{a}$ admits a unique representation as a product*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

with $\nu_{\mathfrak{p}} \in \mathbb{Z}$ and $\nu_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. In other words, J_K is the free abelian group on the set of nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

Proof: Every fractional ideal $\mathfrak{a}$ is a quotient $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ of two integral ideals $\mathfrak{b}$ and $\mathfrak{c}$, which by (3.3) have a prime decomposition. Therefore $\mathfrak{a}$ has a prime decomposition of the type stated in the corollary. By (3.3), it is unique if $\mathfrak{a}$ is integral, and therefore clearly also in general. □

The fractional principal ideals $(a) = a\mathcal{O}$, $a \in K^*$, form a subgroup of the group of ideals J_K, which will be denoted P_K. The quotient group

$$Cl_K = J_K / P_K$$

is called the ideal class group, or class group for short, of K. Along with the group of units $\mathcal{O}^*$ of $\mathcal{O}$, it fits into the exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1,$$

where the arrow in the middle is given by $a \mapsto (a)$. So the class group Cl_K measures the expansion that takes place when we pass from numbers to ideals, whereas the unit group $\mathcal{O}^*$ measures the contraction in the same process. This immediately raises the problem of understanding these groups $\mathcal{O}^*$ and Cl_K more thoroughly. For general Dedekind domains they may turn out to be completely arbitrary groups. For the ring $\mathcal{O}_K$ of integers in a number field K, however, one obtains important finiteness theorems, which are fundamental for the further development of number theory. But these results cannot be had for nothing. They will be obtained by viewing the numbers geometrically as lattice points in space. For this we will now prepare the necessary concepts, which all come from linear algebra.

Exercise I. Decompose 33 + **11** *R* inio irreducible integral clements of Q(A).

Exen::lse 2. Show !hat

$$54=2\cdot3) = \frac{13+./=17}{2} \quad \frac{13-../-47}{2}$$

are two essentially different decompn�itions into irreducible integral elements of Q(,,Gi'i).

Exercise J, Le.:! *d* be squarefree and pa prime number not dividing *2d.* Leto he the ring of integers of Q(../*d*). Show lhal (pl = *po* is a prime ideal of *o* if and only if lhe congruence .,1² = *d* mod *p* has no solution.

Exercise 4. A Dedekind domain wilh a finile number of prime ideals is a principal ideal domain.

Hinl: If n = p:'¹ • • • p;� *f::*.0 i;. an idcul, then choose elements ;r, e p,,p; and apply the Chine� remainder theorem fur 1hc coset.s *;riv,* mod p;',¹¹

f.xerclse *S.* The quotient ring �1/0 of a IJcdekind domain by an ideal n *cf;* 0 is a principal ideal domain.

Hint: Por n = *μn* the only proper ideals of *o/a* are given by p/pn, ... , *μ*ⁿ·¹/p''. Choo!\e ;r e p, p² and show that p' = *o*l*fv* + p''.

Exercis� 6. Every ideal of :1 Dedekind domain can be gc11erated by 1wo eletn1::nls.

Hinl: Use exercise 5.

Exercise 7. In a noetherian ring *R* in which every prime ideal is maximal. each descending chain of ideals n_1 2 112 2 • • • heeomes statiomiry.

Hinl: Show as in (3.4) that (0) is H product p_1 · · · p, of prime ideals and that the -:hain /? 2 P1 2 P1P2 � ••• 2 Pi ···P, = (0) can be refined into a composition

Exercise 8. Let m be a ncnzero integral ideal of the Dedekind domain Cl. Show that in every ideal class of *Cf*ı, there exists an integral ideal ptime *to* m.

Exercise 9. U:1 *o* be an integral domain in which all nom:ero ideals admit a unique fac1orii.illion into prime icl:ab. Show that c, is a Dedekind domain.

Exercise **10.** The fractional ideals *a* of a Dedekind domain *o* arc projcc1ive *o*-modules, i.e., given any surjective homomorphism *M* � *N* of Cl-modules, each homomorphism a � *N* can be lifted *to* a homomorphi,m *h* : 11 ..... *M* such that *f* ∪*h=[!..*

§4. Lattices

In §I, when solving the hasie problems concerning the gaussian integers. we-used at a crucial pluce the inclusion

Z[il <;C

and considered the integers of $\mathbb{Q}(i)$ as lattice points in the complex plane. This point of view has been generalized to arbitrary number fields by HERMANN MINKOWSKI (1864–1909) and has led to results which make up an essential part of the foundations of algebraic number theory. In order to develop Minkowski's theory we first have to introduce the general notion of lattice and study some of its basic properties.

(4.1) Definition. *Let V be an n-dimensional $\mathbb{R}$-vector space. A* lattice *in V is a subgroup of the form*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

with linearly independent vectors $v_1, \dots, v_m$ of V. The m-tuple $(v_1, \dots, v_m)$ is called a basis *and the set*

$$\Phi = \{ x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R},\ 0 \le x_i < 1 \}$$

a fundamental mesh *of the lattice. The lattice is called* complete *or a* $\mathbb{Z}$-structure *of V, if $m = n$.*

The completeness of the lattice is obviously tantamount to the fact that the set of all translates $\Phi + \gamma$, $\gamma \in \Gamma$, of the fundamental mesh covers the entire space V.

The above definition makes use of a choice of linearly independent vectors. But we will need a characterization of lattices which is independent of such a choice. Note that, first of all, a lattice is a finitely generated subgroup of V. But not every finitely generated subgroup is a lattice – for instance $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$ is not. But each lattice $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ has the special property of being a discrete subgroup of V. This is to say that every point $\gamma \in \Gamma$ is an isolated point in the sense that there exists a neighbourhood which contains no other points of Γ. In fact, if

$$\gamma = a_1v_1 + \cdots + a_mv_m \in \Gamma,$$

then, extending $v_1, \dots, v_m$ to a basis $v_1, \dots, v_n$ of V, the set

$$\{ x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R},\ |a_i - x_i| < 1 \text{ for } i = 1, \dots, m \}$$

clearly is such a neighbourhood. This property is indeed characteristic.

(4.2) Proposition. *A subgroup $\Gamma \subseteq V$ is a lattice if and only if it is discrete.*

Proof: Let Γ be a discrete subgroup of V. Then Γ is closed. For let U be an arbitrary neighbourhood of 0. Then there exists a neighbourhood $U' \subseteq U$ of 0 such that every difference of elements of U' lies in U. If there were an $x \notin \Gamma$ belonging to the closure of Γ, then we could find in the neighbourhood $x+U'$ of x two distinct elements $\gamma_1, \gamma_2 \in \Gamma$, so that $0 \neq \gamma_1 - \gamma_2 \in U' - U' \subseteq U$. Thus 0 would not be an isolated point, a contradiction.

Let V_0 be the linear subspace of V which is spanned by the set Γ, and let m be its dimension. Then we may choose a basis $u_1, \dots, u_m$ of V_0 which is contained in Γ, and form the complete lattice

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Gamma$$

of V_0. We claim that the index $(\Gamma : \Gamma_0)$ is finite. To see this, let $\gamma_i \in \Gamma$ vary over a system of representatives of the cosets in Γ/Γ_0. Since Γ_0 is complete in V_0, the translates $\Phi_0 + \gamma$, $\gamma \in \Gamma_0$, of the fundamental mesh

$$\Phi_0 = \{x_1u_1 + \cdots + x_mu_m \mid x_i \in \mathbb{R},\ 0 \le x_i < 1\}$$

cover the entire space V_0. We may therefore write

$$\gamma_i = \mu_i + \gamma_{0i}, \quad \mu_i \in \Phi_0, \quad \gamma_{0i} \in \Gamma_0 \subseteq V_0.$$

As the $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ lie discretely in the bounded set Φ_0, they have to be finite in number. In fact, the intersection of Γ with the closure of Φ_0 is compact and discrete, hence finite.

Putting now $q = (\Gamma : \Gamma_0)$, we have $q\Gamma \subseteq \Gamma_0$, whence

$$\Gamma \subseteq \tfrac{1}{q}\Gamma_0 = \mathbb{Z}\left(\tfrac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\tfrac{1}{q}u_m\right).$$

By the main theorem on finitely generated abelian groups, Γ therefore admits a $\mathbb{Z}$-basis $v_1, \dots, v_r$, $r \le m$, i.e., $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r$. The vectors $v_1, \dots, v_r$ are also $\mathbb{R}$-linearly independent because they span the m-dimensional space V_0. This shows that Γ is a lattice. □

Next we prove a criterion which will tell us when a lattice in the space V – given, say, as a discrete subgroup $\Gamma \subseteq V$ – is complete.

(4.3) Lemma. *A lattice Γ in V is complete if and only if there exists a bounded subset $M \subseteq V$ such that the collection of all translates $M + \gamma$, $\gamma \in \Gamma$, covers the entire space V.*

Proof: If $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ is complete, then one may take M to be the fundamental mesh $\Phi = \{x_1v_1 + \cdots + x_nv_n \mid 0 \le x_i < 1\}$.

Conversely, let M be a bounded subset of V whose translates $M + \gamma$, for $\gamma \in \Gamma$, cover V. Let V_0 be the subspace spanned by Γ. We have to show that $V = V_0$. So let $v \in V$. Since $V = \bigcup_{\gamma\in\Gamma}(M + \gamma)$ we may write, for each $\nu \in \mathbb{N}$,

$$\nu v = a_\nu + \gamma_\nu, \quad a_\nu \in M, \quad \gamma_\nu \in \Gamma \subseteq V_0.$$

Since M is bounded, $\frac{1}{\nu}a_\nu$ converges to zero, and since V_0 is closed,

$$v = \lim_{\nu\to\infty} \tfrac{1}{\nu}a_\nu + \lim_{\nu\to\infty} \tfrac{1}{\nu}\gamma_\nu = \lim_{\nu\to\infty} \tfrac{1}{\nu}\gamma_\nu \in V_0. \qquad \square$$

Now let V be a *euclidean* vector space, i.e., an $\mathbb{R}$-vector space of finite dimension n equipped with a symmetric, positive definite bilinear form

$$\langle\ ,\ \rangle : V \times V \to \mathbb{R}.$$

Then we have on V a notion of volume — more precisely a Haar measure. The cube spanned by an orthonormal basis $e_1, \dots, e_n$ has volume 1, and more generally, the parallelepiped spanned by n linearly independent vectors $v_1, \dots, v_n$,

$$\Phi = \{x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R},\ 0 \le x_i < 1\}$$

has volume

$$\operatorname{vol}(\Phi) = |\det A|,$$

where $A = (a_{ik})$ is the matrix of the base change from $e_1, \dots, e_n$ to $v_1, \dots, v_n$, so that $v_i = \sum_k a_{ik}e_k$. Since

$$(\langle v_i, v_j\rangle) = \Big(\sum_k a_{ik}a_{jk}\Big) = AA^t,$$

we also have the invariant notation

$$\operatorname{vol}(\Phi) = |\det(\langle v_i, v_j\rangle)|^{1/2}.$$

Let Γ be the lattice spanned by $v_1, \dots, v_n$. Then Φ is a fundamental mesh of Γ, and we write for short

$$\operatorname{vol}(\Gamma) = \operatorname{vol}(\Phi).$$

This does not depend on the choice of a basis $v_1, \dots, v_n$ of the lattice because the transition matrix passing to a different basis, as well as its inverse, has integer coefficients, and therefore has determinant ± 1 so that the set Φ is transformed into a set of the same volume.

We now come to the most important theorem about lattices. A subset X of V is called *centrally symmetric*, if, given any point $x \in X$, the point $-x$ also belongs to X. It is called *convex* if, given any two points $x, y \in X$, the whole line-segment $\{ty + (1-t)x \mid 0 \le t \le 1\}$ joining x with y is contained in X. With these definitions we have

(4.4) Minkowski's Lattice Point Theorem. Let r *be* a complcre *lattice in tlie euclidean vector* space *V and X* a *centrally* symmetric, *convex subset ofV. Suppose tliat*

$$\mathrm{vol}(X) > zn\ \mathrm{vol}(I').$$

Then *X contaim at* /ea.<;t one *nonzero lartice pointy* $\in I'$.

Proof: It is enough to show that there exist two distinct lattice points YI, $Y2 \in I'$ such that

$$\left(\tfrac{1}{2}X + \gamma_1\right) \cap \left(\tfrac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

In fact, choosing a point in this intersection,

$$ix1+Y1 = \qquad + \gamma_2, \quad x_1, x_2 \in X,$$

we obtain an element

$$y=y1-Y2=$$

which is the center of the line segment joining x_2 and $-x_1$, and therefore belongs to X n r.

Now, if the sets ½ $X + y$, $y \in I'$, were pairwise disjoint, then the same would be true of their intersections <Pn(½X+y) with a fundamental mesh <P of I', i.e., we would have

$$\mathrm{vol}(<t>)\ e> \sum_{yeCJ'} \mathrm{vol}(<t> \cap (\tfrac{1}{2}X + y)).$$

But translation of <P n (½X + y) by $-y$ creates the set (<P - y) n ½X of equal volume, and the <P - y, $y \in I'$, cover the entire space V, therefore also the set ½ X. Consequently we would obtain

$$\mathrm{vol}(<P)\ � \sum_{,er} \mathrm{vol}((<P - y) \cap 1X) = \mathrm{vol}(�X) = � \ \mathrm{vol}(X),$$

which contradicts the hypothesis. □

Exercise I. Show that a lattice I' in IR" is rnmp!ctc if and only if the quotient IR"/I' 1s compact.

Exercise 2. Show that Minkowski's la1tice point theorem cannot he improved, by giving an example or a centrally symmetric convex set X s;; V such that vol{X) = 2" vol(I') which docs not contain any nonzero point of the lattice r. lf X is compact, however, then the �tatement (4.4) docs remain true in the case of equality.

Exercise 3 (Minkowski's Theorem on Linear Forms). Let

$$L;(X1, \quad x,,) = \quad i= \; 1,$$

be real linear forms such that *det(a,;) c;i* 0. and let c1, , .. , *c*,, be positive real numbers such that $c_1 \cdots c,, >$ I det(a;J)I. Show that there exist integers $m_1 \ldots$, *mn* E Z such that

$$IL1(m1, \ldots 111")1 < c,, \quad i = 1,$$

Hil\t: Use Mlnkuwski's lallice point lf1eorcm.

§ 5. Minkowski Theory

The basic idea in Minkowski 's treatment of an algebraic numher lidd *K* IQ of degree *n* is to interpret its numbers as points inn-dimensional space. This explains why his theory has been called "Geometry of Numbers." It seems appropric1tc, however, to follow the current trend ;md call it "Minkowski Theory" instead, because in the meantime a geometric approach to number theory has been developed which is quite different in nature and much more comprehensive. We will explain this in § 13. In the present section, we consider the canonical mapping

$$j:K \text{-------+} K�:=TTC, \quad af \text{-----};oja=(ra),$$

which results from the *n* complex embeddings r : *K* ---+ C. The C-vector space *Kc* is equipped with the *hamitian scalar product*

$$\langle x, y \rangle = \sum x_\tau \bar{y}_\tau .$$

Let us recall that a hennitian scalar product is given by a form *JI (x,* y) which is linear in the first variable and satisfies *H(x,v)* = *H(y,x)* as well as *H(x,x)* > 0 for*x -f-* 0. In the sequel we always view *KL* as a hermitian space, with respect to the "standard metric" (*)-

The Galois group *G(C/IR)* is generated by complex conjugation

$$F: \; z \; f\text{-----+} \; Z.$$

The notation *F* will be justified only later (see ch,1p. III. *4). *F* acts Oh the one hand on the factors of the product TTr C, but on the other hand it also acts on the indexing set of r's: to each embedding r: *K-.* C corresponds its complex conjugate f: *K* --+ C. Allogether, this defines an involution

$$f: \; Kc\text{------+} \; Kc$$

which, on the points $z = (z_\tau) \in K_{\mathbb{C}}$, is given by

The scalar product $\langle\ ,\ \rangle$ is equivariant under F, that is

$$\langle Fx, Fy\rangle = F\langle x,y\rangle.$$

Finally, we have on the $\mathbb{C}$-vector space $K_{\mathbb{C}} = \prod_\tau \mathbb{C}$ the linear map

$$Tr: K_{\mathbb{C}} \longrightarrow \mathbb{C},$$

given as the sum of the coordinates. It is also F-invariant. The composite

$$K \xrightarrow{j} K_{\mathbb{C}} \to \mathbb{C}$$

gives the usual trace of $K|\mathbb{Q}$ (see (2.6), (ii)),

$$Tr_{K|\mathbb{Q}}(a) = Tr(ja).$$

We now concentrate on the $\mathbb{R}$-vector space

$$K_{\mathbb{R}} = K_{\mathbb{C}}^{+} = \Big[\prod_\tau \mathbb{C}\Big]^{+}$$

consisting of the $G(\mathbb{C}|\mathbb{R})$-invariant, i.e., F-invariant, points of $K_{\mathbb{C}}$. These are the points (z_τ) such that $\bar{z}_\tau = z_{\bar\tau}$. An explicit description of $K_{\mathbb{R}}$ will be given anon. Since $\overline{\tau a} = \bar\tau a$ for $a \in K$, one has $F(ja) = ja$. This yields a mapping

$$j: K \longrightarrow K_{\mathbb{R}}.$$

The restriction of the hermitian scalar product $\langle\ ,\ \rangle$ from $K_{\mathbb{C}}$ to $K_{\mathbb{R}}$ gives a scalar product

$$\langle\ ,\ \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \longrightarrow \mathbb{R}$$

on the $\mathbb{R}$-vector space $K_{\mathbb{R}}$. Indeed, for $x,y \in K_{\mathbb{R}}$, one has $\langle x,y\rangle \in \mathbb{R}$, in view of the relations $\overline{\langle x,y\rangle} = \langle Fx,Fy\rangle = \langle x,y\rangle$, $\langle x,y\rangle = \overline{\langle y,x\rangle} = \langle y,x\rangle$, and, in any case, $\langle x,x\rangle > 0$ for $x \neq 0$.

We call the *euclidean* vector space

$$K_{\mathbb{R}} = \Big[\prod_\tau \mathbb{C}\Big]^{+}$$

the **Minkowski space**, its scalar product $\langle\ ,\ \rangle$ the **canonical metric**, and the associated Haar measure (see §4, p. 26) the **canonical measure**. Since $Tr \circ F = F \circ Tr$ we have on $K_{\mathbb{R}}$ the $\mathbb{R}$-linear map

$$Tr: K_{\mathbb{R}} \longrightarrow \mathbb{R},$$

and its composite with $j : K \to K_{\mathbb{R}}$ is again the usual trace of $K|\mathbb{Q}$,

$$Tr_{K|\mathbb{Q}}(a) = Tr(ja).$$

Remark: We mention in passing – it will not be used in the sequel – that the mapping $j : K \to K_{\mathbb{R}}$ identifies the vector space $K_{\mathbb{R}}$ with the tensor product $K \otimes_{\mathbb{Q}} \mathbb{R}$,

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}}, \quad a \otimes x \mapsto (ja)x.$$

Likewise, $K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} K_{\mathbb{C}}$. In this approach, the inclusion $K_{\mathbb{R}} \subseteq K_{\mathbb{C}}$ corresponds to the canonical mapping $K \otimes_{\mathbb{Q}} \mathbb{R} \to K \otimes_{\mathbb{Q}} \mathbb{C}$ which is induced by the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$. F corresponds to $F(a \otimes z) = a \otimes \bar{z}$.

An explicit description of the Minkowski space $K_{\mathbb{R}}$ can be given in the following manner. Some of the embeddings $\tau : K \to \mathbb{C}$ are real in that they land already in $\mathbb{R}$, and others are complex, i.e., not real. Let

$$\rho_1, \dots, \rho_r : K \to \mathbb{R}$$

be the real embeddings. The complex ones come in pairs

$$\sigma_1, \bar{\sigma}_1, \dots, \sigma_s, \bar{\sigma}_s : K \longrightarrow \mathbb{C}$$

of complex conjugate embeddings. Thus $n = r + 2s$. We choose from each pair some fixed complex embedding, and let ρ vary over the family of real embeddings and σ over the family of chosen complex embeddings. Since F leaves the ρ invariant, but exchanges the $\sigma, \bar{\sigma}$, we have

$$K_{\mathbb{R}} = \Big\{ (z_\tau) \in \prod_\tau \mathbb{C} \;\Big|\; z_\rho \in \mathbb{R},\ z_{\bar{\sigma}} = \bar{z}_\sigma \Big\}$$

This gives the

(5.1) Proposition. *There is an isomorphism*

$$f : K_{\mathbb{R}} \xrightarrow{\sim} \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s}$$

given by the rule $(z_\tau) \mapsto (x_\tau)$ *where*

$$x_\rho = z_\rho, \quad x_\sigma = \mathrm{Re}(z_\sigma), \quad x_{\bar{\sigma}} = \mathrm{Im}(z_\sigma).$$

This isomorphism transforms the canonical metric $\langle\ ,\ \rangle$ *into the scalar product*

$$(x, y) = \sum_\tau \alpha_\tau x_\tau y_\tau,$$

where $\alpha_\tau = 1$, *resp.* $\alpha_\tau = 2$, *if* τ *is real, resp. complex.*

Proof: The mapping is clearly an isomorphism. If $z = (z_\tau) = (x_\tau + iy_\tau) \in K_\mathbb{R}$, then $z_{\bar\tau} = x_\tau - iy_\tau$, and in view of $x_{\bar\tau} = x_\tau$ and $y_{\bar\tau} = -y_\tau$, one gets

$$z_\tau \bar z'_\tau + z_{\bar\tau} \bar z'_{\bar\tau} = z_\tau \bar z'_\tau + \overline{z_\tau \bar z'_\tau} = 2\,\mathrm{Re}(z_\tau \bar z'_\tau) = 2(x_\tau x'_\tau + y_\tau y'_\tau).$$

This proves the claim concerning the scalar products. □

The scalar product $(x,y) = \sum_\tau \alpha_\tau x_\tau y_\tau$ transfers the canonical measure from $K_\mathbb{R}$ to $\mathbb{R}^{r+2s}$. It obviously differs from the standard Lebesgue measure by

$$\mathrm{vol}_{\mathrm{canonical}}(X) = 2^s\, \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)).$$

Minkowski himself worked with the Lebesgue measure on $\mathbb{R}^{r+2s}$, and most textbooks follow suit. The corresponding measure on $K_\mathbb{R}$ is the one determined by the scalar product

$$(x,y) = \sum_\tau \frac{1}{\alpha_\tau} x_\tau y_\tau .$$

This scalar product may therefore be called the Minkowski metric on $K_\mathbb{R}$. But we will systematically work with the canonical metric, and denote by vol the corresponding canonical measure.

The mapping $j : K \to K_\mathbb{R}$ gives us the following lattices in Minkowski space $K_\mathbb{R}$.

(5.2) Proposition. *If $\mathfrak{a} \neq 0$ is an ideal of $\mathcal{O}_K$, then $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_\mathbb{R}$. Its fundamental mesh has volume*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}).$$

Proof: Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$, so that $\Gamma = \mathbb{Z}j\alpha_1 + \dots + \mathbb{Z}j\alpha_n$. We choose a numbering of the embeddings $\tau : K \to \mathbb{C}$, $\tau_1, \dots, \tau_n$ and form the matrix $A = (\tau_l \alpha_i)$. Then, according to (2.12), we have

$$d(\mathfrak{a}) = d(\alpha_1, \dots, \alpha_n) = (\det A)^2 = (\mathcal{O}_K : \mathfrak{a})^2\, d(\mathcal{O}_K) = (\mathcal{O}_K : \mathfrak{a})^2\, d_K,$$

and on the other hand

$$(j\alpha_i, j\alpha_k) = \Big(\sum_{l=1}^n \tau_l\alpha_i\, \bar\tau_l\alpha_k\Big) = A\bar A^t .$$

This indeed yields

$$\mathrm{vol}(\Gamma) = |\det((j\alpha_i, j\alpha_k))|^{1/2} = |\det A| = \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}). \qquad \square$$

Using this proposition, Minkowski's lattice point theorem now gives the following result, which is what we chiefly intend to use in our applications to number theory.

(5.3) Theorem. *Let $\mathfrak{a} \neq 0$ be an integral ideal of K, and let $c_\tau > 0$, for $\tau \in \operatorname{Hom}(K, \mathbb{C})$, be real numbers such that $c_\tau = c_{\bar\tau}$ and*

$$\prod_\tau c_\tau > A\,(\mathcal{O}_K : \mathfrak{a}),$$

where $A = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Then there exists $a \in \mathfrak{a}$, $a \neq 0$, such that

$$|\tau a| < c_\tau \quad \text{for all } \tau \in \operatorname{Hom}(K, \mathbb{C}).$$

Proof: The set $X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$ is centrally symmetric and convex. Its volume $\operatorname{vol}(X)$ can be computed via the map (5.1)

$$f: K_{\mathbb{R}} \to \prod_\tau \mathbb{R}, \quad (z_\tau) \mapsto (x_\tau),$$

given by $x_\rho = z_\rho$, $x_\sigma = \operatorname{Re}(z_\sigma)$, $x_{\bar\sigma} = \operatorname{Im}(z_\sigma)$. It comes out to be 2^s times the Lebesgue-volume of the image

$$f(X) = \Big\{(x_\tau) \in \prod_\tau \mathbb{R} \;\Big|\; |x_\rho| < c_\rho,\; x_\sigma^2 + x_{\bar\sigma}^2 < c_\sigma^2\Big\}.$$

This gives

$$\operatorname{vol}(X) = 2^s \operatorname{vol}_{\text{Lebesgue}}(f(X)) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_\tau c_\tau.$$

Now using (5.2), we obtain

$$\operatorname{vol}(X) > 2^{r+s}\pi^s \left(\tfrac{2}{\pi}\right)^s \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}) = 2^n \operatorname{vol}(\Gamma).$$

Thus the hypothesis of Minkowski's lattice point theorem is satisfied. So there does indeed exist a lattice point $ja \in X$, $a \neq 0$, $a \in \mathfrak{a}$; in other words $|\tau a| < c_\tau$. □

There is also a multiplicative version of Minkowski theory. It is based on the homomorphism

$$j: K^* \to K_{\mathbb{C}}^* = \prod_\tau \mathbb{C}^*.$$

The multiplicative group $K_{\mathbb{C}}^*$ admits the homomorphism

$$N: K_{\mathbb{C}}^* \to \mathbb{C}^*$$

given by the product of the coordinates. The composite

$$K^* \xrightarrow{j} K_{\mathbb{C}}^* \xrightarrow{N} \mathbb{C}^*$$

is the usual norm of $K|\mathbb{Q}$,

$$N_{K|\mathbb{Q}}(a) = N(ja).$$

In order to produce a lattice from the multiplicative theory, we use the logarithm to pass from multiplicative to additive groups

$$\ell : \mathbb{C}^* \to \mathbb{R}, \quad z \mapsto \log|z|.$$

It induces a surjective homomorphism

$$\ell : K_{\mathbb{C}}^* \to \prod_\tau \mathbb{R},$$

and we obtain the commutative diagram

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{\ell} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow{\ell} & \mathbb{R}. \end{array}$$

The involution $F \in G(\mathbb{C}|\mathbb{R})$ acts on all groups in this diagram, trivially on K^*, on $K_{\mathbb{C}}$ as before, and on the points $x = (x_\tau) \in \prod_\tau \mathbb{R}$ by $(Fx)_\tau = x_{\bar\tau}$. One clearly has

$$F \circ j = j, \quad F \circ \ell = \ell \circ F, \quad N \circ F = F \circ N, \quad Tr \circ F = Tr,$$

i.e., the homomorphisms of the diagram are $G(\mathbb{C}|\mathbb{R})$-homomorphisms. We now pass everywhere to the fixed modules under $G(\mathbb{C}|\mathbb{R})$ and obtain the diagram

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{\ell} & [\prod_\tau \mathbb{R}]^+ \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{\ell} & \mathbb{R}. \end{array}$$

The $\mathbb{R}$-vector space $[\prod_\tau \mathbb{R}]^+$ is explicitly given as follows. Separate as before the embeddings $\tau : K \to \mathbb{C}$ into real ones, $\rho_1, \dots, \rho_r$, and pairs of complex conjugate ones, $\sigma_1, \bar\sigma_1, \dots, \sigma_s, \bar\sigma_s$. We obtain a decomposition which is analogous to the one we saw above for $[\prod_\tau \mathbb{C}]^+$,

$$[\prod_\tau \mathbb{R}]^+ = \prod_\rho \mathbb{R} \times \prod_\sigma [\mathbb{R} \times \mathbb{R}]^+.$$

The factor $[\mathbb{R} \times \mathbb{R}]^+$ now consists of the points (x,x), and we identify it with $\mathbb{R}$ by the map $(x,x) \mapsto 2x$. In this way we obtain an isomorphism

$$[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}.$$

which again transforms the map $Tr: [\prod_\tau \mathbb{R}]^+ \to \mathbb{R}$ into the usual map

$$Tr: \mathbb{R}^{r+s} \longrightarrow \mathbb{R}$$

given by the sum of the coordinates. Identifying $[\prod_\tau \mathbb{R}]^+$ with $\mathbb{R}^{r+s}$, the homomorphism

$$\ell : K_{\mathbb{R}}^* \longrightarrow \mathbb{R}^{r+s}$$

is given by

$$\ell(x) = (\log|x_{\rho_1}|, \dots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \dots, \log|x_{\sigma_s}|^2),$$

where we write $x \in K_{\mathbb{R}}^* \subseteq \prod_\tau \mathbb{C}^*$ as $x = (x_\tau)$.

Exercise 1. Write down a constant A which depends only on K such that every integral ideal $\mathfrak{a} \neq 0$ of K contains an element $a \neq 0$ satisfying

$$|\tau a| \le A(\mathcal{O}:\mathfrak{a})^{1/n} \quad \text{for all } \tau \in \operatorname{Hom}(K, \mathbb{C}),\ n = [K:\mathbb{Q}].$$

Exercise 2. Show that the convex, centrally symmetric set

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid \sum_\tau |z_\tau| < t\}$$

has volume $\operatorname{vol}(X) = 2^r \pi^s \frac{t^n}{n!}$ (see chap. III, (2.15)).

Exercise 3. Show that in every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists an $a \neq 0$ such that

$$|N_{K|\mathbb{Q}}(a)| \le M(\mathcal{O}_K:\mathfrak{a}),$$

where $M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ (the so-called Minkowski bound).

Hint: Use exercise 2 to proceed as in (5.3), and make use of the inequality between arithmetic and geometric means,

$$\frac{1}{n} \sum_\tau |z_\tau| \ge \Big(\prod_\tau |z_\tau|\Big)^{1/n}.$$

§ 6. The Class Number

As a first application of Minkowski theory, we are going to show that the ideal class group $Cl_K = J_K/P_K$ of an algebraic number field K is finite. In order to count the ideals $\mathfrak{a} \neq 0$ of the ring $\mathcal{O}_K$ we consider their absolute norm

$$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}:\mathfrak{a}).$$

(Throughout this book the case of the zero ideal $\mathfrak{a} = 0$ is often tacitly excluded, when its consideration would visibly make no sense.) This index is finite by (2.12), and the name is justified by the special case of a principal ideal (a) of $\mathcal{O}_K$, where we have the identity

$$\mathfrak{N}((a)) = |N_{K|\mathbb{Q}}(a)|.$$

Indeed, if $\omega_1, \dots, \omega_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, then $a\omega_1, \dots, a\omega_n$ is a $\mathbb{Z}$-basis of $(a) = a\mathcal{O}_K$, and if $A = (a_{ij})$ denotes the transition matrix, $a\omega_i = \sum a_{ij}\omega_j$, then, as was pointed out already in §2, one has $|\det(A)| = (\mathcal{O}_K : (a))$ as well as $\det(A) = N_{K|\mathbb{Q}}(a)$ by definition.

(6.1) Proposition. *If $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ is the prime factorization of an ideal $\mathfrak{a} \neq 0$, then one has*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}.$$

Proof: By the Chinese remainder theorem (3.6), one has

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}.$$

We are thus reduced to considering the case where $\mathfrak{a}$ is a prime power $\mathfrak{p}^\nu$. In the chain

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$$

one has $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ because of the unique prime factorization, and each quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is an $\mathcal{O}_K/\mathfrak{p}$-vector space of dimension 1. In fact, if $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ and $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$, then $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$ and consequently $\mathfrak{p}^i = \mathfrak{b}$, because otherwise $\mathfrak{b}\mathfrak{p}^{-i}$ would be a proper divisor of $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$. Thus $\bar{a} = a \bmod \mathfrak{p}^{i+1}$ is a basis of the $\mathcal{O}_K/\mathfrak{p}$-vector space $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. So we have $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}$ and therefore

$$\mathfrak{N}(\mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \cdots (\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu) = \mathfrak{N}(\mathfrak{p})^\nu. \qquad \square$$

The proposition immediately implies the multiplicativity

$$\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$$

of the absolute norm. It may therefore be extended to a homomorphism

$$\mathfrak{N} : J_K \longrightarrow \mathbb{R}_+^*$$

defined on all fractional ideals $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$, $\nu_\mathfrak{p} \in \mathbb{Z}$. The following lemma, a consequence of (5.3), is crucial for the finiteness of the ideal class group.

(6.2) Lemma. *In every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists an $a \in \mathfrak{a}$, $a \neq 0$, such that*

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, \mathfrak{N}(\mathfrak{a}).$$

Proof: Given $\varepsilon > 0$, we choose positive real numbers c_τ, for $\tau \in Hom(K,\mathbb{C})$, such that $c_\tau = c_{\bar\tau}$ and

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Then by (5.3) we find an element $a \in \mathfrak{a}$, $a \neq 0$, satisfying $|\tau a| < c_\tau$. Thus

$$|N_{K|\mathbb{Q}}(a)| = \prod_\tau |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

This being true for all $\varepsilon > 0$ and since $|N_{K|\mathbb{Q}}(a)|$ is always a positive integer, there has to exist an $a \in \mathfrak{a}$, $a \neq 0$, such

$$\left|N_{K|\mathbb{Q}}(a)\right| \le \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}). \qquad \square$$

(6.3) Theorem. *The ideal class group $Cl_K = J_K/P_K$ is finite. Its order*

$$h_K = (J_K : P_K)$$

is called the **class number** *of K.*

Proof: If $\mathfrak{p} \neq 0$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ of degree, say, $f \ge 1$, and we have

$$\mathfrak{N}(\mathfrak{p}) = p^f.$$

Given p, there are only finitely many prime ideals $\mathfrak{p}$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, because this means that $\mathfrak{p} \mid (p)$. It follows that there are only finitely many prime ideals $\mathfrak{p}$ of bounded absolute norm. Since every integral ideal admits a representation $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ where $\nu_i > 0$ and

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r},$$

there are altogether only a finite number of ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with bounded absolute norm $\mathfrak{N}(\mathfrak{a}) \le M$.

It therefore suffices to show that each class $[\mathfrak{a}] \in Cl_K$ contains an integral ideal $\mathfrak{a}_1$ satisfying

$$\mathfrak{N}(\mathfrak{a}_1) \le M = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

For this, choose an arbitrary representative $\mathfrak{a}$ of the class, and a $\gamma \in \mathcal{O}_K$, $\gamma \neq 0$, such that $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. By (6.2), there exists $\alpha \in \mathfrak{b}$, $\alpha \neq 0$, such that

$$|N_{K|\mathbb{Q}}(\alpha)| \cdot \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}((\alpha)\mathfrak{b}^{-1}) = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \le M.$$

The ideal $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ therefore has the required property. $\square$

The theorem of the finiteness of the class number h_K means that passing from numbers to ideals has not thrust us into unlimited new territory. The most favourable case occurs of course when $h_K = 1$. This means that $\mathcal{O}_K$ is a principal ideal domain, i.e., that prime factorization of elements in the classical sense holds. In general, however, one has $h_K > 1$. For instance, we know now that the only imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$, d squarefree and < 0, which have class number 1 are those with

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Among real quadratic fields, class number 1 is more common. In the range $2 \le d < 100$ for instance, it occurs for

$$\begin{aligned} d = {} & 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, \\ & 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, \\ & 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97. \end{aligned}$$

It is conjectured that there are infinitely many real quadratic fields of class number 1. But we do not even yet know whether there are infinitely many algebraic number fields (of arbitrary degree) with class number 1. It was found time and again in innumerable investigations that the ideal class groups Cl_K behave completely unpredictably, both in their size and their structure. An exception to this lack of rule is KENKICHI IWASAWA's discovery that the *p-part* of the class number of the field of p^n-th roots of unity obeys a very strict law when n varies (see [136], th. 13.13).

In the case of the field of p-th roots of unity, the question whether the class number is divisible by p has played a very important special rôle because it is intimately linked to the celebrated Fermat's Last Theorem according to which the equation

$$x^p + y^p = z^p$$

for $p \ge 3$ has no solutions in integers $\ne 0$. In a similar way as the sums of two squares $x^2 + y^2 = (x+iy)(x-iy)$ lead to studying the gaussian integers, the decomposition of $x^p + y^p$ by means of a p-th root of unity $\zeta \ne 1$ leads to a problem in the ring $\mathbb{Z}[\zeta]$ of integers of $\mathbb{Q}(\zeta)$. The equation $y^p = z^p - x^p$ there turns into the identity

$$y \cdot y \cdots y = (z-x)(z-\zeta x) \cdots (z-\zeta^{p-1}x).$$

Thus, assuming the existence of a solution, one obtains two multiplicative decompositions of the same number in $\mathbb{Z}[\zeta]$. One can show that this contradicts the unique factorization – provided that this holds in the ring $\mathbb{Z}[\zeta]$. Supposing erroneously that this was the case in general – in other words that the class number h_p of the field $\mathbb{Q}(\zeta)$ were always equal

10 I - some aclually 1hough11hey had proved "Fenna1's Last Theorem" in 1his way. *Kw'1Mt:H,* however, did not fall into this lrap. Instead, he proved that the arguments we have indicated can be salvaged if one only assumes *pf hp* instead of $hp = 1$. In this case he called a prime number p regular. otherwise irregular. He even showed that p is regular if and only if the numerators of the Bernoulli numbers B_2, H4, . , B_{p-3}, are not divisible by p. Among the first 25 prime numbers < 100 only three are irregular: 37, 59, and 67. We still do not know today whether there are infinitely many regular prime numbers.

The connection with Fcnnal's lasl theorem has al last become obsolete. Following a surprising discovery by the mathemaiician *GtkH,\RO FR£Y,* who established a link with the 1heory of *elliptic rnrves,* it was *KMYNl-."IHRIBET,* who munagcd to reduce Fermat's statement to another. much more important conjei.:ture, the Taniyama-Shimura-Weil Conjecture. This was proved in sufficient generality in 1994 by *ANl)R/..W Wu.r.-s,* after many years of work, and with a helping hand from *R1c11.-.RD T�rUJR.* See (144].

TI1e regular and irregular prime numhers do however cominuc to be important.

Exercise I. How many intt:gral ideals a are there with the given norm 'Jl(a) = n'!

Eurrlsc 2. Show that the quadratk fields with discriminant 5. 8, 11, - 3, - 4. -7, -8, - 11 have class number I.

Exercise 3. Show that in every ideal class of an algebraic number field K of degree n, there exists an integrnl ideal a such th111

$$\mathfrak{N}(\mathfrak{a}) \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}\,.$$

Hint: Using exercise: 3. §5. proceed a.�in the proof of (6.3).

Ext!rdst! 4. Show that the absulull.; ,..<1\u<:: ol" the discriminant ldK I is > 1 for c,..ery algebraic number field K "/- Q (Minkow�ki's theorem on the discriminant. see chap. Ill. (2.17)).

Exercise 5. Show that the abwlu1c value of the tiiscriminant $/dK$I tends to oo with 1he degree II of the field.

Exercise 6. Let a be an imegral ideal of K ;md a"'= \a). Show 1ha1 a hecomcs a principal ideal in lhe field $\bar{E}$ K (":/ii). in lhe sense 1h:u a_O,. = (a).

Exercise 7. Show that, for every number field K. there exisf� a finite extension L such that every ideal of K bcrnmcs u principal ideal.

§ 7. Dirichlet's Unit Theorem

After considering the ideal class group Cl_K, we now turn to the second main problem posed by the ring $\mathcal{O}_K$ of integers of an algebraic number field K, the group of units $\mathcal{O}_K^*$. It comains the finite group $\mu(K)$ of the roots of unity that lie in K, but in generaJ is not itself finite. Its size is in fact determined by the number r of real embeddings $\rho : K \to \mathbb{R}$ and the numbers of pairs $\sigma, \bar\sigma : K \to \mathbb{C}$ of complex conjugate embeddings. In order to describe the group, we use the diagram which was set up in §5:

$$\begin{array}{ccccc} K^* & \longrightarrow & K_{\mathbb{R}}^* & \longrightarrow & [\prod \mathbb{R}]^+ \\ & & \Big\downarrow N & & \Big\downarrow Tr \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \longrightarrow & \mathbb{R} \end{array}$$

In the upper part of the diagram we consider the subgroups

$\mathcal{O}_K^* = \{ \varepsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\varepsilon) = \pm 1 \}$, the group of units,

$S = \{ y \in K_{\mathbb{R}}^* \mid N(y) = \pm 1 \}$, the "nonn-onc surface",

$H = \{ x \in [\prod \mathbb{R}]^+ \mid Tr(x) = 0 \}$, the "trace-zero hyperplane".

We obtain the homomorphisms

$$\mathcal{O}_K^* \xrightarrow{j} S \xrightarrow{\ell} H$$

and the composite $\lambda := \ell \circ j : \mathcal{O}_K^* \to H$. The image will be denoted by

$$\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H,$$

and we obtain the

(7.1) Proposition. *The* sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

1s exact.

Proof: We have to show that $\mu(K)$ is the kernel of λ. Fort; $\zeta \in \mu(K)$ and $\tau : K \to \mathbb{C}$ any embedding, we find $\log |\tau\zeta| = \log 1 = 0$, so that certainly $\mu(K) \subseteq \ker(\lambda)$. Conversely, let $\varepsilon \in \mathcal{O}_K^*$ be an element in the kernel, so that $\lambda(\varepsilon) = \ell(j\varepsilon) = 0$. This means that $|\tau\varepsilon| = 1$ for each embedding r K --+ C, so that }t.' = (re) lies in a bounded domain of the IR-vector space KP., On the other hand. j£ is a point of the lattice joK of K3. (see (5.2)). Therefore the kernel of A can contain only a finite number of elements, and thus, being a finite group, contains only roots of unity in K^*.

□

Given this proposition, it remains to determine the group I'. For this, we need the following

(7.2) **Lemma.** *Up to multiplication by units there a.re only finitely many elements a* E OK *of given norm* N Ki-::;,(a) = *a*.

Proof: Let *a* E Z, *a* > I. In every one of the finitely many cosets of DK /aoK there exists, up to muhiplication by units. al most one element a such that IN(a)I = INK11J(a)I =*a*. For if *fi* =*a*+*ay*. *y* E OK, is another one, then

/3 = 1 ± N(fi) a fi-y E OK

because *N(/J)//3* E *CJK,* and by the same token =I± N:a)YE ɒK, i.e., fJ is associated to a. Therefore, up to multiplication by units, there arcatmost(oK :aoK)elementsofnorm±a. D

(7.3) **Theorem.** *The* group r *is* a *complete lattice in* the *(r + s -* !)-*dimensional vector* space *H,* and *is* therefore *isomorphic to* Z/ 1.·.-1.

Proof: We first show that r = is a lattice in H, i.e., a discrete subgroup. The mapping A : oK --+ II by restricting the mapping

$$K^* \xrightarrow{j} \prod \mathbb{C}^* \xrightarrow{\ell} \prod \mathbb{R},$$

and it suf!lces to show that, for any *c* > 0, the bounded domain {(xr) E f1r Rl lx, I Sc} contains only finitely many points of r = Since C((zr)) = (log lzrl), the preimage of this domain with respect is the bounded domain

$$\Big\{ (z_\tau) \in \prod_\tau \mathbb{C}^* \;\Big|\; e^{-c} \le |z_\tau| \le e^{c} \Big\}.$$

It contains only finitely many clements of the sel JoK because this is a subset of the lattice joK in [f1r CJ+ (see (5.2)). Therefore r is a lattice.

We now show that Γ is a complete lattice in H. This is the principal claim of the theorem. We apply the criterion (4.3). So we have to find a bounded set $M \subseteq H$ such that

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma).$$

We construct this set through its preimage with respect to the surjective homomorphism

$$\ell : S \to H.$$

More precisely, we will construct a bounded set T in the norm-one surface S, the *multiplicative* translations $T\varepsilon$, $\varepsilon \in \mathcal{O}_K^*$, of which cover all of S:

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} T\varepsilon.$$

For $y = (y_\tau) \in T$, it will follow that the absolute values $|y_\tau|$ are bounded from above and also away from zero, because $\prod_\tau |y_\tau| = 1$. Thus $M = \ell(T)$ will also be bounded. We choose real numbers $c_\tau > 0$, for $\tau \in \operatorname{Hom}(K, \mathbb{C})$, satisfying $c_\tau = c_{\bar\tau}$ and

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|},$$

and we consider the set

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}.$$

For an arbitrary point $y = (y_\tau) \in S$, it follows that

$$Xy = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c'_\tau\}$$

where $c'_\tau = c_\tau |y_\tau|$, and one has $c'_{\bar\tau} = c'_\tau$ and $\prod_\tau c'_\tau = \prod_\tau c_\tau = C$ because $\prod_\tau |y_\tau| = |N(y)| = 1$. Then, by (5.3), there is a point

$$a = (\tau a) \in Xy, \quad a \in \mathcal{O}_K, \quad a \neq 0.$$

Now, according to lemma (7.2), we may pick a system $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$, $\alpha_i \neq 0$, in such a way that every $\alpha \in \mathcal{O}_K$ with $0 < |N_{K|\mathbb{Q}}(\alpha)| \leq C$ is associated to one of these numbers. The set

$$T = S \cap \bigcup_{i=1}^{N} X(\tau\alpha_i)^{-1}$$

then has the required property: since X is bounded, so is $X(\tau\alpha_i)^{-1}$ and therefore also T, and we have

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} T\varepsilon.$$

In fact, if $y \in S$, we find by the above an $a \in \mathcal{O}_K$, $a \neq 0$, such that $a \in Xy^{-1}$, so $a = xy^{-1}$ for some $x \in X$. Since

$$|N_{K|\mathbb{Q}}(a)| = |N(xy^{-1})| = |N(x)| < \prod_\tau c_\tau = C,$$

a is associated to some α_i, $\alpha_i = \varepsilon a$, $\varepsilon \in \mathcal{O}_K^*$. Consequently

$$y = xa^{-1} = x\alpha_i^{-1}\varepsilon.$$

Since $y, \varepsilon \in S$, one finds $x\alpha_i^{-1} \in S \cap X\alpha_i^{-1} \subseteq T$, and thus $y \in T\varepsilon$. $\square$

From proposition (7.1) and theorem (7.3) we immediately deduce Dirichlet's unit theorem in its classical form.

(7.4) Theorem. *The group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$ is the direct product of the finite cyclic group $\mu(K)$ and a free abelian group of rank $r + s - 1$.*

In other words: there exist units $\varepsilon_1, \dots, \varepsilon_t$, $t = r + s - 1$, called fundamental units, such that any other unit ε can be written uniquely as a product

$$\varepsilon = \zeta\, \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

with a root of unity ζ and integers ν_i.

Proof: In the exact sequence

$$1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \to 0$$

Γ is a free abelian group of rank $t = r + s - 1$ by (7.3). Let $v_1, \dots, v_t$ be a $\mathbb{Z}$-basis of Γ, let $\varepsilon_1, \dots, \varepsilon_t \in \mathcal{O}_K^*$ be preimages of the v_i, and let $A \subseteq \mathcal{O}_K^*$ be the subgroup generated by the ε_i. Then A is mapped isomorphically onto Γ by λ, i.e., one has $\mu(K) \cap A = 1$ and therefore $\mathcal{O}_K^* = \mu(K) \times A$. $\square$

Identifying $[\prod_\tau \mathbb{R}]^+ = \mathbb{R}^{r+s}$ (see §5, p.33), H becomes a subspace of the euclidean space $\mathbb{R}^{r+s}$ and thus itself a euclidean space. We may therefore speak of the volume of the fundamental mesh $\mathrm{vol}(\lambda(\mathcal{O}_K^*))$ of the unit lattice $\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$ and will now compute it. Let $\varepsilon_1, \dots, \varepsilon_t$, $t = r + s - 1$, be a system of fundamental units and Φ the fundamental mesh of the unit lattice $\lambda(\mathcal{O}_K^*)$, spanned by the vectors $\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t) \in H$. The vector

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \dots, 1) \in \mathbb{R}^{r+s}$$

is obviously orthogonal to H and has length 1. The !-dimensional volume of $Q)$ therefore equals lhe $(t + !)$-dimensional volume of the parallelepiped spanned by Ao, A(ci)...., A(c,) in $RI+^1$. But this has volume

).'" >,(,,)).,(,,))
±det : :
(
Ao1+1 A1+1CE1) A1+1\F1)

Adding all rows to a fixed one, say the i-th row, this row has only zeroes, except for the first emry, which equals $,Jr+s$. We therefore get the

(7.5) Proposition. *The volume* of *the fundamental mesh* of *the unit lat- tice* A(o�) *in H* is

$$\operatorname{vol}\big(\lambda(\mathcal{O}_K^*)\big) = \sqrt{r+s}\,R\,,$$

where R is the absolute \'a/ue of the detenninant oLm *arbitrary* minor of rank $t = r + s -$ I of *the following matrix:*

This absolute value *R is called /he* **regulator** of *the field K.*

The importance of the regulator will only be demonstrated later (see chap. VII, §5).

Exercise **1.** Let $D > 1$ be a s4uarefree integer and d the discriminant of the real 4uadratic number field $K =$ Q(,,/D) §2. exercise 4). Let x_1, y_1 be the uni4uely determined rational integer solution equation

$$x^2 - dy� = -4,$$

or - in case this equation has no rational integer solutions - of the e4uation

$$r^2 - dy^2 = 4.$$

for which $x_1 \cdot y_1 > 0$ are as small as possible. Then

$$\epsilon_1 = \frac{t}{} \pm \frac{/ii}{}$$

is a fundamenhil unit of *K.* (The pair of e4ua1ions $,t" - dy^2 = \pm 4$ is called **Pell's equation.)**

Exercise 2. Check the following tah!e of fundamental unit� t'_1 for Q(,/D):

D						Ill
ε_1	$1+\sqrt{2}$	$2+\sqrt{3}$	$(1+\sqrt{5})/2$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$

Hint: Chtx:k one hy one for y = l, 2, 3, whether one of the numhers tly^1:i::4 is a s4.uare x^2. By 1hc unit 1hcorem this is bound !0 happen, with 1he plus sign. However, for fi,;ed y, let preference be given 10 the minus sign. Then 1hc tir.;1 case, in this order. where dyf ,=. 4 =.(;,gives lhe fundamental unite, = $(x$, + y, Jd)/2.

Exercise 3. The I.fa.Ute of HastinJ(s (Oc1oher 14. 1()66).

"Thi.: men of Harold �tood well together, as their woni was. and fonned thirt..:en s4uares, wi1h a like number of men in every square thereof. and woe to 1hc hardy Norman who ventured to enter their redoubts: for u single blow of u Saxon war-h.itched would break his lance and cut through his coat of mail.. When Haro!d threw himself into the fray the Sa,;ons were one mighty square of men. shouting the battle-cries, ·ut �•. 'Olicros1;e !', 'Godemile ! '," IFic!itious historical text, following e.�...cnlia!ly problem no. 129 *in:* H.E. Dundem:y, *Amusmu'llt.f in Matlu:matio,* !9!7 (Dover rcprinL., 1958 and 1970).)

Question. How many troops doe� this suggest Harold II had a! 1he baUle of Ha�lings?

Exercise 4. Lt:1 (be a primitive p-th of unity, p an odd prime number. Show that Z[i;I• = (OZ(($+C^1$}*. Show =(±$\{^1$(1+()"10st <5,nEZ), if $p=5$.

Exercise S. Le1 (be a primitive m-th root of unity, m �].Show 1hat lhe numbers � for (k,m) = I are units in the ring of integers or the field Q({). Thesubgroup of the grour of uniL'! they generate i,; ca!led the group of cyclotumic units.

Exercise 6. Let K be a totally real number field, i.e., X = Hom(K .C) = Hom(K. R). and lei T be 11 proper noneJ1Jply .,uhscl of X. Then there exis1s a uni,r , $3lisfying 0 <re< I for re T. and H > I for r rf; T.

Hint: Apply Minkowsld.:r.lank:c point theorem to the uni1 l:micc in 1racc-:t.Cro spate.

§8. Extensions of Dedekind Domains

Having studied the ideal class group and the group of units of the ring OK of integers of a number *tlcld K,* we now propose to make a first *survey* of the set of prime ideals of OK. They are oflen referred to a� the prime ideals of K - an imprecise manner of speaking which is, however. not likely to cause any misunderstanding.

Every prime ideal):If- 0 of OK contains a rational prime number p (see §3. *p.* 17) and is therefore a divisor of the ideal $JJOK$. Hence the question arises as to how a prirne number p factors into prime ideals of lhe ring OK. We treat this problem in a more general context, staning from an arbitrary Dedekind domain oar the base instead of Z md taking im:reud of OK the integral closure $\mathcal{O}$ of o in a finite extension of its field of fractions.

(8.1) Proposition. Leto be *a Dedekind* domain *with* field of *fractions K, lei* Ll *K* be a *finite extension* of *K and O tiJe integral clomre* of *o in L. Then0* i.� *again a Dedekind domain.*

Proof: Being the integral closure of o, *O* is integrally closed. The fact that the nonzero prime ideals \l) of *O* are maximal is proved similarly as in the case *o* = Z (see (3.1)): p = \l) n *o* is a nonzero prime ideal of o. Thus the integral domain C'J/� is an extension of the field o/p, and therefore has itself to be a field. because if it were not. then it would admit a nonzero prime ideal whose intersection with o/p would again be a nonzero prime ideal in o/p. It remains to show that *O* is noetherian. In the case that is of chief interest to us, namely. if Ll *K* is a separable extension. the proof is very easy. Let a1, , *o.n* be a basis of Ll *K* contained in *(')*, of discriminant *d* = *d(a1,* *an)*, Then *d* -=I=- 0 by (2.8), and (2.9) tells us that *O* is contained in the linitely generated a-module oa_1/d + • + oa_{11}/d. Every ideal of *O* is also contained in this finitely generated c-module, and therefore is itself an a-module of finite type, hence *a fortiori* a finitely generated C'J-module. This shows that *O* is noetherian, provided Ll *K* is separable. We ask the reader's permission to content ourselves for the time being with this case. We shall come hack to the general case on a more convenient occasion. In fact, we shall give the proof in a more general framework in 9 12 (see (12.8)). □

For a prime ideal p of *o* one always has

pO,<O.

In fact, let Jf E p "- p^2 (p -=I=- 0), so that *no*= pa with pf a, hence p+a = o. Writing 1 = *h* + *s.* with *h* E p and *s* E a, we find *s* ff:. p and sp £ pa = rr o. If one had pO = *0,* then it would follow that *sO* = *spO* <; *rrO,* so that *s* = *.rrx* for some *x* E On *K* = o, i.e., *s* E p, a contradiction.

A prime ideal p -=I=- 0 of the ring *o* decomJXlses in ('J in a unique way into a product of prime ideals,

pO �<µ\' .,µ;, .

Instead of p(') we will often write simply p. The prime ideals 'l]; occurring in the decomposition are precisely those prime ideals ,,P of *O* which lie over p in the sense that one has the relation

p = \l)no.

This we also denote for short by \l) Ip, and we call � a prime divisor of p. The exponent *e;* is called the **ramification index,** and the degree of the field extension

$$f_i = [\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}]$$

is called the inertia degree of $\mathfrak{P}_i$ over $\mathfrak{p}$. If the extension $L|K$ is separable, the numbers e_i, f_i and the degree $n = [L:K]$ are connected by the following law.

(8.2) Proposition. Let $L|K$ be separable. Then we have the *fundamental identity*

$$\sum_{i=1}^{r} e_i f_i = n .$$

Proof: The proof is based on the Chinese remainder theorem

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}.$$

$\mathcal{O}/\mathfrak{p}\mathcal{O}$ and $\mathcal{O}/\mathfrak{P}_i^{e_i}$ are vector spaces over the field $\kappa = \mathfrak{o}/\mathfrak{p}$, and it suffices to show that

$$\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n \quad \text{and} \quad \dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i .$$

In order to prove the first identity, let $\omega_1, \dots, \omega_m \in \mathcal{O}$ be representatives of a basis $\bar\omega_1, \dots, \bar\omega_m$ of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ over κ (we have seen in the proof of (8.1) that $\mathcal{O}$ is a finitely generated $\mathfrak{o}$-module, so certainly $\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) < \infty$). It suffices to show that $\omega_1, \dots, \omega_m$ is a basis of $L|K$. Assume the $\omega_1, \dots, \omega_m$ are linearly dependent over K, and hence also over $\mathfrak{o}$. Then there are elements $a_1, \dots, a_m \in \mathfrak{o}$, not all zero, such that

$$a_1\omega_1 + \cdots + a_m\omega_m = 0 .$$

Consider the ideal $\mathfrak{a} = (a_1, \dots, a_m)$ of $\mathfrak{o}$ and find $a \in \mathfrak{a}^{-1}$ such that $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, hence $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Then the elements $aa_1, \dots, aa_m$ lie in $\mathfrak{o}$, but not all belong to $\mathfrak{p}$. The congruence

$$aa_1\bar\omega_1 + \cdots + aa_m\bar\omega_m \equiv 0 \bmod \mathfrak{p}$$

thus gives us a linear dependence among the $\bar\omega_1, \dots, \bar\omega_m$ over κ, a contradiction. The $\omega_1, \dots, \omega_m$ are therefore linearly independent over K.

In order to show that the ω_i are a basis of $L|K$, we consider the $\mathfrak{o}$-modules $M = \mathfrak{o}\omega_1 + \cdots + \mathfrak{o}\omega_m$ and $N = \mathcal{O}/M$. Since $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, we have $\mathfrak{p}N = N$. As $L|K$ is separable, $\mathcal{O}$, and hence also N, are finitely generated $\mathfrak{o}$-modules (see p. 45). If $\alpha_1, \dots, \alpha_s$ is a system of generators of N, then

$$\alpha_i = \sum_j a_{ij}\alpha_j \quad \text{for } a_{ij} \in \mathfrak{p}.$$

Let A be the matrix $(a_{ij}) - I$, where I is the unit matrix of rank s, and let B be the adjoint matrix of A, whose entries are the minors of rank $(s-1)$

of *A*. Then one has *A(cr1, ...* , a_1f = 0 and *BA= di,* with *d* = det(A). (see (2.3)), Hence

0 = *BA(a* , ... *a.,)' = (dct1, ... da.*

and therefore *dN* = 0, i.e., *dO* ::; *M* = *ocv1* + ··· + *Ow111*. We have *d* -=I= 0, because expanding the determinant *d* = det((a;;) - /) we find *d* = (-l}' mod p because *a11* E p. It follows that *L* = *dL* = *Kw1* + + *Kcvm*. cv1, . , *w111* is therefore indeed a basis of Ll *K*.

In order to prove the second identity, let us consider the descending chain

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

of K-vector spaces. The successive quotients q:3/ ;q:3;1+1 in this chain are isomorphic to O/q:31, for if *a* E q:3)" "- q:3;+1, then the homomorphism

0------+ q:3)'/q:3;'+1, *a* i-----+ *aa*,

has kernel �' and is surjective because �i is the gcd of q:3;·+1 and *(a)= aO* so that q:3/ = *cr:O* + q:3;+1. Since *.f;* = *[0/�;* : K], we obtain dim,;(q:3/ /q:3;'+1) = *,t;-* and therefore

$$\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{\nu=0}^{e_i-1} \dim_\kappa(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = e_i f_i \qquad \square$$

Suppose now that the separable extension Ll *K* is given by a primitive element *O* E *O* with minimal polynomial

p(XJ E o[X].

so that *L* = *K (0)*. We may then deduce a result about the nature of the decomposition of p in *O* which, albeit not complete, does show characteristic phenomena and a striking simplicity. It is incomplete in that a finite number of prime ideals are excluded; only those relatively prime to the **conductor** of the ring of0] can be considered. This conductor is defined to he the biggest ideal J of *O* which is contained in o(O]. In other words

$$\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq \mathcal{o}[\theta]\}.$$

Since *O* is a finitely generated o-module (see proof of (8.1)), one has -8 *-1-* 0.

(8.3) **Proposition.** *Let* p be *a prime ideal* of *o which is relatively prime to* the *conductor:S* ofo[0], and *let*

$$\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r}$$

be rhe *focrorization* ofrhe *pnlynomfol* f,(X) = *p(X)* mod pinto *irreduc:ibles* 'p;(X) = *Pi(X)* mod p overthe *residue* class *fieldo/p, with all p,(X) € o[X] monic. Then*

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}, \quad i = 1, \ldots, r,$$

are rhe different *prime* idea/.s *of O :1bove* p. The *inertia* degree *Ji* of�; i.�*the* degree of"p;(X), *and* one *ha.*�

p = >+n'l"l

Proof: Writing *O'* = oLOJ and *O* = o/p, we have a canonical isomorphism

0/pO ;; O'/pO' ;; o(XJ/(p(X)).

The tirs1 isomorphism follows from lhe relative 11rimali1y pO + 3" = *0.* As � S; *O'*, it follows that *O* = *pO+O'*, i.e., the homomorphism *O'*--,.*0/pO* is surjec1ive. lt has kernel *pO* n *O',* which equals pCJ'. Since (p. �*no)* = I. it follow, that pO n *O'* � (p + ,\')(pO n *0')* � pO'.

The second isomorphism is deduced from the surjective homomorphism

c,(XJ - o[Xi/(p(X))

ilskernel is the ideal generated by p and *p(X),* and in view of *O'* =0(8) = o(Xj/(p(X)), *we*ha,c *O'/pO'* ;; ofXI/(p(X)).

Sim:e "p(X) = n�=I *"ji;(X)"*•, rhe Chinese remainder lheorem linally gives 1hc isomorphism

o[XJ/(iitX)) ;; E!,o[XI/(p,(X))"
i=I

This shows that the prime ideals of the ring *R* = O!X]/('p(X)) are the principal ideals (/J;) generated by the *'p;(X)* mlXl *'p(X),* for i = I, ., *r.* that the degree *IR/Cji,):* B] equals the degree of the polynomial 'p,(X), and tha1

(Ol =*<ii)*= no,,J".
i=I

In view of lhc isomorphism OfXI/("p(X)) � *OfpO,* /(X) 1-,J- /(0). the same situation holds in 1hc ring *O* =*0 j'pfJ.* Thus lhc prime ideals �; of *0* correspond to the prime ideJls ("p,-), and they are 1he prindpal ideals generated by the *p;* (0) moJ))0. The degree [*c5*/�, : Bl is the degree of the polynomial *"p;(X),* and we have (0) = n�=1i_p;•. Now *let* q.:3; = *p0+p;(0)(')* he thi.: preimagc of i,p, with respt:Cl to the canonical homomorphism

o-o;po.

Then 1+!,·, for *i* = I. ., *r,* varies over the prime ideals of *O* above p. */1* = I *0/�;* : o/p) is the degree of the JX)lynomial /J;(X). Furthcnnore 13? is the preimage of�? (he0tuse *e;* = #I$" IVE N}), and pO 2 n;-1.-.P?' -�o that po1n;..,.,1J? and therefore pO = n;·=.11:· because *Lt•;/;=* II.

D

The prime ideal pis said to **split completely** (or to be **totally split)** in *L,* if in the decomposition

$$p = q3�1 \quad . q3�•,.$$

onehasr $= n =$!L: KJ, so that $e; = f; = 1$ for all i $=$ I. ,*r.* pis called **nonsplit, or indecomposed,** if $r = $ I, i.e., if there is only a single prime ideal of *L* over p. From the fundamental identity

$$\sum_{i=I} r,e,fi � n$$

we now understand the name of inertia degree: the smaller this degree is, the more the ideal p will be tend to factor into different prime ideals.

The prime ideal q:l, in the decomposition p $=$ n;·=I qJ;" is called **unramified** over *o* (or over *K)* if e1 $=$ I and if the residue class field extension 0/q:lilo/p is separable. If not, it is called **ramified,** and **totally ramified** if furthennore $Ji =$ I. The prime ideal p is called unramified if all q}; are unramified, otherwise it is called ramified. The extension *LIK* itself is called unramified if all prime ideals p of *K* are unramilied in L

The case where a prime ideal p of *K* is ramified in *L* is an exceptional phenomenon. In fact, we have the

(8.4) Proposition. *If L K is separable,* then there,ire *only finitely* many *prime* ideals of *K which are ramified in L.*

Proof: Let *O* E *O* be a primitive element for *L,* i.e.. $L = K(0)$, and let p(X) E o[XJ be its minimal polynomial. Let

$$d = d(l,0. \quad , 0n-l) = \prod (0; - 0_1)^2 \in o$$

be the discriminant of *p(X)* (see §2, p. 11). Then every prime ideal p of *K* which is relatively prime to *d* and to the conductor J of *o[O* J is unramified. In fact, by (8.3), the ramincalion indices *ei* equal I as soon as they are equal to I in the factorization of *"p(X)* $=$ *p(X)* mod pin o_/p, so certainly if "p(X) has no multiple roots. But this is the case since the discriminant $d = d$ mlXI p of *p(X)* is nonzero. The residue class field extensions 0/q};lo/p are generated by $iJ = fJ$ mod �i and therefore separable. Hence p is unramilicd. 0

The precise description of lhe ramified prime ideals is given by the **discriminant** of 01*o.* It is defined to be the ideal *iJ* of *o* which is generated by the discriminants d(w1, , *wn)* of all bases w1, .,*wn* of *LIK* contained in *0*. We will show in chapter Ill, *2 that the prime divisors of U are exactly the prime ideals which ramify in *L*.

Example: The law of decomposition of prime numbers */J* in a quadratic number field *Q(,JQ)* is intimately related to Gauss's famous quadratic reciprocity law. The latter concerns the problem of integer solutions of the equation

$$x^2+hy=a, \quad (a,hEZ).$$

the simplest among the nontrivial diophantinc equations. The theory of this equation reduces immediately to the case where b is an odd prime number p and $(a,p) = $ I (exercise 6). Let us assume this for the sequel. We are then facing the question as to whether a is a quadratic residue mod p. i.e., whether the congruence

$$x^2 = a \bmod p$$

does or docs not have a solution. In other words. we want to know if the equation _f^2 = *ii*, for a given element a = a mcxl p E F;,, admits a solution in the field *FI'* or not. For this one intrcxluces the Legendre symboJ (%), which, for *every* rational number a relatively prime *top, is* defined to be (_*) = l or -1, according as $x^2 == a$ mod p has or docs not have a solution. This symbol is multiplicative,

(�)�(�)(%)

This is because the group IF;, is cyclic of order *p-1* and the subgroup IF;,2 of squares has index 2, i.e., F;1;F;,^{2} � Z/22. Since(�)= I<===;,, a E 11<;2, one also has

$$p(a)= a^{''-''} \bmod p.$$

In the case of squarefree a, the Legendre symbol (%) bears the following relation with prime factorization. (*) = I signifies that

$$x^2 - a-= (x - i:t)(x + a) \bmod p$$

for some a E 2. The conductor of 2/�} *in* the ring of inicgers of *Q(./a)* is a divisor of 2 (see S 2, exercise 4). We may therefore apply proposition (8.3) and obtain the

(8.5) Proposition. For squarefreea *and (p, la)* = I, *welwvctheequivalence*

(�)=I {::::::> *p istotallysplitinQCJO).*

For the Legendre symbol, one has the following remarkable law, which like none other has left its mark on the development of algebraic number theory.

(8.6) Theorem (Gauss's Reciprocity Law). *For two distinct odd prime numbers ℓ and p, the following identity holds:*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}.$$

One also has the two "supplementary theorems"

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$ implies $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ since $p \neq 2$.

In order to determine $\left(\frac{2}{p}\right)$, we work in the ring $\mathbb{Z}[i]$ of gaussian integers. Since $(1+i)^2 = 2i$, we find

$$(1+i)^p = (1+i)\big((1+i)^2\big)^{\frac{p-1}{2}} = (1+i)i^{\frac{p-1}{2}}2^{\frac{p-1}{2}},$$

and since $(1+i)^p \equiv 1+i^p \bmod p$ and $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \bmod p$, it follows that

$$\left(\frac{2}{p}\right)(1+i)i^{\frac{p-1}{2}} \equiv 1+i(-1)^{\frac{p-1}{2}} \bmod p.$$

From this, an easy computation yields

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{4}} \bmod p, \quad \text{resp.} \quad \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p+1}{4}} \bmod p,$$

if $\frac{p-1}{2}$ is even, resp. odd. Since $\frac{p^2-1}{8} = \frac{p-1}{2}\frac{p+1}{4} = \frac{p+1}{2}\frac{p-1}{4}$, we deduce $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

In order to prove the first formula, we work in the ring $\mathbb{Z}[\zeta]$, where ζ is a primitive ℓ-th root of unity. We consider the Gauss sum

$$\tau = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{a}{\ell}\right)\zeta^a$$

and show that

$$\tau^2 = \left(\frac{-1}{\ell}\right)\ell.$$

For this, let a and b vary over the group $(\mathbb{Z}/\ell\mathbb{Z})^*$, put $c = ab^{-1}$ and deduce from the identity $\left(\frac{a}{\ell}\right) = \left(\frac{a^{-1}}{\ell}\right)$ that

$$\left(\frac{-1}{\ell}\right)\tau^2 = \sum_{a,b}\left(\frac{-ab}{\ell}\right)\zeta^{a+b} = \sum_{a,b}\left(\frac{ab^{-1}}{\ell}\right)\zeta^{a-b} = \sum_{b,c}\left(\frac{c}{\ell}\right)\zeta^{bc-b}$$
$$= \sum_{c\neq 1}\left(\frac{c}{\ell}\right)\sum_b \zeta^{b(c-1)} + \sum_b\left(\frac{1}{\ell}\right).$$

Now $\sum_c \left(\frac{c}{\ell}\right) = 0$, as one sees by multiplying the sum with a symbol $\left(\frac{x}{\ell}\right) = -1$, and putting $\xi = \zeta^{c-1}$ gives $\sum_b \zeta^{b(c-1)} = \xi + \xi^2 + \dots + \xi^{\ell-1} = -1$, from which we indeed find that

$$\left(\frac{-1}{\ell}\right)\tau^2 = -\sum_{c\neq 1}\left(\frac{c}{\ell}\right) + \ell - 1 = \ell.$$

This, together with the congruence $\left(\frac{\ell}{p}\right) \equiv \ell^{\frac{p-1}{2}} \bmod p$ and the identity $\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}$, implies

$$\tau^p = \tau(\tau^2)^{\frac{p-1}{2}} = \tau(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\left(\frac{\ell}{p}\right) \bmod p.$$

On the other hand one has

$$\tau^p \equiv \sum_a\left(\frac{a}{\ell}\right)\zeta^{ap} \equiv \left(\frac{p}{\ell}\right)\sum_a\left(\frac{ap}{\ell}\right)\zeta^{ap} \equiv \left(\frac{p}{\ell}\right)\tau \bmod p,$$

so that

$$\left(\frac{p}{\ell}\right)\tau \equiv \tau(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\left(\frac{\ell}{p}\right) \bmod p.$$

Multiplying by τ and dividing by $\pm\ell$ yields the claim. □

We have proved Gauss's reciprocity law by a rather contrived calculation. In § 10, however, we will recognize the true reason why it holds in the law of decomposition of primes in the field of ℓ-th roots of unity. The Gauss sums do have a higher theoretical though, as will become apparent later (see VII, §2 and §6).

Exercise 1. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathfrak{o}$, then one has $\mathfrak{a} = \mathfrak{a}\mathcal{O} \cap \mathfrak{o}$ and $\mathfrak{a}|\mathfrak{b} \iff \mathfrak{a}\mathcal{O}|\mathfrak{b}\mathcal{O}$.

Exercise 2. For ideal $\mathfrak{A}$ of $\mathcal{O}$ there exists a $\theta \in \mathcal{O}$ such that the conductor $\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq \mathfrak{o}[\theta]\}$ is prime to $\mathfrak{A}$ and such that $L = K(\theta)$.

Exercise 3. If a prime ideal $\mathfrak{p}$ of K is totally split in two separable extensions $L|K$ and $L'|K$, then it is also totally split in the composite extension.

Exercise **4,** A prime ideal p of K is totally split in the separable extension LIK if and only if it is totally split in the Galois closure NIK of l, lK.

Exercise 5. For a number field K the statement of proposition com.:cming the prime decomposition in the extension $K(0)$ holds for all prime pf(O:O[RI).

Exercise 6. Given a positive integer $h >$ I, an a relatively prime lo h is a quadratic residue mod h if and only if it is a residue modulo each prime divisor p of h, and if $a=$ I mod 4 when 41h. resp. $a=$ I mod 8 when Slh.

Exercise 7. Let (a,p) =land $av=r_{,,}$ mod p, $v =$ I, �-1, $0 < r_{,,} < p$. T�en t.he $r_{,,}$ give a permutation τc of the numhers I. .., p - I. Show that sgn τc = (¹//).

Exercise 8. Let iln =�•where $r = \frac{1\sqrt{5}}{}$, $p' = \frac{1}{2}\sqrt{5}$ $(a_{,,}$ is the 11-th Fibon,it:ci number). If pis a prime number *cf.* 2,5, then one has

$$a_p = (j) \mod p.$$

Exercise 9. Study the Legendre symbol (¾) as a function of $p >$ 3. Show that the property of 3 being a quadratic residue or nonresidue mod p depends only on the class of p mod 12.

Exercise IO. Show that the numher of solutions of $x^2 = a$ mod p equals I + (fJ).

Exercise **11.** Show that the number of solutions of the congruence $ax^2 + hx + c =$ 0 mod p. where (a,p} = 1,equals I+ $(\frac{/)^2-4ac}{p})$.

§9. Hilbert's Ramification Theory

The question of prime decomposition in a finite extension LIK takes a particularly interesting and important tum once we assume LIK to be a Galois extension. The prime ideals arc then subject to the action of the Galois group

$$G � G(LIK).$$

The "ramification theory" that arises from this assumption has been introduced into number theory by *D,ivw HILBERT* (1862-1943). Given a in the ring CJ of integral elements of L, the conjugate aa, for every a E G. also belongs to CJ, i.e., G acts on 0. If '13 is a prime ideal of CJ above p, then so is a,P. for each a E G, because

$$a,P \text{ no}= \quad a(,P \text{ no})= ap= \mathrm{p}.$$

The ideals $a,P,$ for a E G, are called the prime ideals **conjugate** to ,P.

(9.1) Proposition. *The* Galois group *G acts transitively on* the set *of all* prime *ideals* [1],p*ofO lying* above p, *i.e.,* the.�e prime *ideals* are *al/* conjugates of *each other.*

Proof: Let 13 and >..JJ' *be* two prime ideals above *p.* Assume >..JJ' *::/= a_}]* for any *a* E G. By the Chinese remainder theorem there exists *x* E Osuch that

xa==Omo<lW' and x==lmoda$ forall uEG.

Then *the nonn NL1K(X)* = *nf1E(i* ax belongs to�/ n O = *p, On* the other hand, *x* ¢ *a*� for any *a* E G, hence *ax*¢� forany *a* E *G.* Consequently n,-cG *ax*¢�no= p, a contradiction. 0

(9.2) Definition. If,P is *a* prime *ideal* of *O. then the subgroup*

G'Jl�{acGia'lJ�'P)

is ca/led *the* **decomposition group** of$ over *K. The* fixed *field*

Z'l-l={xELlax=x forallaEG,,p)

is called *the* **decomposition field** of',}} over *K.*

The decomposition group encodes in group-theoretic language the number of different prime ideals into which a prime ideal p of *o* decomposes ln *CJ.* For if q3 is one of them and *a* varies over a system of representatives of the cosets in G/Gr+i, then *aq:3* varies over the different prime ideals above p, each one occurring precisely once, i.e., their number equals the index (G: G'l-J). In particular, one has

G,:i, = *1* {::::::=;> Z13 = *L* {=::=:, pis totally split,

G'l-l = *G* {::::::::} Z<:JJ = *K* � p is nonsplit.

The decomposition group of a prime ideal *a* q3 conjugate to q3 is the t:Oil_jugale- .-;ubgmup

Ga'l-J = *a* G,:pa-[1].

In fact, for r E *G,* one has the equivalences

t"EGa'l-J {::::::::} ral.JJ=al.JJ {::::::::} a-[1],al.JJ=I.JJ

$$\iff \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}} \iff \tau \in \sigma G_{\mathfrak{P}}\sigma^{-1}$$

Remark: The decomposition group regulates the prime decomposition also in the case of a non-Galois extension. For subgroups *U* and *V* of a group G, consider the equivalence relation in G defined by

a ~ *r,'* {::::::::} *a'*= *l/OV* for *u* EV, *v* E V.

The corresponding equivalence classes

$$UaV=\backslash uavluEU, \ \mathrm{vEV}\}$$

are called the **double** cosets of G modd U, V. The set of these double cosets, which form a partition of G, is denoted $U\backslash G/V$.

Now !cl LI K be an arbitrary separable extension, and embed it inlo a Galois extension NIK with Galois group G. In G, consider the subgroup H = G(NIL). Let p be a prime ideal of Kand Pp the set of prime ideals of L above p. If 11 is a prime ideal of N above p, then the rule

$$H\backslash G/G,v\text{---+ } Pp, \quad HaG,v \text{ i-------+ a11nL.}$$

gives a well-defined bijection. The proof is left to the reader.

In the Galois case, the inertia degrees f1, . . , _t;. and the ramification indices e1, . . , er in the prime decomposition

$$\mathrm{p} = 11�^{1} \quad \text{-11�'}$$

of a prime ideal p of K are both independent of i.

$$f'i = \text{" " "} = f,. = f, \quad \text{CJ} = \bullet \text{" "} = e,. = \text{ ...;.}$$

In fact, writing 11 = 11_1, we find 11; = *a;11* for suitable *a;* E G, and the isomorphism *a;* : *(')* --+ *(')* induces an isomorphism

$$0/11 \text{ \_:::\_,.. } O/a;11, \quad a \text{ mod 11i-------+ } aia \quad \text{mod } ai11,$$

so that

$$J, \sim [\ 0/a,!J): \text{o/p}] \sim [\ \text{0/!J}): \text{o/p}]. \quad ; \sim \text{I.}$$

Furthermore, since *a;* (pO) = pO, we deduce from

$$\text{!JJ"lpO} = \text{a,(!JJ")la,(pO)} = \text{(a,!J)J"lpO}$$

the equality of thee;, i = I, *r*. Thus the prime decomposition ofp in C'J takes on the following simple fonn in the Galois case:

$$\text{p}\sim\text{(I)a!JJ)',}$$

where a varies over a system of representatives of G /Gr;µ. The decomposition field Z,,p of 11 over K has the following significance for the decomposition of p and the invariants e and f.

(9.3) **Proposition.** *Let* 11z = 11 n Z'+I be *the* prime *ideal* of Zti *below* q]. *Then* we have:

(i) 11z *is nonsplit* in *L, i.e.,* qJ *is the* only prime *ideal ofl* above11z-

(ii) 1J *over* Z<JJ *has ramification index e* and *inertia* degree f.

(iii) *The* ramification *index* and *the inertia* degree of111. over K *both equal* I.

Proof: (i) Since $G(L|Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$, the prime ideals above $\mathfrak{P}_Z$ are the $\sigma\mathfrak{P}$, for $\sigma \in G(L|Z_{\mathfrak{P}})$, and they are all equal to $\mathfrak{P}$.
(ii) Since in the Galois case, ramification indices and inertia degrees are independent of the prime divisor, the fundamental identity in this case reads

$$n = efr,$$

where $n := \#G$, $r = (G : G_{\mathfrak{P}})$. We see therefore that $\#G_{\mathfrak{P}} = [L : Z_{\mathfrak{P}}] = ef$. Let e', resp. e'', be the ramification index of $\mathfrak{P}$ over $Z_{\mathfrak{P}}$, resp. of $\mathfrak{P}_Z$ over K. Then $\mathfrak{p} = \mathfrak{P}_Z^{e''} \cdots$ in $Z_{\mathfrak{P}}$ and $\mathfrak{P}_Z = \mathfrak{P}^{e'}$ in L, so that $\mathfrak{p} = \mathfrak{P}^{e'e''} \cdots$, i.e., $e = e'e''$. One also obviously gets the analogous identity for the inertia degrees $f = f'f''$. The fundamental identity for the decomposition of $\mathfrak{P}_Z$ in L then reads $[L : Z_{\mathfrak{P}}] = e'f'$, i.e., we have $e'f' = ef$, and therefore $e'' = f'' = 1$. □

The ramification index e and the inertia degree f admit a further interesting group-theoretic interpretation. Since $\sigma\mathcal{O} = \mathcal{O}$ and $\sigma\mathfrak{P} = \mathfrak{P}$, every $\sigma \in G_{\mathfrak{P}}$ induces an automorphism

$$\bar\sigma : \mathcal{O}/\mathfrak{P} \longrightarrow \mathcal{O}/\mathfrak{P}, \quad a \bmod \mathfrak{P} \longmapsto \sigma a \bmod \mathfrak{P},$$

of the residue class field $\mathcal{O}/\mathfrak{P}$. Putting $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$ and $\kappa(\mathfrak{p}) = o/\mathfrak{p}$, we obtain the

(9.4) Proposition. *The extension $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ is normal and admits a surjective homomorphism*

$$G_{\mathfrak{P}} \longrightarrow G\big(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\big).$$

Proof: The inertia degree of $\mathfrak{P}_Z$ over K equals 1, i.e., $Z_{\mathfrak{P}}$ has the same residue class field $\kappa(\mathfrak{p})$ as K with respect to $\mathfrak{p}$. Therefore we may, and do, assume that $Z_{\mathfrak{P}} = K$, i.e., $G_{\mathfrak{P}} = G$. Let $\theta \in \mathcal{O}$ be a representative of an element $\bar\theta \in \kappa(\mathfrak{P})$ and $f(X)$, resp. $\bar g(X)$, the minimal polynomial of θ over K, resp. of $\bar\theta$ over $\kappa(\mathfrak{p})$. Then $\bar\theta = \theta \bmod \mathfrak{P}$ is a zero of the polynomial $\bar f(X) = f(X) \bmod \mathfrak{p}$, i.e., $\bar g(X)$ divides $\bar f(X)$. Since $L|K$ is normal, $f(X)$ splits over $\mathcal{O}$ into linear factors. Hence $\bar f(X)$ splits into linear factors over $\kappa(\mathfrak{P})$, and the same is true of $\bar g(X)$. In other words, $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ is a normal extension.

Now let $\bar\theta$ be a primitive element for the maximal separable subextension of $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ and

$$\bar\sigma \in G\big(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\big) = G\big(\kappa(\mathfrak{p})(\bar\theta)|\kappa(\mathfrak{p})\big)$$

Then *aiJ* is a root of if(X), and hence of *J(X),* i.e., there exists a *zero(}'* of *f* (X) such that *0'* = *a 0* mod qJ. *O'* is a conjugate of *O,* i.e., *0'* = *o 0* for some *o* E G(LIK). Since *oO* = *rr0* mod >.p, the automorphism *o* is mapped by the homomorphism in question to rJ. This proves the surjectivity.

□

(9.5) **Definition.** *The kernel* /,ll £ G'll *of the homomorphism*

G� - G(K(']'.l)IK(p))

is called the **inertia group** ofqJ over *K. The fixed field*

T<p={xELlax=x forallaE/,:p}

is ca/led *the* **inertia field** ofqJ over *K.*

This inertia field *T*,p appears in the tower of fields

$$K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L,$$

and we have the exact sequence

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow G\big(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\big) \longrightarrow 1.$$

Its properties arc expressed in the

(9.6) Proposition. *The extension* Tq,IZq, *i.� normal, and one ha.�*

$$G(T_{\mathfrak{P}}|Z_{\mathfrak{P}}) \cong G\big(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\big), \quad G(L|T_{\mathfrak{P}}) = I_{\mathfrak{P}}.$$

If the residue field extension K(q]) IK (p) *is separable, then one has*

$$\#I_{\mathfrak{P}} = [L : T_{\mathfrak{P}}] = e, \quad (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f$$

In this case one finds for *the* prime ide;li *'-PT* of *T;p below q3:*

(i) TI,e *ramification index ofq]* over *'-P·r is e and the* inertia degree is I.

(ii) *The ramification index* of!,pr over!,pz i.� I, and *the* inertia *degree* i.� *f.*

Proof: The first two claims follow from the identity #G,+l = *e.f.* So we only have to show statements **(i)** and (ii). Using the fundamental identity, they all follow from *K('-Pr)* = *K(�).* As the inertia group *f.:p* of� over *K* is also the inertia group of qJ over *T*q,, it follows from an application of proposition (9.4) to the extension *LIT,:µ* that G(K(!,p)IK('f.lr)) = I, hence *K(!,pr)* = K(!,p). □

In the diagram

K

we have indicated the ramification indices of the individual tield extensions on top, and the inertia degrees on the bottom. In the special case where the residue field extension K(qJ)IK(p) is separable we find

!�; = I {=::} T,11 = I {:::::::} p is unramiiicd in L.

In this case the Galois group G(K(q,})IK(p)) � G,,p of the residue class field extension may be viewed as a subgroup of G = G(LIK).

Hilbert's ramification theory, with its various refinements and generalizations, belongs naturally to the theory of valuations, which we will develop in the next chapter (see chap. 11, §9).

Exercise 1. If /.IK is a Galois extension of algebraic number fields v,ith noncyclic Galois group, then there are at most finitely many nonsplit prime ideals of *K*.

Exercise 2. If LI K is a Galois extension of algebraic number fields, and � a prime ideal which is unrarnitied over/<. (i.e., p = 1,Pn K is unramificd in/.), then there is one and only one automorphism ,p,.p E G(l,IK) such that

ip,_pa=a'1mod� forallaEO,

where $q = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$. ft is called the Frobenius automorphism. The dcrnmposition group $G_{\mathfrak{P}}$ is cyclic and *ip13*is a generator of G,1:.1-

Exercise 3. Let LI K be a solvable e:dension of prime degree p (not necessarily Galois). If the unramificd prime ideal p in *L* has two prime factors ilJ and 11}' of degree 1, then it is already totally split (theorem of *F.K. SCHMIDT).*

Hint: Use the following result of *GAI.OIS* (sec [75], chap. II, § 3): if *G* is a transitive solvable pennutation group of prime degree *p,* then there is no nontrivial pem1utation *o* E G which fixes two distinct letters.

Exercise **4,** Let *L* IK be a finite (not necessarily Galois) extension of algebraic number fields and *NIK* the nonnal closure of *LIK.* Show that u prime ideal p uf K is totally split in *L* if ,md only if it is totally split in *N.*

Hint: Use the double cosct decomposition *H\G/G13,* where *G* = G(NIK). *H* = G(NIL} and G'-P is the decomposition group of a prime ideal� over p.

§ 10. Cyclotomic Fields

The concepts and results of the theory as far as it has now been developed have reached a degree of abstraction which we will now balance by something more concrete. We will put the insights of the general theory to the task and make them more explicil in the example of the n-th cyclotomic field Qi((), where (is a primitive n-th root of unity. Among all number fields, this !ield occupies a special, central place. So studying it does not only furnish a worthwhile example but in fact an essential building block for the further theory.

It will be our first goal to determine explicitly the ring of integers of the field Q((). For this we need the

(10.1) Lemma. Let *11 be a prime* power f^{11} and *put* A = 1 - *l;. Then the principal* ideal (A) *in* the *ringo* of *integer.�* ofQ(l;) *is 11primc ideal* of degree I, *and* we /Jave

$$\ell \mathcal{O} = (\lambda)^d, \quad \text{where} \quad d = \varphi(\ell^\nu) = [\mathbb{Q}(\zeta) : \mathbb{Q}].$$

Furthennore, *the* basis l, (, , *1;^11-1* o[Q(()IQ has the *discriminant*

d(l,l;, 1;1^1-1)=±£'". s=f''-^1(vf-v-l).

Proof: The minimal polynomial of (over Q is the 11-th cyclotomic polynomial

$$\phi_n(X) = (X^{\ell^\nu} - 1)/(X^{\ell^{\nu-1}} - 1) = X^{\ell^{\nu-1}(\ell-1)} + \cdots + X^{\ell^{\nu-1}} + 1.$$

Putting X = I, we obtain the identity

$$\ell = \prod (1 - \zeta^g).$$

But I - *(g* = *s11(1* - (), for the algebraic integer *Ei:* = t--±-Z- 1 + (+ •· + (g-l_ If *1(* is an integer such that gg' = I mod then

1-l; 1-((1:)1:' �=�=I+*I;'*�+ +((g)g'-i

is integral as well, i.e.. *Fg* is a unit. Co�sequently £ = e(l - l;)'i'Wl, with the unite= n�F:g, hence £0 = (A)IO(t'l. Since IQ((): Q] = ip(r), the fundamental identity (8.2) shows that (A) is a prime ideal of degree I.

Let (= (1, . . *r,1* be the conjugates of (. Then the cyclotomic polynomial is *¢n(X)* = nf,...1(X -(1) and (sec §2, p. 11)

±d(l,(. ,J-I) � n ((,-(;) � n ,t,;(,,) � Nc,md</>;(n)
i#-j i=l

Differentiating the equation

$$(X^{\ell^{\nu-1}}-1)\phi_n(X)=X^{\ell^\nu}-1$$

and substituting ζ for X yields

$$(\xi-1)\phi_n'(\zeta)=\ell^\nu\zeta^{-1}$$

with the primitive ℓ-th root of unity $\xi=\zeta^{\ell^{\nu-1}}$. But $N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)=\pm\ell$, so that

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\xi-1)=N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)^{\ell^{\nu-1}}=\pm\ell^{\ell^{\nu-1}}.$$

Observing that ζ has norm ±1 we obtain

$$d(1,\zeta,\dots,\zeta^{d-1})=\pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}\big(\phi_n'(\zeta)\big)=\pm\ell^{\nu\ell^{\nu-1}(\ell-1)-\ell^{\nu-1}}=\pm\ell^s$$

with $s=\ell^{\nu-1}(\nu\ell-\nu-1)$. □

The ring of integers of $\mathbb{Q}(\zeta)$ is now determined, for arbitrary n, as follows.

(10.2) Proposition. A $\mathbb{Z}$-basis of *the ring* $\mathcal{O}$ of *integers* of $\mathbb{Q}(\zeta)$ is given *by* $1,\zeta,\dots,\zeta^{d-1}$, *with* $d=\varphi(n)$, *in other* words,

$$\mathcal{O}=\mathbb{Z}+\mathbb{Z}\zeta+\dots+\mathbb{Z}\zeta^{d-1}=\mathbb{Z}[\zeta].$$

Proof: We first prove the proposition in the case where n is a prime power ℓ^ν. Since $d(1,\zeta,\dots,\zeta^{d-1})=\pm\ell^s$, (2.9) gives us

$$\ell^s\mathcal{O}\subseteq\mathbb{Z}[\zeta]\subseteq\mathcal{O}.$$

Putting $\lambda=1-\zeta$, lemma (10.1) tells us that $\mathcal{O}/\lambda\mathcal{O}\cong\mathbb{Z}/\ell\mathbb{Z}$, so that $\mathcal{O}=\mathbb{Z}+\lambda\mathcal{O}$, and

$$\lambda\mathcal{O}+\mathbb{Z}[\zeta]=\mathcal{O}.$$

Multiplying this by λ and substituting the result $\lambda\mathcal{O}=\lambda^2\mathcal{O}+\lambda\mathbb{Z}[\zeta]$, we obtain

$$\lambda^2\mathcal{O}+\mathbb{Z}[\zeta]=\mathcal{O}.$$

Iterating this procedure, we find

$$\lambda^t\mathcal{O}+\mathbb{Z}[\zeta]=\mathcal{O}\quad\text{for all } t\ge1.$$

Fort = *s* r.p(C) this implies. in view of£ *o* =),._l9ti"lo (sec (10.1)). that

$$\mathcal{O} = \lambda^t\mathcal{O} + \mathbb{Z}[\zeta] = \ell^t\mathcal{O} + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta].$$

In the general case, let *n* = €'(1 €�. Then (; = is a primitive t:;' -th root of unity, and one has

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_r)$$

and Q:((1) • Q((i-l) nQ((i) = Q. By what we have just seen. for each i = I, , *r,* the elements I,(;. . <t-1, where *d;* = form an integral basis ofQ((;)IQJ. Since the discriminants d(l. (;, = ±(' are pairwise relatively prime, we conclude successively from that the elements (/1 ••?;/', with *j;* = 0. *d;* - 1, fom1 an integral basis of Q(OIQ, But each one of these elements is a power of *C.* Therefore every *a* E *o* may be written as a JX!lynomial *a* = *f(()* with coefficients in Z. Since (has degree rp(/l) over Q, the degree of the polynomial f(() may be reduced to r.p(11) - I. In this way one obtains a representation

a =ao+a1(+ +arp(nl-l('f'(l.'}-l

Thus I,(, , ('''(n)-1 is indeed an integral basis. □

Knowing that zrtl is the ring of imcgcrs of the field Q:(() we are now in a position to state explicitly the law of decomposition of prime numbers *p* into prime ideals of Q(n. It is of the most beautiful simplicity.

(10.3) Proposition. *Let* 11 = TT// *p*1'1, *be the prime factorization ofn and, for every prime number p, let fp be lhc* smallest *positive integer such that*

pf,,= I mod *n/p'''p.*

Then one has in Q(() *the factorization*

p = ())1 ••·p,-)'f'(fl''l'J.

where p1, , p,. *are di.�tinct prime* ideals, *,-1.II* of *degree fp-*

Proof: Since *o* = Zf(l, the conductor of Z[(I equals I. and we may apply proposition (8.3) to any prime number p. As a consequence, every p

decomposes into prime ideals in exactly the same way as the minimal polynomial $\phi_n(X)$ of ζ factors into irreducible polynomials mod p. All we have to show is therefore that

$$\phi_n(X) \equiv (\bar{p}_1(X)\cdots\bar{p}_r(X))^{\varphi(p^\nu)} \mod p,$$

where $\bar{p}_1(X), \dots, \bar{p}_r(X)$ are distinct irreducible polynomials over $\mathbb{F}_p$ of degree f_p. In order to see this, put $n = p^\nu m$. As ξ_i, resp. η_j, vary over primitive roots of unity of order m, resp. p^ν, the products $\xi_i\eta_j$ vary precisely over the primitive n-th roots of unity, i.e., one has the decomposition over $\mathcal{O}$:

$$\phi_n(X) = \prod_{i,j}(X - \xi_i\eta_j).$$

Since $X^{p^\nu} - 1 \equiv (X-1)^{p^\nu} \mod p$, one has $\eta_j \equiv 1 \mod \mathfrak{P}$, for any prime ideal $\mathfrak{P} | p$. In other words,

$$\phi_n(X) \equiv \prod_i (X-\xi_i)^{\varphi(p^\nu)} = \phi_m(X)^{\varphi(p^\nu)} \mod \mathfrak{P}.$$

This implies the congruence

$$\phi_n(X) \equiv \phi_m(X)^{\varphi(p^\nu)} \mod p.$$

Observing that f_p is the smallest positive integer such that $p^{f_p} \equiv 1 \mod m$, it is obvious that this congruence reduces us to the case where $p \nmid n$, and hence $\varphi(p^\nu) = \varphi(1) = 1$.

As the characteristic p of $\mathcal{O}/\mathfrak{P}$ does not divide n, the polynomials $X^n - 1$ and nX^{n-1} have no common root in $\mathcal{O}/\mathfrak{P}$. So $X^n - 1 \mod \mathfrak{P}$ has no multiple roots. We therefore see that passing to the quotient $\mathcal{O} \to \mathcal{O}/\mathfrak{P}$ maps the group μ_n of n-th roots of unity bijectively onto the group of n-th roots of unity of $\mathcal{O}/\mathfrak{P}$. In particular, the primitive n-th root of unity ζ modulo $\mathfrak{P}$ remains a primitive n-th root of unity. The smallest extension field of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ containing it is the field $\mathbb{F}_{p^{f_p}}$ because its multiplicative group $\mathbb{F}^*_{p^{f_p}}$ is cyclic of order $p^{f_p} - 1$. $\mathbb{F}_{p^{f_p}}$ is therefore the field of decomposition of the reduced cyclotomic polynomial

$$\bar{\phi}_n(X) = \phi_n(X) \mod p.$$

Being a divisor of $X^n - 1 \mod p$, this polynomial has no multiple roots, and if

$$\bar{\phi}_n(X) = \bar{p}_1(X)\cdots\bar{p}_r(X)$$

is its factorization into irreducibles over $\mathbb{F}_p$, then every $\bar{p}_i(X)$ is the minimal polynomial of a primitive n-th root of unity $\bar{\zeta} \in \mathbb{F}_{p^{f_p}}$. Its degree is therefore f_p. This proves the proposition. □

Let us emphasize two special cases of the above law of decomposition:

(10.4) Corollary. *A prime number p is* ramified *in* $\mathbb{Q}(\zeta)$ *if and only if*

$$n \equiv 0 \bmod p,$$

except in the case where $p = 2 = (4, n)$. *A prime number* $p \neq 2$ *is totally split in* $\mathbb{Q}(\zeta)$ *if and only if*

$$p \equiv 1 \bmod n.$$

The completeness of these results concerning the integral basis and the decomposition of primes in the field $\mathbb{Q}(\zeta)$ will not be matched by our study of the group of units and the ideal class group. The problems arising in this context are in fact among the most difficult problems posed by algebraic number theory. At the same time one encounters here plenty of astonishing laws which are the subject of a theory which has been developed only recently, **Iwasawa theory.**

The law of decomposition (10.3) in the cyclotomic field provides the proper explanation of Gauss's reciprocity law (8.6). This is based on the following

(10.5) Proposition. *Let ℓ and p be odd prime numbers,* $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$, *and ζ a primitive ℓ-th root of unity. Then one has:*

$$p \text{ is totally split in } \mathbb{Q}(\sqrt{\ell^*}) \iff p \text{ splits in } \mathbb{Q}(\zeta) \text{ into an even number of prime ideals.}$$

Proof: The little computation in §8, p. 51 has shown us that $\ell^* = \tau^2$ with $\tau = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{a}{\ell}\right)\zeta^a$, so that $\mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(\zeta)$. If p is totally split in $\mathbb{Q}(\sqrt{\ell^*})$, say $p = \mathfrak{p}_1\mathfrak{p}_2$, then some automorphism σ of $\mathbb{Q}(\zeta)$ such that $\sigma\mathfrak{p}_1 = \mathfrak{p}_2$ transforms the set of all prime ideals lying above $\mathfrak{p}_1$ bijectively into the set of prime ideals above $\mathfrak{p}_2$. Therefore the number of prime ideals of $\mathbb{Q}(\zeta)$ above p is even. Now assume conversely that this is the case. Then the index of the decomposition group $G_{\mathfrak{P}}$, or in other words, the degree $[Z_{\mathfrak{P}} : \mathbb{Q}]$ of the decomposition field of a prime ideal $\mathfrak{P}$ of $\mathbb{Q}(\zeta)$ over p is even. Since $G(\mathbb{Q}(\zeta)|\mathbb{Q})$ is cyclic, it follows that $\mathbb{Q}(\sqrt{\ell^*}) \subseteq Z_{\mathfrak{P}}$. The inertia degree of $\mathfrak{P} \cap Z_{\mathfrak{P}}$ over $\mathbb{Q}$ is 1 by (9.3), hence also the inertia degree of $\mathfrak{P} \cap \mathbb{Q}(\sqrt{\ell^*})$. This implies that p is totally split in $\mathbb{Q}(\sqrt{\ell^*})$. □

From this proposition we obtain the reciprocity law for two odd prime numbers ℓ and p.

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$$

as follows. It suffices to show that

$$\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right).$$

In fact, the completely elementary result $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (see §8, p. 51) then gives

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p}\right)(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}.$$

By (8.5) and (10.5), we know that $\left(\frac{\ell^*}{p}\right) = 1$ if and only if p decomposes *in the* field $\mathbb{Q}(\zeta)$ of ℓ-th roots of unity into an even *number* of prime ideals. By (10.3), this number is $r = \frac{\ell-1}{f}$, where f is the smallest positive integer such that $p^f \equiv 1 \bmod \ell$, i.e., r is even if and only if f is a divisor of $\frac{\ell-1}{2}$. But this is tantamount to the condition $p^{(\ell-1)/2} \equiv 1 \bmod \ell$. Since an element in the cyclic group $\mathbb{F}_\ell^*$ has an order dividing $\frac{\ell-1}{2}$ if and only if it belongs to $\mathbb{F}_\ell^{*2}$, the last congruence is equivalent to $\left(\frac{p}{\ell}\right) = 1$. So we do have $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$ as claimed.

Historically, Gauss's reciprocity law marked the beginning of algebraic number theory. It was discovered by *Euler*, but first proven by *Gauss*. The quest for similar laws concerning higher power residues, i.e., *the* congruences $x^n \equiv a \bmod p$, with $n > 2$, dominated number theory for a long time. Since this problem required working with the n-th cyclotomic field, *Kummer's* attempts to solve it led to his seminal discovery of ideal theory. We have developed the basics of this theory in the preceding sections and tested it successfully in the example of cyclotomic fields. The further development of this theory has led to a totally comprehensive generalization of Gauss's reciprocity law, Artin's reciprocity law, one of the high points in the history of number theory, and of compelling charm. This law is the main theorem of class field theory, which we will develop in chapters IV-VI.

Exercise 1. (Dirichlet's Prime Number Theorem). For every natural number n there are infinitely many prime numbers $p \equiv 1 \bmod n$.

Hint: Assume there are only finitely many. Let P be their product and consider the n-th cyclotomic polynomial ϕ_n. Not all numbers $\phi_n(xnP)$, for $x \in \mathbb{Z}$, can equal ± 1. Let $p \mid \phi_n(xnP)$ for suitable x. Deduce $p \equiv 1 \bmod n$ from this. (Dirichlet's prime number theorem is valid more generally for prime numbers $p \equiv a \bmod n$, provided $(a,n) = 1$ (see VII, (5.14) and VII, § 13).)

Exercise 2. For every finile abelian group A there exists a Galois extension LIQ wilh Galois group G(LIQ) � A.

Hint: lh,e exercise I.

l<'.xercise .t Every quadratic number field Q(./d) is contained in snme cyclotomic field Q(I;,,). (,, a primitive n-th root of unity.

Exercise 4. Describe the quadratic subfield� of Q({")IQ-. in the case where n is odd.

Exercise 5. Show that Q(.;=T), Q(.J2), (H/=2) are the quadrntic subfields of Q({N)IQ forn = 2Y.q:::: 3.

§ 11. Localization

To "localize" means to form quotients, 1he most familiar r.:ase being the passage from an integral domain A to i1s field of fractions

$$K = \{1, \mid a \in \Lambda. \ h \in A, \{Oil\bullet$$

More genemlly. choosing instead of A, IOJ any nonempty S � A, {01 whir.:h is closed under muhiplicarion. one again ob1ains a ring struclurc on the set

$$J\backslash S^{-1} = 1; \ EK \mid a \ EA.. \backslash'Es\}.$$

The most important special case of such a multiplicative subset is the complement $S = A$, p of a prime ideal p of A. In thi� case one writes Ap instead of AS^{-1}. and one calls the ring Ap lhc localization of A at p. When dealing with problems that involve a single prime ideal p of A al a lime it is oflen expedient to replace A by the localization Ap. This procedure forgeli. everything that has nothing to do with p. and brings oul more clearly all the propenies cunceming p. For imaance, the mapping

$$q i\text{------}\ qAp$$

gives a I-I-correspondence between the prime ideals q � p of A and the prime ideals of Ap. More generally for any multiplicative sCl S. one has the

(11.l) Proposition. *The mapping.,;*

$$q t\text{----}) \ qS^{-1} \ ;ind \ D � \ 0 \cap A$$

arc muwafly inverse *I-I-correspondence.* �*f,etwee11 the* prime *ideal.* �q� *A"S* of *A a11d che prime* ideals D of AS 1.

Proof: If q � A" S is a prime ideal of A. then

u'-- q''c-l__lq_; qE q. s Ed

is a prime ideal of As-[1]. Indeed, in obvious notation, the relation%� ED, i.e., S =!fa.implies that $s''aa' = qss'$ E q. Therefore aa' E q:_because s'' ¢ q, and hence a or a' belong to q, which shows that � or ? belong to D. Furthermore one has

q�QnA.

since $i = a$ ED n A implies $q = as$ E q, whence a E q because s ¢ q.

Conversely, let Q be an arbitrary prime ideal of As^{-1}. Then q = D n A is obviously a prime ideal of A, and one has q £; A "'- S. In fact, if q were to contain ans ES, then we would have I = s •}ED. because+ E As-[1]. Furthermore one has

For if TE 0, then a= T •s ED n A= q, hence�= a} E qs^{-1}. The mappings q r-+ qs-[1] and D 1--+ D n A are therefore inverses of each other, which proves the proposition. □

Usually S will be the complement of a union LJP"X p over a set X of prime ideals of A. In this case one writes

A(X)� \f I $f.gcA$. g,'Omo<lpfmpcxj

instead of As^{-1}. The prime ideals of A(X) correspond by (11.1) 1-1 to the prime ideals of A which are contained in LJp.:X p, all the others are being eliminated when passing from A to A(X). For instance, if X is finite or omits only finitely many prime ideals of A, then only lhc prime ideals from X survive in $A(X)$.

In the case that X consists of only one prime ideal 1,1, the ring A(X) is the localization

A,� { f I $f.g$ EA. g ,' 0 mod p}

of A at p. Here we have the

(11.2) Corollary. *If* p isaprimeideaJofA, *then* A_p *is* a local ring, i.e., Ap has a *unique maximal* ideal. *namely* mp = pAp. There *is a canonical embedding*

A/p '-------+ A,/m,,

identifying Ap/mp *with the field of fractions of A/i.,. In p<-1.rticular,* if p *is* a *maximal* ideal of A, *then one* has

A/p" � Ap/m; for n 2: I.

Proof: Since the ideals of Ap correspond 1-1 to the ideals of A contained in p, the ideal $m_{11} = pA_{11}$ is the unique maximal ideal. Let us consider the homomorphism

$$l: A/pn\text{-----}+ A_{11}/m�, \quad a \bmod pn \text{ i--------+ } a \bmod m;.$$

For $n = I$, f is injective because p $=$ mp n A. Hence Ap/mpAp becomes the field of fractions of A/p. Let p be maximal and n 2-. I. For every .1· E A '"- p one has $pn + sA = A$, i.e., $S = s$ mlXI p^{11} is a unit in A/pn. For $n = 1$ this is clear from the maximality of p, and for n :::: 1 it follows by induction: $A=$ $p^{11\ 1}$ $+sA$ =} p $=pA$ =p(pn-l $+sA)$ ':Z pn $+sA$ =} p" $+sA$ = !\.

Injectivity off: let a EA be such that a Em;, i.e.. $a=$ h/s with h E s ¢ p. Then $as=$ h E p^{11}, so that a ."f $= 0$ in $A/pt1$, and hence $ii=$ O in

Surjectivity off: let a/s E Ap, a EA, s ¢ p. Then by the alxive, there exists an a' E A such that $a = a's$ mod pn. Therefore $a/s = a'$ mod pn Ap, i.e., a/s mod m; lies in the image off. □

In a local ring with maximal ideal m, every element a ¢ m is a unit. Indeed, since the principal ideal (a) is not contained in any other maximal ideal, it has to be the whole ring. So we have

$$A^* = A''' - m.$$

The simplest local rings, except for fields, are discrete valuation rings.

(11.3) Definition. *A discrete valuation ring* i.� a *principal ideal domain o with a unique maximal ideal* p -/- 0.

The maximal ideal is of the fonn p $=$ (rr) $=$ rro, for some prime element *Jr.* Since every element not contained in p is a unit, it follows that, up to associated elements, *Jr* is the only prime element of Every nonzero clement of *o* may therefore be written as *E ;rn,* for some *E* E *o**, and n 2-. 0, More generally, every clement a -/- 0 of the tield of fractions K may be uniquely written as

$$a = ETCn, \quad EEO^*, \quad nEZ.$$

The exponent n is called the valuation of a. It is denoted $v(a)$, and it is obviously characlCrized by the equation

$$(a) = p<'(aJ\_$$

The valuation is a function

$$1.1: K^*\text{-----}+ Z.$$

Extending it to K by the convention $v(0) = \infty$, a simple calculation shows that it satisfies the conditions

$$v(ab) = v(a) + v(b), \quad v(a+b) \geq \min\{v(a), v(b)\}.$$

This innocuous looking function gives rise to a theory which will occupy all of the next chapter.

The discrete valuation rings arise as localizations of Dedekind domains. This is a consequence of the

(11.4) Proposition. *If $\mathcal{o}$ is a Dedekind domain, and $S \subseteq \mathcal{o} \setminus \{0\}$ is a multiplicative subset, then $\mathcal{o}S^{-1}$ is also a Dedekind domain.*

Proof: Let $\mathfrak{A}$ be an ideal of $\mathcal{o}S^{-1}$ and $\mathfrak{a} = \mathfrak{A} \cap \mathcal{o}$. Then $\mathfrak{A} = \mathfrak{a}S^{-1}$, because if $\frac{a}{s} \in \mathfrak{A}$, $a \in \mathcal{o}$ and $s \in S$, then one has $a = \frac{a}{s} s \in \mathfrak{A} \cap \mathcal{o} = \mathfrak{a}$, so that $\frac{a}{s} = a \cdot \frac{1}{s} \in \mathfrak{a}S^{-1}$. As $\mathfrak{a}$ is finitely generated, so is $\mathfrak{A}$, i.e., $\mathcal{o}S^{-1}$ is noetherian. It follows from (11.1) that every prime ideal of $\mathcal{o}S^{-1}$ is maximal, because this holds in $\mathcal{o}$. Finally, $\mathcal{o}S^{-1}$ is integrally closed, for if $x \in K$ satisfies the equation

$$x^n + \frac{a_1}{s_1} x^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

with coefficients $\frac{a_i}{s_i} \in \mathcal{o}S^{-1}$, then multiplying it with the n-th power of $s = s_1 \cdots s_n$ shows that sx is integral over $\mathcal{o}$, whence $sx \in \mathcal{o}$ and therefore $x \in \mathcal{o}S^{-1}$. This shows that $\mathcal{o}S^{-1}$ is a Dedekind domain. □

(11.5) Proposition. *Let $\mathcal{o}$ be a noetherian integral domain. $\mathcal{o}$ is a Dedekind domain if and only if, for all prime ideals $\mathfrak{p} \neq 0$, the localizations $\mathcal{o}_\mathfrak{p}$ are discrete valuation rings.*

Proof: If $\mathcal{o}$ is a Dedekind domain, then so are the localizations $\mathcal{o}_\mathfrak{p}$. The maximal ideal $\mathfrak{m} = \mathfrak{p}\mathcal{o}_\mathfrak{p}$ is the only nonzero prime ideal of $\mathcal{o}_\mathfrak{p}$. Therefore, choosing any $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$, one necessarily finds $(\pi) = \mathfrak{m}$, and furthermore $\mathfrak{m}^n = (\pi^n)$. Thus $\mathcal{o}_\mathfrak{p}$ is a principal ideal domain, and hence a discrete valuation ring.

Letting $\mathfrak{p}$ vary over all prime ideals $\neq 0$ of $\mathcal{o}$, we find in any case that

$$\mathcal{o} = \bigcap_{\mathfrak{p}} \mathcal{o}_\mathfrak{p}.$$

For if $\frac{a}{b} \in \bigcap_\mathfrak{p} \mathcal{o}_\mathfrak{p}$, with $a, b \in \mathcal{o}$, then

$$\mathfrak{a} = \{x \in \mathcal{o} \mid xa \in b\mathcal{o}\}$$

is an ideal which c_ann�t be con�ained in any prime ideal of *o*. In fact, for any p, we may wnte h = -¹;: with *c* E *o*, *s ff*. p, so that *sa* = *he*, hence *s* Ea " p. As a is not c_onta��ed in any maximal ideal, it follows that a= *o*, hence *a*= I - *a* Eh o, 1.e., h E o.

Suppose now that the Op are discrete valuation rings. Being principal ideal domains, they are integrally closed (see §2), so o = np Op is also integrally dosed. Finally, from (11.1) it follows that every prime ideal p -*I*- 0 of o is maximal because this is so in Op. Therefore o is a Dedekind domain. n

For a Dedekind domain o, we have for each prime ideal p -*I*- 0 the discrete valuation ring Op and the corresponding valuation

vp : K^*----)- Z

of the field of fractions. The significance of these valuations lies in their relation to the prime ideal factorization. If *x* E K''' and

(xl � IT p",
p

is the prime factorization of the principal ideal (x), then, for each p, one has

\!p = vp(X).

In fact, for a fixed prime ideal q -*I*- 0 of *o*, the first equation above implies (because p Oq = Oq for p -*I*- q) that

xoq = (TTp"P)oq = q"•1oq = m�".
p

Hence indeed *Vq(X)* = *Vq*, In view of this relation, the valuations vp arc also called **exponential valuations.**

The reader should check that the localization of the ring Z at the prime ideal (p) = *pZ* is given by

Z(J,J = {*I *a,h* E Z, pfh}.

The maximal ideal pZ(f') consists of all fractions *a/h* satisfying *p 1 h,* and the group of units consists of all fractions *a/h* satisfying *p ah*. The valuation associated to Z(p),

Vp : Q)- Z U \ooj,

is called the **p-adic valuation** of Q. The valuation *vp(x)* of an clement *x* E Q* is given by

vr,(x) = *v,*

where x = *p"a/h* with integers *a,h* relatively prime top.

To end this section, we now want to compare a Dedekind domain $\mathfrak{o}$ to the ring

$$\mathfrak{o}(X) = \{\tfrac{f}{g} \mid f, g \in \mathfrak{o},\ g \not\equiv 0 \bmod \mathfrak{p} \ \text{for} \ \mathfrak{p} \in X\},$$

where X is a set of prime ideals $\neq 0$ of $\mathfrak{o}$ which contains almost all prime ideals of $\mathfrak{o}$. By (11.1), the prime ideals $\neq 0$ of $\mathfrak{o}(X)$ are given as $\mathfrak{p}_X = \mathfrak{p}\,\mathfrak{o}(X)$, for $\mathfrak{p} \in X$, and it is easily checked that $\mathfrak{o}$ and $\mathfrak{o}(X)$ have the same localizations

$$\mathfrak{o}_\mathfrak{p} = \mathfrak{o}(X)_{\mathfrak{p}_X}.$$

We denote by $Cl(\mathfrak{o})$, resp. $Cl(\mathfrak{o}(X))$, the ideal class groups of $\mathfrak{o}$, resp. $\mathfrak{o}(X)$. They, as well as the groups of units $\mathfrak{o}^*$ and $\mathfrak{o}(X)^*$, are related by the following

(11.6) Proposition. *There is a canonical exact sequence*

$$1 \longrightarrow \mathfrak{o}^* \longrightarrow \mathfrak{o}(X)^* \longrightarrow \bigoplus_{\mathfrak{p} \notin X} K^*/\mathfrak{o}_\mathfrak{p}^* \longrightarrow Cl(\mathfrak{o}) \longrightarrow Cl(\mathfrak{o}(X)) \longrightarrow 1,$$

and one has $K^*/\mathfrak{o}_\mathfrak{p}^* \cong \mathbb{Z}$.

Proof: The first arrow is inclusion and the second one is induced by the inclusion $\mathfrak{o}(X)^* \to K^*$, followed by the projections $K^* \to K^*/\mathfrak{o}_\mathfrak{p}^*$. If $a \in \mathfrak{o}(X)^*$ belongs to the kernel, then $a \in \mathfrak{o}_\mathfrak{p}^*$ for $\mathfrak{p} \notin X$, and also for $\mathfrak{p} \in X$ because $\mathfrak{o}_\mathfrak{p} = \mathfrak{o}(X)_{\mathfrak{p}_X}$, hence $a \in \bigcap_\mathfrak{p} \mathfrak{o}_\mathfrak{p}^* = \mathfrak{o}^*$ (see the argument in the proof of (11.5)). This shows the exactness at $\mathfrak{o}(X)^*$. The arrow

$$\bigoplus_{\mathfrak{p} \notin X} K^*/\mathfrak{o}_\mathfrak{p}^* \longrightarrow Cl(\mathfrak{o})$$

is induced by mapping

$$\bigoplus_{\mathfrak{p} \notin X} \alpha_\mathfrak{p} \bmod \mathfrak{o}_\mathfrak{p}^* \longmapsto \prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})},$$

where $v_\mathfrak{p} : K^* \to \mathbb{Z}$ is the exponential valuation of K associated to $\mathfrak{o}_\mathfrak{p}$. Let $\bigoplus_{\mathfrak{p} \notin X} \alpha_\mathfrak{p} \bmod \mathfrak{o}_\mathfrak{p}^*$ be an element in the kernel, i.e.,

$$\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} = (a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a)}$$

for some $a \in K^*$. Because of unique prime factorization, this means that $v_\mathfrak{p}(a) = 0$ for $\mathfrak{p} \in X$, and $v_\mathfrak{p}(\alpha_\mathfrak{p}) = v_\mathfrak{p}(a)$ for $\mathfrak{p} \notin X$. It follows that $a \in \bigcap_{\mathfrak{p} \in X} \mathfrak{o}_\mathfrak{p}^* = \mathfrak{o}(X)^*$ and $a \equiv \alpha_\mathfrak{p} \bmod \mathfrak{o}_\mathfrak{p}^*$. This shows exactness in the middle. The arrow

$$Cl(\mathfrak{o}) \longrightarrow Cl(\mathfrak{o}(X))$$

comes from mapping a i---+ ao(X). The classes of prime ideals p E X are mapped onto the classes of prime ideals of o(X). Since C/(o(X)) is generated by these classes, the arrow is surjective. For p ¢ X we have po(X) = (1), and this means that the kernel consists of the classes of the ideals TTp¢X p"r. This, however, is visibly the image of the preceding arrow. Therefore the whole sequence is exact. Finally, the valuation vp : K• _,.. Z produces the isomorphism K^*/o; ;:: Z. □

For the ring of integers o_K of an algebraic number field K, the proposition yields the following results. Let S denote a finite set of prime ideals of o_K (not any more a multiplicative subset), and let X be the set of all prime ideals that do not belong to S. We put

$$of= \text{OK}(X).$$

The units of this ring are called the **S-units,** and the group *Ctf* = *Cl(of)* the S-class **grnup** of K.

(11.7) Corollary. *For the group* K^5 = (oft *of* S-units of K *there* i.� *an* isomorphism

$$K^S \cong \mu(K) \times \mathbb{Z}^{\#S+r+s-1},$$

where r ands are defined as in§ 5, *p.* 30.

Proof: The torsion subgroup of *Ks* is the group *11(K)* of roots of unity in K. Since Cl(o) is finite, we obtain the following identities from the exact sequence (11.6) and from (7.4):

$$\text{rank}(Ks) = \text{rank}(oK) + \text{rank}(\underset{p,c,<;}{EB}\ Z) = \#S + r + s - 1.$$

This proves the corollary. □

(11.8) Corollary. *The S-class group Clk* = Cf(ok) is finite.

Exercise **1.** Let A be an arbitrary ring, not an integral domain, let M be an A-module and Sa multiplirntivcly dosed A such that Or/:. S. In M x S consider the equivalence relation

$$(m,s) \sim (m',s') \iff \exists\, s'' \in S \text{ such that } s''(s'm - sm') = 0.$$

Show that the of equivalence classes *(m,s)* fonm an A-module. and that M --;. *Ms, a* f-)- isa homomorphism. In particular, *As* is a ring. It is called the **localization** A respeel to S.

Exercise 2. Show that, in the above situation, the prime ideals of *As* correspond 1-l to the prime ideals of *A* which are disjoint from 5. If pc; *A* <md P.1 C; correspond in this way. then *As/P₁*· is the localization of A/p with respect to the of *S*

Exercise 3. Let f : M --+ N be a homomorphism of A-modules. Then the following conditions are equivalent:

(i) f is injective(surjective).

(ii) $f\mu$: $M\mu$ ➔ N-., is inje<.:tivc (surjcctivc) for every prime ideal p.

(iii) fm Mm --+ Nm is injective (surjcctivc) for every maximal idea! m.

Exercise **4.** Let Sand T be two multiplicative subsets of A, and r• the image of T in A.₁. Then one has $A.w$ � (A.dr-

Exercise 5. Let : A ---,. B he a homomorphism of rings and S a multiplicatively closed subset that *f(S)* C; S•. Then f induces a homomorphism A.₁•-----),-*B*.

Exercise 6, Let A he an integral domain. If the localiz11lion A₁· is integral over A, then A.₁ = A.

Exercise 7 (Nakayama's **Lemma).** Let A be a local ring with maximal ideal m, let M he an A-module and N � M a submodule such that M/N is linitcly generated. Then one has the implication:

$$M=N+mM \;===^{*}\; M=N.$$

§**12.** Orders

The ring *OK* of integers of an algebraic number lield *K* is our chief interest because of its excellent property of being a Dedekind domain. Due to important theoretical as well as practical circumstances. however, one is pushed to devise a theory of greater gencralily which comprises also the theory of rings of algebraic integers which, like the ring

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{5} \subseteq \mathbb{Q}(\sqrt{5}),$$

are not necessarily imcgrally dosed. These rings are the so-called **orders.**

(12.1) Definition. *Let K* IQ be *an algebraic number field* of degree *n.* An order of *K* i.� *a subring o of OK which contains* an *integral* basis of *length n. The* ring *OK* is *called the* **maximal order** of *K.*

In concrete terms, orders are obtained as rings of the form

$$\mathcal{O} = \mathbb{Z}[\alpha_1, \dots, \alpha_r],$$

where $a_1, \dots, a_r$ are integers such that $K == \mathbb{Q}(a_1, \dots, a_r)$. Being a submodule of the free 2-module t)K, o does of course admit a Z-basis which, as Qo $= K$, has to be at the same time a basis of K IQ, and therefore has length n. Orders arise often as rings of multipliers, and as such have their practical applications. For instance, if $a_1, \dots a_n$ is any basis of K IQ and $M = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$, then

$$o_M = (a \in K \mid aM \subseteq M\}$$

is an order. The theoretical significance of orders, however, lies in the fact that they admit "singularities", which are excluded as long as only Dedekind domains with their "regular" localizations o_p arc considered. We will explain what this means in the next section.

In the preceding section we studied the localizations of a Dedekind domain o_K. They are extension rings of o_K which are integrally closed, yet no longer integral over Z, Now we study orders. They are subrings of o_K which are integral over Z, yet no longer integrally closed. As a common generalization of both types of rings let us consider for now all one-dimensional noetherian integral domains. These are the noetherian integral domains in which every prime ideal $p \neq \{\}$ is a maximal ideal. The term "one-dimensional" refers to the general definition of the Krull dimension of a ring as being the maximal length d of a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d$,

(12.2) Proposition. *An order of K is a one-dimensional noethcrian integral domain.*

Proof: Since o is a finitely generated Z-module of rank $n = [K : \mathbb{Q}]$, every ideal a is also a finitely generated Z-module, and *a fortiori* a finitely generated o-rnodulc. This shows that o is noetherian. If p $\neq$ 0 is a prime ideal and $a \in$ p $\cap$ Z, $a \neq 0$, then $ao \subseteq$ p $\subseteq$ o, i.e., p and o have the same rank n. Therefore o/p is a finite integral domain, hence a field, and thus p is a maximal ideal. □

In what follows, we always let a be a one-dimensional noethcrian integral domain and K its field of fractions. We sel out by proving the following s1ronger version of the Chinese remainder lhcorem.

(12.3) Proposition. *lfa #- 0 is an ideal oft), then*

o/a. ;:;: EB Oµ/uoµ = EB op/uop.
p p=>ll

Proof: Let ap = *o* n *aop.* For almost all p one has p £. *a* and therefore *aop* = Op, hence Clp = *o.* Furthermore, one has ll = np cip = np:::,a ap. Indeed, for any *a* E nv Op, the ideal b = {x E *o* I *xa* E o/ docs not belong to any of the maximal ideals p (in fact, one has *s*�*a* E o for any Sp '{- p). consequently, b = *o,* i.e., *a*= I *a* En, as claimed. (II.I) implies that, if p 2 *a,* then p is the only prime ideal containing iip- Therefore, given two distinct prime ideals):land q of *o,* the ideal ciµ+aq cannot he contained in any maximal ideal. whence Op+ iiq = *o.* The Chinese remainder theorem (3.6) now gives the isomorphism

o/a � EB o/iip,
p=>ll

and we have o/0₁₁= Op/noµ, because P = p mod Op is the only maximal -�� □

For the ring o, the fractional ideals of *o,* in other words, the finitely generated nonzero o-submodules of the field of fraclions *K,* no longer form a group - unless *o* happens to be Dedekind. The way out is to restrict attention to the **invertible ideals,** i.e., to those fractional ideals *a* of *o* for which there exists a fractional ideal *b* such that

ab= *o.*

These fonn an ahelian group, for trivial reasons. The inverse of a is still the fractional ideal

u-¹={xEKlxus;o},

because it is the biggest ideal such that uu-¹ <; *o.* The invertible ideals of *o* may be characterized as those fractional ideals whicl1 are "locally" principal:

(12.4) Proposition. *A* fractional *ideal a* of *o* is invertible if ,md *only* it: for every *prime* ideal).l *-1-* 0.

is a fractional principal ideal of Op.

Proof: Let $\mathfrak{a}$ be an invertible ideal and $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Then $1 = \sum a_i b_i$ with $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$, and not all $a_i b_i \in \mathcal{O}_\mathfrak{p}$ can lie in the maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Suppose $a_1 b_1$ is a unit in $\mathcal{O}_\mathfrak{p}$. Then $\mathfrak{a}_\mathfrak{p} = a_1\mathcal{O}_\mathfrak{p}$ because, for $x \in \mathfrak{a}_\mathfrak{p}$, $xb_1 \in \mathfrak{a}_\mathfrak{p}\mathfrak{b} = \mathcal{O}_\mathfrak{p}$, hence $x = xb_1(b_1a_1)^{-1}a_1 \in a_1\mathcal{O}_\mathfrak{p}$.

Conversely, assume $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ is a principal ideal $a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$, $a_\mathfrak{p} \in K^*$, for every $\mathfrak{p}$. Then we may and do assume that $a_\mathfrak{p} \in \mathfrak{a}$. We claim that the fractional ideal $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$ is an inverse for $\mathfrak{a}$. If this were not the case, then we would have a maximal ideal $\mathfrak{p}$ such that $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{p} \subsetneq \mathcal{O}$. Let $a_1, \dots, a_n$ be generators of $\mathfrak{a}$. As $a_i \in \mathfrak{a}\mathcal{O}_\mathfrak{p}$, we may write $a_i = a_\mathfrak{p}\frac{b_i}{s_i}$ with $b_i \in \mathcal{O}$, $s_i \in \mathcal{O} \setminus \mathfrak{p}$. Then $s_i a_i \in a_\mathfrak{p}\mathcal{O}$. Putting $s = s_1 \cdots s_n$, we have $sa_i \in a_\mathfrak{p}\mathcal{O}$ for $i = 1, \dots, n$, hence $sa_\mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathcal{O}$ and therefore $sa_\mathfrak{p}^{-1} \in \mathfrak{a}^{-1}$. Consequently, $s = sa_\mathfrak{p}^{-1}a_\mathfrak{p} \in \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{p}$, a contradiction. □

We denote the group of invertible ideals of $\mathcal{O}$ by $J(\mathcal{O})$. It contains the group $P(\mathcal{O})$ of fractional principal ideals $a\mathcal{O}$, $a \in K^*$.

(12.5) Definition. *The quotient group*

$$Pic(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$$

is called the Picard group of the ring $\mathcal{O}$.

In the case where $\mathcal{O}$ is a Dedekind domain, the Picard group is of course nothing but the ideal class group Cl_K. In general, we have the following description for $J(\mathcal{O})$ and $Pic(\mathcal{O})$.

(12.6) Proposition. *The correspondence $\mathfrak{a} \mapsto (\mathfrak{a}_\mathfrak{p})$ yields an isomorphism*

$$J(\mathcal{O}) \cong \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p}),$$

identifying the subgroup $P(\mathcal{O})$ with the image of $P(\mathcal{O})$ in the direct sum. One gets

$$Pic(\mathcal{O}) \cong \Big(\bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})\Big)/P(\mathcal{O}).$$

Proof: For every $\mathfrak{a} \in J(\mathcal{O})$, $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ is a principal ideal by (12.4), and we have $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ for almost all $\mathfrak{p}$ because $\mathfrak{a}$ lies in only finitely many maximal ideals $\mathfrak{p}$. We therefore obtain a homomorphism

./(o)-----,. EB P{op), n � (ap).
p

It is injective, for if $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p}$, then $\mathfrak{a} \subseteq \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} = \mathcal{O}$ (see the proof of (11.5)), and one has to have $\mathfrak{a} = \mathcal{O}$ because otherwise there would exist a maximal ideal $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p} \subsetneq \mathcal{O}$, i.e., $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_\mathfrak{p} \subsetneq \mathcal{O}_\mathfrak{p}$. In order to prove surjectivity, let $(a_\mathfrak{p}\mathcal{O}_\mathfrak{p}) \in \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})$ be given. Then the $\mathcal{O}$-submodule

$$\mathfrak{a} = \bigcap_\mathfrak{p} a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$$

of K is a fractional ideal. Indeed, since $a_\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ for almost all $\mathfrak{p}$, there is some $c \in \mathcal{O}$ such that $ca_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p}$, i.e., $c\mathfrak{a} \subseteq \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} = \mathcal{O}$. We have to show that one has

$$\mathfrak{a}\mathcal{O}_\mathfrak{p} = a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$$

for every $\mathfrak{p}$. The inclusion $\subseteq$ is trivial. In order to show that $a_\mathfrak{p}\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{a}\mathcal{O}_\mathfrak{p}$, let us choose $c \in \mathcal{O}$, $c \neq 0$, such that $ca_\mathfrak{p}^{-1}a_\mathfrak{q} \in \mathcal{O}_\mathfrak{q}$ for the finitely many $\mathfrak{q}$ which satisfy $a_\mathfrak{p}^{-1}a_\mathfrak{q} \notin \mathcal{O}_\mathfrak{q}$. By the Chinese remainder theorem (12.3), we may find $a \in \mathcal{O}$ such that

$$a \equiv c \bmod \mathfrak{p} \quad \text{and} \quad a \in ca_\mathfrak{p}^{-1}a_\mathfrak{q}\mathcal{O}_\mathfrak{q} \quad \text{for } \mathfrak{q} \neq \mathfrak{p}.$$

Then $\varepsilon = ac^{-1}$ is a unit in $\mathcal{O}_\mathfrak{p}$ and $a_\mathfrak{p}\varepsilon \in \bigcap_\mathfrak{q} a_\mathfrak{q}\mathcal{O}_\mathfrak{q} = \mathfrak{a}$, hence

$$a_\mathfrak{p}\mathcal{O}_\mathfrak{p} = (a_\mathfrak{p}\varepsilon)\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{a}\mathcal{O}_\mathfrak{p}. \qquad \square$$

Passing from the ring $\mathcal{O}$ to its **normalization** $\tilde{\mathcal{O}}$, i.e., to the integral closure of $\mathcal{O}$ in K, one obtains a Dedekind domain. This is not all that easy to prove, however, because $\tilde{\mathcal{O}}$ is in general not a finitely generated $\mathcal{O}$-module. But at any rate we have the

(12.7) Lemma. *Let $\mathcal{O}$ be a one-dimensional noetherian integral domain and $\tilde{\mathcal{O}}$ its normalization. Then, for each ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}$, the quotient $\tilde{\mathcal{O}}/\mathfrak{a}\tilde{\mathcal{O}}$ is a finitely generated $\mathcal{O}$-module.*

Proof: Let $a \in \mathfrak{a}$, $a \neq 0$. Then $\tilde{\mathcal{O}}/\mathfrak{a}\tilde{\mathcal{O}}$ is a quotient of $\tilde{\mathcal{O}}/a\tilde{\mathcal{O}}$. It thus suffices to show that $\tilde{\mathcal{O}}/a\tilde{\mathcal{O}}$ is a finitely generated $\mathcal{O}$-module. To this end, consider in $\mathcal{O}$ the descending chain of ideals containing $a\mathcal{O}$

$$\mathfrak{b}_m = (a^m\tilde{\mathcal{O}} \cap \mathcal{O}, a\mathcal{O}).$$

This chain becomes stationary. In fact, the prime ideals of the ring $\mathcal{O}/a\mathcal{O}$ are not only maximal but also minimal in the sense that $\mathcal{O}/a\mathcal{O}$ is a zero-dimensional noetherian ring. In such a ring every descending chain of ideals becomes stationary (see §3, exercise 7). If the chain $\bar{\mathfrak{b}}_m = \mathfrak{b}_m \bmod a\mathcal{O}$ is stationary at n, then so is the chain $\mathfrak{b}_m$. We show that, for this n, we have

$$\tilde{\mathcal{O}} \subseteq a^{-n}\mathcal{O} + a\tilde{\mathcal{O}}.$$

Lei /j $=$ i E 6, *h, c* E *o.* Apply the descending chain condition to the ring *0/<-·0* and lhe chain of ideals *(II"').* where *ii* $=$ *a* mod *co.* Then *(iih)* = (ah-1[1]), i.e., we !ind some .(e *o* such that *ah* :: .wh+[1] mod *l'O.* hence (l - *xa)ah Eco.* and therefore

$$f3 = \frac{h}{Z.(1-xa)} + fixa = di--,..-- \frac{h\,(1-xa)ah}{} + /Jxa\ Ea^{1,}\ o + aD.$$

Let *h* be lhe smallest positive integer such that *fJ* E *a-"o* + *ab.* It then suffices 10 show that *h* _::: *n.* Assume *h* > *n.* Writing

$$fi = � + mi \quad \text{with } u \in o,\ ii \in b,$$

we have *u* = *ah(/1 - aU)* E *a"O no�* a_{11}= tlh+l because *h* > *11,* hence *u* = *ah+tti' +au', u'* Et:, *ii'* E *0.* Substituting this into(*) gives

$$\beta = �_{a\,-} + a(1i+ii')\ Ea^{1}{}_{-}{}^{1}{}'o + a0.$$

This contn1dic1s the minimality of *h.* So we do have *b* £: *a "o* + *ai:J.*

0/aO thus becomes a submodule of the a-module (a ·*"o* + *aO)/aO* generated by *a-"* mod *aO.* h is 1hercforc itself a fini1ely genera1ed o-module. q.c.d. □

(12.8) Proposition *(KRULL-AK/7.UK!).* *Lero be* a one-dimCJJ/;ion.1/ *noetherian integrnl domain with held* of *{ractior1s K. Let* Ll *K be* a *Jinitc* exrcn.�ion *and()* the *imegr;iJ*clo.�ure of *o* in *L. Then O* is a Dedekind domain.

Proof: The far.:ts !hat *O* is inicgrally dosed and that every nonzero prime ideal is mnximal. arc deduced a.,; in (3.1). ll remains 10 show 1hat CJ is noe1hcrian. Let w_1·.. , *r,>,,* he a basis of *L*]K which is contained in *CJ.* Then the ring0_0 = orw$_1$· , *w,,*l is a finitely genemted o-mo<lule and in particular is noetherian since *o* is nocthcrian. We argue as before that CJ_0 is one-dimensional and are thus reduced to the case *L* = *K.* So lcl '21 be an ideal of CJ and *a* E Qt r *o, a ::f:.* 0: then hy the above lemma *OjuO* is a finitely generated o-mOOulc. Since *o* is noetherian, so is the o-submodule *Zi./aO.* and .ilso the 0-rnodulc Qt. D

Remark: The above proor is taken from *K,tl'L'\NSKY's* book 182J (see also 110 I I). 11 show1>al the same time 1h:.11proposition (8.1), which we had proved only in the 1.:a� of a separable extension *LIK,* is valid for general tinite extensions of the field of fractions of a Dedekind domain.

Next we want to compare the one-dimensional noetherian integral domain *o* with its nonnalization *6.* The fact that 8 is a Dedekind domain is evident and does not require the lengthy proof of (12.8) provided we make the following hypothesis:

(*) *o* is an integral domain whose normalization is a linitely generated o-modulc.

This condition will be assumed for all that follows. It avoids pathological situations and is satisfied in all interesting cases, in particular for the orders in an algebraic number field.

The groups of units and the Picard groups of *o* and *O* are compared with each other by the following

(12.9) Proposition. *One has the canonical exact sequence*

I ------+ ------+ *O** ------+ EB*o;;o;* ------+ *Pic(o)*------+ *Pic(O)* -------+ 1.
p

In the sum, p *varies over the prime ideals* -=*I*=- 0 of o *and* Op *denote.� the* integral *closure* of Op *in K.*

Proof: If j) varies over the prime ideals of 0, we know from (12.6) that

J(ol '"

If p is a prime ideal of *o,* then pO splits in the Dedekind domain into a product

$$\mathfrak{p}\bar{\mathcal{O}} = \bar{\mathfrak{p}}_1^{e_1} \cdots \bar{\mathfrak{p}}_r^{e_r},$$

i.e., there are only finitely many prime ideals of() above p. The same holds for the integral closure Op of Op, Since every nonzero prime ideal of Op has to lie above pop, the localization *Op* has only a finite number of prime ideals and is therefore a principal ideal domain (see S3, exercise 4). In view of (12.6), it follows that

P(Op) = *J* (Op) � EB P(Oµ)
p::::,p

and therefore

1 (o) '" EB EB P(o,J '" EB P(op).
P Pcc!P P

Observing that $P(R) \cong K^*/R^*$ for any integral domain R with field of fractions K, we obtain the commutative exact diagram

$$\begin{tikzcd}
1 \arrow[r] & K^*/\mathcal{O}^* \arrow[r] \arrow[d, "\alpha"] & \bigoplus K^*/\mathcal{O}_{\mathfrak{p}}^* \arrow[r] \arrow[d, "\beta"] & Pic(\mathcal{O}) \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & K^*/\tilde{\mathcal{O}}^* \arrow[r] & \bigoplus K^*/\tilde{\mathcal{O}}_{\mathfrak{p}}^* \arrow[r] & Pic(\tilde{\mathcal{O}}) \arrow[r] & 1.
\end{tikzcd}$$

For such a diagram one has in complete generality the well-known **snake lemma:** the diagram gives in a canonical way an exact sequence

$$1 \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\gamma)$$

$$\longrightarrow \operatorname{coker}(\alpha) \longrightarrow \operatorname{coker}(\beta) \longrightarrow \operatorname{coker}(\gamma) \longrightarrow 1$$

relating the kernels and cokernels of α, β, γ (see [23], chap. III, §3, lemma 3.3). In our particular case, α, β, and therefore also γ, are surjective, whereas

$$\ker(\alpha) = \tilde{\mathcal{O}}^*/\mathcal{O}^* \quad \text{and} \quad \ker(\beta) =$$

This then yields the exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \tilde{\mathcal{O}}^* \longrightarrow \qquad \longrightarrow Pic(\mathcal{O}) \longrightarrow Pic(\tilde{\mathcal{O}}) \longrightarrow 1. \qquad \square$$

A prime ideal $\mathfrak{p} \neq 0$ of $\mathcal{O}$ is called **regular** if $\mathcal{O}_{\mathfrak{p}}$ is integrally closed, and thus a discrete valuation ring. For the regular prime ideals, the summands in (12.9) are trivial. There are only finitely many non-regular prime of $\mathcal{O}$, namely the divisors of the **conductor** of $\mathcal{O}$. This is by definition the biggest ideal of $\tilde{\mathcal{O}}$ which is contained in $\mathcal{O}$, in other words,

$$\mathfrak{f} = \{a \in \tilde{\mathcal{O}} \mid a\tilde{\mathcal{O}} \subseteq \mathcal{O}\}.$$

Since $\tilde{\mathcal{O}}$ is a finitely generated $\mathcal{O}$-module, we have $\mathfrak{f} \neq 0$.

(12.10) Proposition. *For any prime ideal $\mathfrak{p} \neq 0$ of $\mathcal{O}$ one has*

$$\mathfrak{p} \nmid \mathfrak{f} \iff \mathfrak{p} \textit{ is regular.}$$

If this is the case, then $\mathfrak{P} = \mathfrak{p}\tilde{\mathcal{O}}$ is a prime ideal of $\tilde{\mathcal{O}}$ and $\mathcal{O}_{\mathfrak{p}} = \tilde{\mathcal{O}}_{\mathfrak{P}}$.

Proof: Assume $\mathfrak{p} \nmid \mathfrak{f}$, i.e., $\mathfrak{p} \not\supseteq \mathfrak{f}$, and let $t \in \mathfrak{f} \setminus \mathfrak{p}$. Then $t\tilde{\mathcal{O}} \subseteq \mathcal{O}$, hence $\tilde{\mathcal{O}} \subseteq \frac{1}{t}\mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$. If $\mathfrak{m} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_\mathfrak{p}$ then, putting $\mathfrak{P} = \mathfrak{m} \cap \tilde{\mathcal{O}}$, $\mathfrak{P}$ is a prime ideal of $\tilde{\mathcal{O}}$ such that $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathcal{O}$, hence $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$ because $\mathfrak{p}$ is maximal. Trivially, $\mathcal{O}_\mathfrak{p} \subseteq \tilde{\mathcal{O}}_\mathfrak{P}$, and if conversely $\frac{b}{s} \in \tilde{\mathcal{O}}_\mathfrak{P}$ for $b \in \tilde{\mathcal{O}}$, $s \in \tilde{\mathcal{O}} \setminus \mathfrak{P}$, then $tb \in \mathcal{O}$ and $ts \in \mathcal{O} \setminus \mathfrak{p}$, hence $\frac{b}{s} = \frac{tb}{ts} \in \mathcal{O}_\mathfrak{p}$. Therefore $\mathcal{O}_\mathfrak{p} = \tilde{\mathcal{O}}_\mathfrak{P}$. Thus, by (11.5), $\mathcal{O}_\mathfrak{p}$ is a valuation ring, i.e., $\mathfrak{p}$ is regular.

One has furthermore that $\mathfrak{P} = \mathfrak{p}\tilde{\mathcal{O}}$. In fact, $\mathfrak{P}$ is the only prime ideal of $\tilde{\mathcal{O}}$ above $\mathfrak{p}$. For if $\mathfrak{q}$ is another one, then $\tilde{\mathcal{O}}_\mathfrak{P} = \mathcal{O}_\mathfrak{p} \subseteq \tilde{\mathcal{O}}_\mathfrak{q}$, and therefore

$$\mathfrak{P} = \tilde{\mathcal{O}} \cap \mathfrak{P}\tilde{\mathcal{O}}_\mathfrak{P} \supseteq \tilde{\mathcal{O}} \cap \mathfrak{q}\tilde{\mathcal{O}}_\mathfrak{q} = \mathfrak{q},$$

hence $\mathfrak{P} = \mathfrak{q}$. Consequently, $\mathfrak{p}\tilde{\mathcal{O}} = \mathfrak{P}^e$, with $e \geq 1$, and furthermore $\mathfrak{m} = \mathfrak{p}\mathcal{O}_\mathfrak{p} = (\mathfrak{p}\tilde{\mathcal{O}})\mathcal{O}_\mathfrak{p} = \mathfrak{P}^e\mathcal{O}_\mathfrak{p} = \mathfrak{m}^e$, i.e., $e = 1$ and thus $\mathfrak{P} = \mathfrak{p}\tilde{\mathcal{O}}$.

Conversely, assume $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring. Being a principal ideal domain, it is integrally closed, and since $\tilde{\mathcal{O}}$ is integral over $\mathcal{O}$, hence *a fortiori* over $\mathcal{O}_\mathfrak{p}$, we have $\tilde{\mathcal{O}} \subseteq \mathcal{O}_\mathfrak{p}$. Let $x_1, \dots, x_n$ be a system of generators of the $\mathcal{O}$-module $\tilde{\mathcal{O}}$. We may write $x_i = \frac{a_i}{s_i}$ with $a_i \in \mathcal{O}$, $s_i \in \mathcal{O} \setminus \mathfrak{p}$. Setting $s = s_1 \cdots s_n \in \mathcal{O} \setminus \mathfrak{p}$, we find $sx_i \in \mathcal{O}$ and therefore $s\tilde{\mathcal{O}} \subseteq \mathcal{O}$, i.e., $s \in \mathfrak{f} \setminus \mathfrak{p}$. It follows that $\mathfrak{p} \nmid \mathfrak{f}$. $\square$

We now obtain the following simple description for the sum $\bigoplus_\mathfrak{p} \tilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$ in (12.9).

(12.11) Proposition. $\bigoplus_\mathfrak{p} \tilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* \cong (\tilde{\mathcal{O}}/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^*$.

Proof: We apply the Chinese remainder theorem (12.3) repeatedly. We have

$$(1) \qquad \mathcal{O}/\mathfrak{f} \cong \bigoplus_\mathfrak{p} \mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p}.$$

The integral closure $\tilde{\mathcal{O}}_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ possesses only the finitely many prime ideals that lie above $\mathfrak{p}\mathcal{O}_\mathfrak{p}$. They give the localizations $\tilde{\mathcal{O}}_\mathfrak{P}$, where $\mathfrak{P}$ varies over the prime ideals above $\mathfrak{p}$ of the ring $\tilde{\mathcal{O}}$. At the same time $\tilde{\mathcal{O}}_\mathfrak{p}$ is the localization of $\tilde{\mathcal{O}}$ with respect to the multiplicative subset $\mathcal{O} \setminus \mathfrak{p}$. Since $\mathfrak{f}$ is an ideal of $\tilde{\mathcal{O}}$, it follows that $\mathfrak{f}\mathcal{O}_\mathfrak{p} = \mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p}$. The Chinese remainder theorem yields

$$\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p} \cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} \tilde{\mathcal{O}}_\mathfrak{P}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{P}$$

and

$$(2) \qquad \tilde{\mathcal{O}}/\mathfrak{f} \cong \bigoplus_\mathfrak{p} \bigoplus_{\mathfrak{P}|\mathfrak{p}} \tilde{\mathcal{O}}_\mathfrak{P}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{P}.$$

Passing to unit groups, we get from (1) and (2) that

$$(3)\qquad (\tilde{\mathcal{O}}/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^* \cong \bigoplus_{\mathfrak{p}} (\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p})^*$$

For $\mathfrak{f} \subseteq \mathfrak{p}$ we now consider the homomorphism

$$\varphi : \tilde{\mathcal{O}}_\mathfrak{p}^* \to (\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p})^*$$

It is surjective. In fact, if $\varepsilon \bmod \mathfrak{f}$ is a unit in $\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p}$, then ε is a unit in $\tilde{\mathcal{O}}_\mathfrak{p}$. This is so because the units in any ring are precisely those elements that are not contained in any maximal ideal, and the preimages of the maximal ideals of $\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p}$ give precisely all the maximal ideals of $\tilde{\mathcal{O}}_\mathfrak{p}$, since $\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p} \subseteq \mathfrak{p}\tilde{\mathcal{O}}_\mathfrak{p}$. The kernel of φ is a subgroup of which is contained in $\mathcal{O}_\mathfrak{p}$, and which contains $\mathcal{O}_\mathfrak{p}^*$. It is therefore equal to We now conclude that

$$\tilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* \cong (\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p})^*.$$

This remains true also for $\mathfrak{p} \not\supseteq \mathfrak{f}$ because then both sides are equal to 1 according to (12.10). The claim of the proposition now follows from (3). □

Our study of one-dimensional noetherian integral domains was motivated by the consideration of *orders*. For them, (12.9) and (12.11) imply the following generalization of Dirichlet's unit theorem and of the theorem on the finiteness of the class group.

(12.12) Theorem. *Let $\mathcal{O}$ be an order in an algebraic number field K, $\mathcal{O}_K$ the maximal order, and $\mathfrak{f}$ the conductor of $\mathcal{O}$.*

Then the groups $\mathcal{O}_K^*/\mathcal{O}^*$ and $Pic(\mathcal{O})$ are finite and one has

$$\# Pic(\mathcal{O}) = \frac{h_K}{(\mathcal{O}_K^* : \mathcal{O}^*)} \frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*},$$

where h_K is the class number of K. In particular, one has that

$$\operatorname{rank}(\mathcal{O}^*) = \operatorname{rank}(\mathcal{O}_K^*) = r + s - 1.$$

Proof: By (12.9) and (12.11), and since $Pic(\mathcal{O}_K) = Cl_K$, we have the exact sequence

$$1 \longrightarrow \mathcal{O}_K^*/\mathcal{O}^* \longrightarrow (\mathcal{O}_K/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^* \longrightarrow Pic(\mathcal{O}) \longrightarrow Cl_K \longrightarrow 1.$$

This gives the claim. □

The delinition of the Picard group of a one-dimensional noetherian integral domain *o* avoids the problem of the uniqueness of prime ideal decomposition by restricting allcntion to the invertible ideals, and thus leaving aside the information carried by noninvcrtibles. But there is another important generalization of the ideal class group which docs take inLo account *all* prime ideals of *o*. It is based on an artificial re-introduction of the uniqueness of *prime decompmition. Thi.*� group *i.*� called the divisor class group, *or* Chow group of *o*. Its definition starts from the free abelian group

$$o;v(V) = \mathrm{EB}_{p}\ Zp$$

on the *set* of all maximal ideals *p* of *o* (i.e., the set of all prime ideals � 0). This group is called the divisor group of *o*. Its elements are fonnal sums

$$D = \mathrm{I:}_{p} n,p$$

with np E Z and flp = *0* for almOSl all *p*, called divisors (or 0-cycles). Corollary (3.9) simply says that, in the case of a Dedekind domain, the divisor group *Div(o)* and the group of ideals are canonically isomorphic. The additive notation and the name of the group stem from function theory where divisors for analytic functions play the *same* role as ideals do for algebraic numbers (sec chap. Ill, *3).

In order to define lhe divisor class group we have to associate to every /" *EK*� a "principal divisor" div(/). We use the case of a Dedekind domain to guide us. There the principal ideal (_/") was given by

$$<n = \prod_{p} p^{"\bullet"0}.$$

where $v_p : K^*$ � ::Z is the p-adic exponential valuation associated to the valuation ring O_p. In general, o_p is not anymore a discrete valualion ring. Nevertheless, o_p defines a homomorphism

$$\mathrm{ordp}: K^* \ \text{�}\ ::Z$$

which generalizes the valuation function. If $f = a/h \in K^*$, with $a, h \in o$, then we put

$$\mathrm{ordp}(f) = f''v(op/aop) \ \text{�}\ foP(op/hop).$$

where denotes the length of an Op-module *M*, i.e., the maximal length strictly decreasing chain

$$M = Mo \ \text{�}\ M1 ;1 \cdot\ 1\ Mt = 0$$

of all-submodules. In the special case where Oµ is a discrete valuation ring with maximal ideal m, the value $v = v_{p(a)}$ of $a \in$ Op, for *a -f* 0, is given by the equation

$$aOp=rn".$$

It is equal to the lcnglh of the Op-module op/mv, because the longest chain of submodules is

$$\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}^{\nu} \supset \mathfrak{m}/\mathfrak{m}^{\nu} \supset \cdots \supset \mathfrak{m}^{\nu}/\mathfrak{m}^{\nu} = (0).$$

Thus the function ordp agrees with the ex1xmential valuation Vp in this case.

The property of the function ordp to be a homomorphism follows from the fact (which is easily proved) that the length function $t_{o''}$ is multiplicative on short exact sequences of Op-mlXlules.

Using the functions ordp : K^* ---+ Z, we can now associate to every element f E K^* the divisor

div(f) � Locd,(f)p,

and thus obtain a canonical homomorphism

div: K'' -----+ Div(o).

The elements div(f) are called principal divisors. They fonn a subgroup P(o) of Div(o). Two divisors *lJ* and *D'* which differ only by a principal divisor arc called rationally equivalent.

(12.13) Definition. *The quotient group*

$$CH^1(o) = Div(o)/P(o)$$

is called *the* divisor class group or Chow group *of o*.

The Chow group is related to the Picard group by a canonical homomorphism

div: *Pic(o)*-----+ CI/^{1}(o)

which is defined as follows. If *a* is an invertible ideal, then, by (12.4), aOp- for any prime ideal i-, -/- 0, is a principal ideal apOp, ap EK*, and we put

div(a) = L- ordp(ap)):l.
p

This gives us a homomorphism

div: J(o) ----- + *Div(o)*

of the ideal group *J* (o) which takes principal ideals into principal divisors, and therefore induces a homomorphism

div : *Pic(o)* -----+ *CH* ^{1}(o).

In the special case of a Dedekind domain we obtain:

(12.14) Proposition. *If o is a Dedekind domain. rhen*

$$\text{div}: Pic(o)\text{-},,,. \ Cl/^1(o)$$

is *:m isomorphi�m.*

fi:xerclse 1. Show thal

$$CfX.YJ/(XY - X\}. \quad C[X, YJ/(XY - !).$$

$$CIX.Y)/(X^2-Y^3). \quad C[X,YI/(Y^1-X^1-X^1)$$

areonc-rlimem,ional noeJheriim rings. *Which* one.� are integral domain'-'-' DeJr.rn1ine their nmmali7.alions.

Hint: For instance in the fast ell.ample, put I= X/Y and show that the homomorphism $C\{X. Y/$----,. c,,,. ,\'I-+$(^2$ - /,YI-+ $f(t^1$ - /), ha.� kernel $(Y^1 - X^2 - X\cdot')$.

Exercise 2, Let a am.I b be positive integers that arc not perfect squares. Show that \he fundamental unit of the order Z + Z ./a of the tield Q(./a) is also the fundamental unit of the order 'J'. + Z-/a + Z-.,Ch + Z,/a� in the field Q(./a,�).

Exercise 3. Le1 K be a number field of degree n = IK : QI. A complete module in K is a subgroup of the fom1

$$M = Za1+\cdots + Zt.t�.$$

where a_1 ....- a,. arc linearly independent elements of K. Show that 1he ring of mulriplicn.

$$\mathcal{O} = \{\alpha \in K \mid \alpha M \subseteq M\}$$

is an onler in K. bo1 in general not the maxima! order.

Exercise 4. Determine the ring of nrnltiplierj; o of 1hc complete module M = Z + z./2 inQ(,/2). Show that t = ! + ./2 is a fum.hunemul uni1 of o. Dct..:rminc .ill integer solutions of ..Pell'$ equation··

$$x^2 - 2/ = 7.$$

Hint: $N(x + y./2) = x^1 - 2y^2$, $N(3 + ,/2) = N('5 + 3,/2) = 7$.

Exencise 5. In a one-dimensional noetherian integral domain lhe regular prime ideals ,f. 0 are precisely lhe inv1:rtihlc prime ideals.

§ lJ. One-dimensional Schemes

The first approach to the theory of algebraic number fields is dominated by the methods of arithmetic and algebra. But the theory may also be treated fundamemally from a geometric point of view. which will bring out novel *a�pects* in *a* variety of way�. This geometric interpretation hinges on the possibility of viewing numbers a� functions on a topologkal space.

In order to explain this, let us start from polynomials

$$f(x) = a_n x^n + \cdots + a_0$$

with complex coefficients $a_i \in \mathbb{C}$, which may be immediately interpreted as functions on the complex plane. This property may be formulated in a purely algebraic way as follows. Let $a \in \mathbb{C}$ be a point in the complex plane. The set of all functions $f(x)$ in the polynomial ring $\mathbb{C}[x]$ which vanish at the point a forms the maximal ideal $\mathfrak{p} = (x - a)$ of $\mathbb{C}[x]$. In this way the points of the complex plane correspond 1-1 to the maximal ideals of $\mathbb{C}[x]$. We denote the set of all these maximal ideals by

$$M = \operatorname{Max}(\mathbb{C}[x]).$$

We may view M as a new kind of space and may interpret the elements $f(x)$ of the ring $\mathbb{C}[x]$ as functions on M as follows. For every point $\mathfrak{p} = (x - a)$ of M we have the canonical isomorphism

$$\mathbb{C}[x]/\mathfrak{p} \xrightarrow{\sim} \mathbb{C},$$

which sends the residue class $f(x) \bmod \mathfrak{p}$ to $f(a)$. We may thus view this residue class

$$f(\mathfrak{p}) := f(x) \bmod \mathfrak{p} \in \kappa(\mathfrak{p})$$

in the residue class field $\kappa(\mathfrak{p}) = \mathbb{C}[x]/\mathfrak{p}$ as the "value" of f at the point $\mathfrak{p} \in M$. The topology on $\mathbb{C}$ cannot be transferred to M by algebraic means. All that can be salvaged algebraically are the point sets defined by equations of the form

$$f(x) = 0$$

(i.e., only the finite sets and M itself). These sets are defined to be the closed subsets. In the new formulation they are the sets

$$V(f) = \{\mathfrak{p} \in M \mid f(\mathfrak{p}) = 0\} = \{\mathfrak{p} \in M \mid \mathfrak{p} \supseteq (f(x))\}.$$

The algebraic interpretation of functions given above leads to the following geometric perception of completely general rings. For an arbitrary ring $\mathfrak{o}$, one introduces the spectrum

$$X = \operatorname{Spec}(\mathfrak{o})$$

as being the set of all prime ideals $\mathfrak{p}$ of $\mathfrak{o}$. The Zariski topology on X is defined by stipulating that the sets

$$V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{p} \supseteq \mathfrak{a}\}$$

be the closed sets, where $\mathfrak{a}$ varies over the ideals of $\mathfrak{o}$. This does make X into a topological space (observe that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$) which, however, is usually not Hausdorff. The closed points correspond to the maximal ideals of $\mathfrak{o}$.

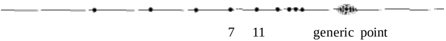
The elements $f \in \mathcal{O}$ now play the rôle of functions on the topological space X: the "value" of f at the point $\mathfrak{p}$ is defined to be

$$f(\mathfrak{p}) := f \bmod \mathfrak{p}$$

and is an element of the residue class field $\kappa(\mathfrak{p})$, i.e., in the field of fractions of $\mathcal{O}/\mathfrak{p}$. So the values of f do not in general lie in a single field.

Admitting also the non-maximal prime ideals as non-closed points, turns out to be extremely useful – and has an intuitive reason as well. For instance in the case of the ring $\mathcal{O} = \mathbb{C}[x]$, the point $\mathfrak{p} = (0)$ has residue class field $\kappa(\mathfrak{p}) = \mathbb{C}(x)$. The "value" of a polynomial $f \in \mathbb{C}[x]$ at this point is $f(x)$ itself, viewed as an element of $\mathbb{C}(x)$. This element should be thought of as the value of f at the **unknown** place x – which one may imagine to be everywhere or nowhere at all. This intuition complies with the fact that the closure of the point $\mathfrak{p} = (0)$ in the Zariski topology of X is the total space X. This is why $\mathfrak{p}$ is also called the **generic point** of X.

Example: The space $X = \mathrm{Spec}(\mathbb{Z})$ may be represented by a line.



For every prime number one has a closed point, and there is also the generic point (0), the closure of which is the total space X. The nonempty open sets in X are obtained by throwing out finitely many prime numbers $p_1, \dots, p_n$. The integers $a \in \mathbb{Z}$ are viewed as functions on X by defining the value of a at the point (p) to be the residue class

$$a(p) = a \bmod p \in \mathbb{Z}/p\mathbb{Z}.$$

The fields of values are then

$$\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/7\mathbb{Z},\ \mathbb{Z}/11\mathbb{Z},\ \dots, \mathbb{Q}.$$

Thus every prime field occurs exactly once.

An important refinement of the geometric interpretation of elements of the ring $\mathcal{O}$ as functions on the space $X = \mathrm{Spec}(\mathcal{O})$ is obtained by forming the **structure sheaf** $\mathcal{O}_X$. This means the following. Let $U \neq \emptyset$ be an open subset of X. If $\mathcal{O}$ is a one-dimensional integral domain, then the ring of "regular functions" on U is given by

$$\mathcal{O}(U) = \left\{ \frac{f}{g} \;\middle|\; g(\mathfrak{p}) \neq 0 \text{ for all } \mathfrak{p} \in U \right\}.$$

in other words, it is the localization of o with respect to the multiplicative set $S = o \setminus \bigcup_{p \in U} p$ (see §11). In the general case, $o(U)$ is defined to consist of all elements

$$s = (s_p) \in \prod_{p \in U} o_p$$

which locally are quotients of two elements of o. More precisely, this means that for every $p \in U$, there exists a neighbourhood $V \subseteq U$ of p, and elements $f, g \in o$ such that, for each $q \in V$, one has $g(q) \neq 0$ and $s_q = f/g$ in o_q. These quotients have to be understood in the more general sense of commutative algebra (see §11, exercise 1). We leave it to the reader to check that one gets back the above definition in the case of a one-dimensional integral domain o.

If $V \subseteq U$ are two open sets of X, then the projection

$$\prod_{p \in U} o_p \longrightarrow \prod_{p \in V} o_p$$

induces a homomorphism

$$\rho_{UV} : o(U) \longrightarrow o(V),$$

called the restriction from U to V. The system of rings $o(U)$ and mappings ρ_{UV} is a sheaf on X. This notion means the following.

(13.1) Definition. *Let X be a topological space. A presheaf $\mathcal{F}$ of abelian groups (rings, etc.) consists of the following data.*

(1) *For every open set U, an abelian group (a ring, etc.) $\mathcal{F}(U)$ is given.*

(2) *For every inclusion $U \subseteq V$, a homomorphism $\rho_{UV} : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ is given, which is called restriction.*

These data are subject to the following conditions:

(a) $\mathcal{F}(\emptyset) = 0$,

(b) ρ_{UU} *is the identity* $\mathrm{id}: \mathcal{F}(U) \longrightarrow \mathcal{F}(U)$,

(c) $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$, *for open sets* $W \subseteq V \subseteq U$.

The elements $s \in \mathcal{F}(U)$ are called the sections of the presheaf $\mathcal{F}$ over U. If $V \subseteq U$, then one usually writes $= s|_V$. The definition of a presheaf can be reformulated most in the language of categories. The open sets of the topological space X form a category X_{top} in which only inclusions are admitted as morphisms. A presheaf of abelian groups (rings) is then simply a contravariant functor

$$\mathcal{F}: X_{top} \longrightarrow (ab), \ (rings)$$

into the category of abelian groups (resp. rings) such that $\mathcal{F}(\emptyset) = 0$.

(13.2) Definition. *A presheaf $\mathcal{F}$ on the topological space X is called a sheaf if, for all open coverings $\{U_i\}$ of the open sets U, one has:*

(i) *If $s, s' \in \mathcal{F}(U)$ are two sections such that $s|_{U_i} = s'|_{U_i}$ for all i, then $s = s'$.*

(ii) *If $s_i \in \mathcal{F}(U_i)$ is a family of sections such that*

$$s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$$

for all i, j, then there exists a section $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$ for all i.

The stalk of the sheaf $\mathcal{F}$ at the point $x \in X$ is defined to be the direct limit (see chap. IV, §2)

$$\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U),$$

where U varies over all open neighbourhoods of x. In other words, two sections $s_U \in \mathcal{F}(U)$ and $s_V \in \mathcal{F}(V)$ are called equivalent in the disjoint union $\dot{\bigcup}_{U \ni x} \mathcal{F}(U)$ if there exists a neighbourhood $W \subseteq U \cap V$ of x such that $s_U|_W = s_V|_W$. The equivalence classes are called germs of sections at x. They are the elements of $\mathcal{F}_x$.

We now return to the spectrum $X = \operatorname{Spec}(\mathcal{o})$ of a ring $\mathcal{o}$ and obtain the

(13.3) Proposition. *The rings $\mathcal{o}(U)$, together with the restriction mappings ρ_{UV}, form a sheaf on X. It is denoted by $\mathcal{O}_X$ and called the structure sheaf on X. The stalk of $\mathcal{O}_X$ at the point $\mathfrak{p} \in X$ is the localization $\mathcal{o}_{\mathfrak{p}}$, i.e., $\mathcal{O}_{X,\mathfrak{p}} \cong \mathcal{o}_{\mathfrak{p}}$.*

The proof of this proposition follows immediately from the definitions. The couple $(X, \mathcal{O}_X)$ is called an affine scheme. Usually, however, the structure sheaf $\mathcal{O}_X$ is dropped from the notation. Now let

$$\varphi : \mathcal{o} \longrightarrow \mathcal{o}'$$

be a homomorphism of rings and $X = \operatorname{Spec}(\mathcal{o})$, $X' = \operatorname{Spec}(\mathcal{o}')$. Then φ induces a continuous map

$$f : X' \longrightarrow X, \quad f(\mathfrak{p}') := \varphi^{-1}(\mathfrak{p}'),$$

and, for every open subset U of X, a homomorphism

$$f_U^\# : \mathcal{o}(U) \longrightarrow \mathcal{o}'(U'), \quad s \longmapsto s \circ f|_{U'},$$

where $U' = f^{-1}(U)$. The maps $f_U^\#$ have the following two properties.

a) If $V \subseteq U$ are open sets, then the diagram

$$\begin{tikzcd} \mathcal{O}(U) \arrow[r, "f_U"] \arrow[d, "r"] & \mathcal{O}'(U') \arrow[d, "r"] \\ \mathcal{O}(V) \arrow[r, "f_V"] & \mathcal{O}'(V') \end{tikzcd}$$

is commutative.

b) for $\mathfrak{p}' \in U' \subseteq X'$ and $a \in \mathcal{O}(U)$ one has

$$a(f(\mathfrak{p}')) = 0 \implies f_U(a)(\mathfrak{p}') = 0.$$

A continuous map $f : X' \to X$ together with a family of homomorphisms $f_U : \mathcal{O}(U) \to \mathcal{O}'(U')$ which satisfy conditions a) and b) is called a **morphism** from the scheme X' to the scheme X. When referring to such a morphism, the maps f_U are usually not written explicitly. One can show that every morphism between two affine schemes $X' = \operatorname{Spec}(o')$ and $X = \operatorname{Spec}(o)$ is induced in the way described above by a ring homomorphism $\varphi : o \to o'$.

The proofs of the above claims are easy, although some of them are a bit lengthy. The notion of scheme is the basis of a very extensive theory which occupies a central place in mathematics. As introductions into this important discipline let us recommend the books [51] and [104].

We will now confine ourselves to considering noetherian integral domains o of dimension ≤ 1, and propose to illustrate geometrically, via the scheme-theoretic interpretation, some of the facts treated in previous sections.

1. Fields. If K is a field, then the scheme $\operatorname{Spec}(K)$ consists of a single point (0) on top of which the field itself sits as the structure sheaf. One must not think that these one-point schemes are all the same because they differ essentially in their structure sheaves.

2. Valuation rings. If o is a discrete valuation ring with maximal ideal $\mathfrak{p}$, then the scheme $X = \operatorname{Spec}(o)$ consists of two points, the closed point $x = \mathfrak{p}$ with residue class field $\kappa(\mathfrak{p}) = o/\mathfrak{p}$, and the generic point $\eta = (0)$ with residue class field $\kappa(\eta) = K$, the field of fractions of o. One should think of X as a point x with an infinitesimal neighbourhood described by the generic point η:

X:

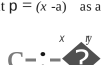
This intuition is justified by the following observation.

The discrete valuarion rings arise as localizations

$$o,\text{?}[f \mid J.geo,\ g(p),601$$

of Dedekind domains o. There is no neighbourhood of p in $X =$ Spcc(o) on which *all* fum:1ion.'i f E o_p *are* defined becau.?e, if o is not a local ring. we find by the Chinese remainder theorem for every point q "# p, q :t,. 0,. an element g e o satisfying g ::::. 0 mod q and >: :;;;; I mo<l p. Then } e Op as a function is nol defined at q. But every element { E Op is defined on a sufficii::ntly small neighbourhood; hence one may say that all clements f of the discrete valuation ring Op are like functions defined on a "germ" of neighbourhoods of p. Thus Spcc(o,,) may be thoughl of as such a "germ of neighbourhoods" of p.

We want 10 point out a small discrepancy of intuitions. Considering the spectrum of 1he one-dimensional ring C[x], the points of which constitute the complex:plane, we will not want to visualize the infinitesimal neighbourhood X,, = Spcc(Cfxfp) ofa point p = (x -a) as a small fine segment, but rather as a little disc:



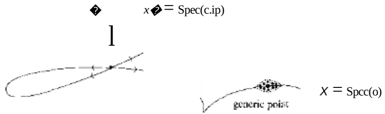
This two-dimensional nature is actually inherent in all discrete valuation rings with algebraically closed residue field. But the algebraic jus1itica1ion of this imuition is provided only by the introduction of a new 1opology, the etale topology, which is much finer than the Zariski topology (sec 11031. {f32!).

3. Dedekind *rings.* The spectrum $X =$ *Spcc(o)* of" Dedekind domain o is visualized as a smooth curve. At each poilll p one may consider the locali1.ation o_p. The inclusion $o \to o_p$ induces a morphism

$$f : X_{\mathfrak p} = \operatorname{Spec}(\mathcal{O}_{\mathfrak p}) \longrightarrow X\,,$$

which extracts the scheme $X_{\mathfrak p}$ from X as an "infinitesimal neighbourhood" of p:

4. Singularities. We now consider a one-dimensional noclherian integral domain o which is not a Dedekind domain, *e.u.*, an order in an algebraic number field which is different from the maximal order. Again we view the scheme $X = \mathrm{Spec}(o)$ as a curve, Bul now the curve will not be everywhere smooth, but will have singularities at certain points.

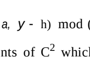


These arc precisely the nongeneric points p for which the localization o_p is no longer a discrete valuation ring, that is to say, the maximal ideal pop is not generated by a single element. For example, in the one-dimensional ring $o = C[x.y]/(y^2 - x^3)$, the closed points of the scheme X are given by the prime ideals

$$)l == (x - a, y - h) \bmod (y^2, -C^1)$$

where (a, h) varies over the points of C^2 which satisfy the equation

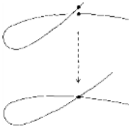
$$h^2 - a^3 = 0.$$



The only singular point is the origin. Jt corresponds to the maximal ideal)lo= (X, Y), where $X = x \bmod (/- - x')$, $Y = y \bmod (y^1 - x^3)$ E o. The maximal ideal)loOp$_0$ of the local ring is generated by the elements $X, y,$ and cannot be generated by a single element.

5. Normalization. Passing to the nomialization O of a one-dimensional noetherian integral domain o means, in geometric terms, taking the *resolution* of the singularities !hat were just discussed. Indeed, if $X = \mathrm{Spec}(o)$ and

$\tilde{X} = \operatorname{Spec}(\tilde{\mathcal{O}})$, then the inclusion $\mathcal{O} \hookrightarrow \tilde{\mathcal{O}}$ induces a morphism $f: \tilde{X} \to X$.



$\tilde{X}$

X

Since $\tilde{\mathcal{O}}$ is a Dedekind domain, the scheme $\tilde{X}$ is to be considered as smooth. If $\mathfrak{p}\tilde{\mathcal{O}} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ is the prime factorization of $\mathfrak{p}$ in $\tilde{\mathcal{O}}$, then $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are the different points of $\tilde{X}$ that are mapped to $\mathfrak{p}$ by f. One can show that $\mathfrak{p}$ is a regular point of X – in the sense that $\mathcal{O}_{\mathfrak{p}}$ is a discrete valuation ring – if and only if $r = 1$, $e_1 = 1$ and $f_1 = (\tilde{\mathcal{O}}/\mathfrak{P}_1 : \mathcal{O}/\mathfrak{p}) = 1$.

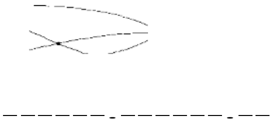
6. Extensions. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Let $L|K$ be a finite separable extension, and $\mathcal{O}$ the integral closure of $\mathcal{O}$ in L. Let $Y = \operatorname{Spec}(\mathcal{O})$, $X = \operatorname{Spec}(\mathcal{O})$, and

$$f: X \to Y$$

the morphism induced by the inclusion $\mathcal{O} \hookrightarrow \mathcal{O}$. If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$ and

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

the prime decomposition of $\mathfrak{p}$ in $\mathcal{O}$, then $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are the different points of X which are mapped to $\mathfrak{p}$ by f. The morphism f is a "ramified covering." It is graphically represented by the following picture:



X

Y

ramified points

This picture, however, is a fair rendering of the algebraic situation only in the case where the residue class fields of $\mathcal{O}$ are algebraically closed (like for the ring $\mathbb{C}[x]$). Then, from the fundamental identity $\sum_i e_i f_i = n$, there are exactly $n = [L:K]$ points $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ of X lying above each point $\mathfrak{p}$ of Y, except when $\mathfrak{p}$ is ramified in $\mathcal{O}$. At a point $\mathfrak{p}$ of ramification, several of the points $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ coalesce. This also explains the terminology of ideals that "ramify."

If $L|K$ is Galois with Galois group $G = G(L|K)$, then every automorphism $\sigma \in G$ induces via $\sigma : \mathcal{O} \to \mathcal{O}$ an automorphism of schemes $\sigma : X \to X$. Since the ring $\mathfrak{o}$ is fixed, the diagram

$$\begin{tikzcd} X \arrow[rr, "\sigma"] \arrow[dr] & & X \arrow[dl] \\ & Y & \end{tikzcd}$$

is commutative. Such an automorphism is called a covering transformation of the ramified covering X/Y. The group of covering transformations is denoted by $\operatorname{Aut}_Y(X)$. We thus have a canonical isomorphism

$$G(L|K) \cong \operatorname{Aut}_Y(X).$$

In chap. II, §7, we will see that the composite of two unramified extensions of K is again unramified. The composite $\tilde{K}$, taken inside some algebraic closure $\bar{K}$ of K, of *all* unramified extensions $L|K$ is called the maximal unramified extension of K. The integral closure $\tilde{\mathcal{O}}$ of $\mathfrak{o}$ in $\tilde{K}$ is still a one-dimensional integral domain, but in general no longer noetherian, and, as a rule, there will be infinitely many prime ideals lying above a given prime ideal $\mathfrak{p} \neq 0$ of $\mathfrak{o}$. The scheme $\tilde{Y} = \operatorname{Spec}(\tilde{\mathcal{O}})$ with the morphism

$$f : \tilde{Y} \to Y$$

is called the universal covering of Y. It plays the same rôle for schemes that the universal covering space $\tilde{X} \to X$ of a topological space plays in topology. There the group of covering transformations $\operatorname{Aut}_X(\tilde{X})$ is canonically isomorphic to the fundamental group $\pi_1(X)$. Therefore we define in our present context the fundamental group of the scheme Y by

$$\pi_1(Y) = \operatorname{Aut}_Y(\tilde{Y}) = G(\tilde{K}|K).$$

This establishes a first link of Galois theory with classical topology. This link is pursued much further in etale topology.

The geometric point of view of algebraic number fields explained in this section is corroborated very convincingly by the theory of function fields of algebraic curves over a finite field $\mathbb{F}_p$. In fact, a very close analogy exists between both theories.

§ 14. Function Fields

We conclude this chapter with a brief sketch of the theory of **function fields.** They represent a striking analogy with algebraic number fields, and since they are immediately related to geometry, they actually serve as an important model for the theory of algebraic number fields.

The ring $\mathbb{Z}$ of integers with its field of fractions $\mathbb{Q}$ exhibits obvious analogies with the polynomial ring $\mathbb{F}_p[t]$ over the field $\mathbb{F}_p$ with p elements and its field of fractions $\mathbb{F}_p(t)$. Like $\mathbb{Z}$, $\mathbb{F}_p[t]$ is also a principal ideal domain. The prime numbers correspond to the monic irreducible polynomials $p(t) \in \mathbb{F}_p[t]$. Like the prime numbers they have finite fields $\mathbb{F}_{p^d}$, $d = \deg(p(t))$, as their residue class rings. The difference is, however, that now all these fields have the same characteristic. The geometric character of the ring $\mathbb{F}_p[t]$ becomes much more apparent in that, for an element $f = f(t) \in \mathbb{F}_p[t]$, the value of f at a point $\mathfrak{p} = (p(t))$ of the affine scheme $X = \operatorname{Spec}(\mathbb{F}_p[t])$ is actually given by the value $f(a) \in \mathbb{F}_p$, if $p(t) = t - a$, or more generally by $f(a) \in \mathbb{F}_{p^d}$ if $a \in \mathbb{F}_{p^d}$ is a zero of $p(t)$. This is due to the isomorphism

$$\mathbb{F}_p[t]/\mathfrak{p} \xrightarrow{\sim} \mathbb{F}_{p^d}$$

which takes the residue class $f(\mathfrak{p}) = f \bmod \mathfrak{p}$ to $f(a)$. In the analogy between, on the one hand, the progression of the prime numbers 2, 3, 5, 7, ... and the growing of the cardinalities $p, p^2, p^3, p^4, \dots$ of the residue fields $\mathbb{F}_{p^d}$ on the other, resides one of the most profound mysteries of arithmetic.

One obtains the same arithmetic theory for the finite extensions K of $\mathbb{F}_p(t)$ as for algebraic number fields. This is clear from what we have developed for arbitrary one-dimensional noetherian integral domains. But the crucial difference with the number field case is seen in that the function field K hides away a finite number of further prime ideals, besides the prime ideals of $\mathcal{O}$, which must be taken into account in a fully-fledged development of the theory.

This phenomenon appears already for the rational function field $\mathbb{F}_p(t)$, where it is due to the fact that the choice of the unknown t which determines the ring of integrality $\mathbb{F}_p[t]$ is totally arbitrary. A different choice, say $t' = 1/t$, determines a completely different ring $\mathbb{F}_p[1/t]$, and thus completely different prime ideals. It is therefore crucial to build a theory which is independent of such choices. This may be done either via the theory of valuations, or scheme theoretically, i.e., in a geometric way.

Let us first sketch the more naïve method, via the theory of valuations. Let K be a finite extension of $\mathbb{F}_p(t)$ and $\mathcal{O}$ the integral closure of $\mathbb{F}_p[t]$ in K.

By §11, for every prime ideal $\mathfrak{p} \neq 0$ of $\mathcal{O}$ there is an associated normalized discrete valuation, i.e., a surjective function

$$v_{\mathfrak{p}}: K \longrightarrow \mathbb{Z} \cup \{\infty\}$$

satisfying the properties

(i) $v_{\mathfrak{p}}(0) = \infty$,

(ii) $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$,

(iii) $v_{\mathfrak{p}}(a+b) \geq \min\{v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)\}$.

The relation between the valuations and the prime decomposition in the Dedekind domain $\mathcal{O}$ is given by

$$(a) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(a)}.$$

The definition of a discrete valuation of K does not require the subring $\mathcal{O}$ to be given in advance, and in fact, aside from those arising from $\mathcal{O}$, there are finitely many other discrete valuations of K. In the case of the field $\mathbb{F}_p(t)$ there is one more valuation, besides the ones associated to the prime ideals $\mathfrak{p} = (p(t))$ of $\mathbb{F}_p[t]$, namely, the degree valuation v_∞. For $\frac{f}{g} \in \mathbb{F}_p(t)$, $f, g \in \mathbb{F}_p[t]$, it is defined by

$$v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f).$$

It is associated to the prime ideal $\mathfrak{p} = y\mathbb{F}_p[y]$ of the ring $\mathbb{F}_p[y]$, where $y = 1/t$. One can show that this exhausts all normalized valuations of the field $\mathbb{F}_p(t)$.

For an arbitrary finite extension K of $\mathbb{F}_p(t)$, instead of restricting attention to prime ideals, one now considers all normalized discrete valuations $v_{\mathfrak{p}}$ of K in the above sense, where the index $\mathfrak{p}$ has kept only a symbolic value. As an analogue of the ideal group we form the "divisor group", i.e., the free abelian group generated by these symbols,

$$Div(K) = \Big\{ \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} \;\Big|\; n_{\mathfrak{p}} \in \mathbb{Z},\ n_{\mathfrak{p}} = 0 \text{ for almost all } \mathfrak{p} \Big\}.$$

We consider the mapping

$$\operatorname{div}: K^* \longrightarrow Div(K), \quad \operatorname{div}(f) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f)\mathfrak{p},$$

the image of which is written $P(K)$, and we define the divisor class group of K by

$$Cl(K) = Div(K)/P(K).$$

Unlike the ideal class group of an algebraic number field, this group is not finite. Rather, one has the canonical homomorphism

$$\deg : Cl(K) \longrightarrow \mathbb{Z},$$

which associates to the class of $\mathfrak{p}$ the degree $\deg(\mathfrak{p}) = [\kappa(\mathfrak{p}) : \mathbb{F}_p]$ of the residue class field of the valuation ring of $\mathfrak{p}$, and which associates to the class of an arbitrary divisor $\mathfrak{a} = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p}$ the sum

$$\deg(\mathfrak{a}) = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \deg(\mathfrak{p}).$$

For a principal divisor $\operatorname{div}(f)$, $f \in K^*$, we find by an easy calculation that $\deg(\operatorname{div}(f)) = 0$, so that the mapping deg is indeed well-defined. As an analogue of the finiteness of the class number of an algebraic number field, one obtains here the fact that, if not $Cl(K)$ itself, the kernel $Cl^0(K)$ of deg is finite. The infinitude of the class group of function fields must not be considered as strange. On the contrary, it is rather the finiteness in the number field case that should be regarded as a deficiency which calls for correction. The adequate appreciation of this situation and its amendment will be explained in chap. III, § 1.

The ideal, completely satisfactory framework for the theory of function fields is provided by the notion of scheme. In the last section we introduced affine schemes as pairs $(X, \mathcal{O}_X)$ consisting of a topological space $X = \operatorname{Spec}(\mathcal{O})$ and a sheaf of rings $\mathcal{O}_X$ on X. More generally, a scheme is a topological space X with a sheaf of rings $\mathcal{O}_X$ such that, for every point of X, there exists a neighbourhood U which, together with the restriction $\mathcal{O}_U$ of the sheaf $\mathcal{O}_X$ to U, is isomorphic to an affine scheme in the sense of § 13. This generalization of affine schemes is the correct notion for a function field K. It shows all prime ideals at once, and misses none.

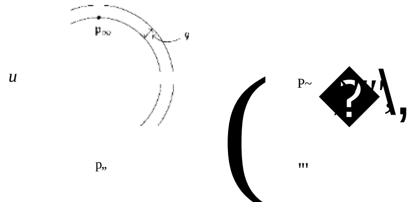
In the case $K = \mathbb{F}_p(t)$ for instance, the corresponding scheme $(X, \mathcal{O}_X)$ is obtained by gluing the two rings $A = \mathbb{F}_p[u]$ and $B = \mathbb{F}_p[v]$, or more precisely the two affine schemes $U = \operatorname{Spec}(A)$ and $V = \operatorname{Spec}(B)$. Removing from U the point $\mathfrak{p}_0 = (u)$, and the point $\mathfrak{p}_\infty = (v)$ from V, one has $U - \{\mathfrak{p}_0\} = \operatorname{Spec}(\mathbb{F}_p[u, u^{-1}])$, $V - \{\mathfrak{p}_\infty\} = \operatorname{Spec}(\mathbb{F}_p[v, v^{-1}])$, and the isomorphism $f : \mathbb{F}_p[u, u^{-1}] \to \mathbb{F}_p[v, v^{-1}]$, $u \mapsto v^{-1}$, yields a bijection

$$\varphi : V - \{\mathfrak{p}_\infty\} \to U - \{\mathfrak{p}_0\}, \quad \mathfrak{p} \mapsto f^{-1}(\mathfrak{p}).$$

We now identify in the union $U \cup V$ the points of $V - \{\mathfrak{p}_\infty\}$ with those of $U - \{\mathfrak{p}_0\}$ by means of φ, and obtain a topological space X. It is immediately obvious how to obtain a sheaf of rings $\mathcal{O}_X$ on X from the two sheaves $\mathcal{O}_U$ and $\mathcal{O}_V$. Removing from X the point $\mathfrak{p}_\infty$, resp. $\mathfrak{p}_0$, one gets canonical isomorphisms

$$(X - \{\mathfrak{p}_\infty\}, \mathcal{O}_X|_{X - \{\mathfrak{p}_\infty\}}) \cong (U, \mathcal{O}_U), \quad (X - \{\mathfrak{p}_0\}, \mathcal{O}_X|_{X - \{\mathfrak{p}_0\}}) \cong (V, \mathcal{O}_V).$$

The pair $(X, \mathcal{O}_X)$ is the scheme corresponding to the field $\mathbb{F}_p(t)$. It is called the **projective line** over $\mathbb{F}_p$ and denoted $\mathbb{P}^1_{\mathbb{F}_p}$.



More generally, one may similarly associate a scheme $(X, \mathcal{O}_X)$ to an arbitrary extension $K \supset \mathbb{F}_p(t)$. For the precise description of this procedure we refer the reader to [51].

Chapter II

The Theory of Valuations

§1. The p-adic Numbers

The p-adic numbers were invented at the beginning of the twentieth century by the mathematician KURT HF.NSF!. (1861-1941) with a view to introduce into number theory the powerful method of power series expansion which plays such a predominant r61e in function theory. The idea originated from the observation made in the last chapter that the numbers f E Z may be viewed in analogy with the polynomials/(:) E C[zj as functions on the space X of prime numbers in Z, associating to them their "value" at the point p EX, i.e., the element

$$f(p) \ ,[illegible]J \bmod p$$

in the residue class field $K(p) = \mathbb{Z}/p\mathbb{Z}$.

This point of view suggests the further question: whether not only the "value" of the integer f E Z at p, but also the higher derivatives *off* can he reasonably defined. In the case of the polynomials $f(z)$ E C[zl, the higher derivatives at the point $z = a$ are given by the coeflicients of the expansion

$$f(z) = ao + a1(z - a) + \cdot \ \bullet + a11(z - at,$$

and more generally, for rational functions $f(z) =$ E C(z), with /?, h E C[z], they are defined by the Taylor expansion

$$\{(z) = ,tJ\, av(z - a)v,$$

provided there is no pole at $z = a$, i.e., as long as $(L - a)$ f $h(z)$. The fact that such an expansion can also be written down, relative to a prime number p in Z, for any rational number f E Q as long as it lies in the local ring

$$\mathbb{Z}_{(p)} = \left\{ \tfrac{g}{h} \mid g, h \in \mathbb{Z},\ p \nmid h \right\}$$

leads us to the notion of p-adk number. First, every positive integer f EN admits a p•adic expansion

$$f = a_0 + a_1 p + \cdots + a_n p^n,$$

with coefficients a_i in $\{0, 1, \dots, p-1\}$, i.e., in a fixed system of representatives of the "field of values" $\kappa(p) = \mathbb{F}_p$. This representation is clearly unique. It is computed explicitly by successively dividing by p, forming the following system of equations:

$$\begin{aligned} f &= a_0 + pf_1,\\ f_1 &= a_1 + pf_2,\\ &\;\;\vdots\\ f_{n-1} &= a_{n-1} + pf_n,\\ f_n &= a_n. \end{aligned}$$

Here $a_i \in \{0, 1, \dots, p-1\}$ denotes the representative of $f_i \bmod p \in \mathbb{Z}/p\mathbb{Z}$. In concrete cases, one sometimes writes the number f simply as the sequence of digits $a_0, a_1 a_2 \dots a_n$, for instance

$$\begin{aligned} 216 &= 0.0011011 \quad \text{(2-adic)},\\ 216 &= 0.0022 \quad \text{(3-adic)},\\ 216 &= 1.331 \quad \text{(5-adic)}. \end{aligned}$$

As soon as one tries to write down such p-adic expansions also for negative integers, let alone for fractions, one is forced to allow infinite series

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu = a_0 + a_1 p + a_2 p^2 + \cdots.$$

This notation should at first be understood in a purely formal sense, i.e., $\sum_{\nu=0}^{\infty} a_\nu p^\nu$ simply stands for the sequence of partial sums

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu, \quad n = 1, 2, \dots.$$

(1.1) Definition. *Fix a prime number p. A p-adic integer is a formal infinite series*

$$a_0 + a_1 p + a_2 p^2 + \cdots,$$

where $0 \le a_i < p$, for all $i = 0, 1, 2, \dots$. The set of all p-adic integers is denoted by $\mathbb{Z}_p$.

The p-adic expansion of an arbitrary number $f \in \mathbb{Z}_{(p)}$ results from the following proposition about the residue classes in $\mathbb{Z}/p^n\mathbb{Z}$.

(1.2) Proposition. *The residue classes $a \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely represented in the form*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \bmod p^n$$

where $0 \le a_i < p$ for $i = 0, \dots, n-1$.

Proof (induction on n): This is dear for $n = 1$. Assume the statement is proved for $n-1$. Then we have a unique representation

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-2} p^{n-2} + g p^{n-1},$$

for some integer g. If $g \equiv a_{n-1} \bmod p$ such that $0 \le a_{n-1} < p$, then a_{n-1} is uniquely detennined by a, and the congruence of the proposition holds.

□

Every integer f and, more generally, every rational number $f \in$ the denominator of which is not divisible by p, defines a sequence of classes

$$\bar{f}_n = f \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1, 2,$$

for which we find, by the preceding proposition,

$$\begin{aligned} \bar{f}_1 &= a_0 \bmod p, \\ \bar{f}_2 &= a_0 + a_1 p \bmod p^2, \\ \bar{f}_3 &= a_0 + a_1 p + a_2 p^2 \bmod p^3 \quad \text{etc.,} \end{aligned}$$

with uniquely dctcnnincd coefficients $a_0, a_1, a_2, \ldots \in \{0, 1, \ldots, p-1\}$ which keep their meaning from one line to the next. The sequence of numbers

$$s_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \quad n = 1, 2,$$

defines a p-adic integer

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p.$$

We call it the **p-adic expansion** of f.

In analogy with the Laurent series $f(z) = \sum_{\nu=-m}^{\infty} a_\nu (z-a)^\nu$, we now extend the domain of p-adic integers into that of the formal series

$$a_\nu p^\nu = a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + \cdot$$

where $m \in \mathbb{Z}$ and $0 \le a_\nu < p$. Such series we call simply **p-adic numbers** and we write $\mathbb{Q}_p$ for the set of all these p-adic numbers. If $f \in \mathbb{Q}$ is any rational number, then we write

$$f = \frac{g}{h} p^{-m} \quad \text{where } g, h \in \mathbb{Z}, \quad (gh, p) = 1,$$

and if

$$a_0 + a_1 p + a_2 p^2 + \cdot$$

is the p-adic expansion of n, then we attach to f the p-adic number

$$a_0p^{-m} + a_1p^{-m+1} + \cdots + a_m + a_{m+1}p + \cdots \in \mathbb{Q}_p$$

as its p-adic expansion.

In this way we ohtain a canonical mapping

$$\mathbb{Q} \to \mathbb{Q}_p,$$

which takes $\mathbb{Z}$ into $\mathbb{Z}_p$ and is injective. For if $a, b \in \mathbb{Z}$ have the same p-adic expansion, then $a - b$ is divisible by p^n for every n, and hence $a = b$. We now identify $\mathbb{Q}$ with its image in $\mathbb{Q}_p$, so that we may write $\mathbb{Q} \subseteq \mathbb{Q}_p$ and $\mathbb{Z} \subseteq \mathbb{Z}_p$. Thus, for every rational number $f \in \mathbb{Q}$, we obtain an identity

$$f = \sum a_\nu p^\nu$$

This establishes the arithmetic analogue of the function-theoretic power series expansion for which we were looking.

Examples: a) $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$.

In fact, we have

$$-1 = (p-1) + (p-1)p + \cdots + (p-1)p^{n-1} - p^n,$$

$$\text{hence } -1 \equiv (p-1) + (p-1)p + \cdots + (p-1)p^{n-1} \mod p^n.$$

b) $\frac{1}{1-p} = 1 + p + p^2 + \cdots$

In fact,

$$1 = (1 + p + \cdots + p^{n-1})(1-p) + p^n,$$

$$\text{hence} \quad \frac{1}{1-p} \equiv 1 + p + \cdots + p^{n-1} \mod p^n.$$

One can define addition and muhiplication of p-adic numbers which tum $\mathbb{Z}_p$ into a ring, and $\mathbb{Q}_p$ into its field of fractions. However, the direct approach, defining sum and product via the usual carry-over rules for digits, as one does it when dealing with real numbers as decimal fractions, leads into complications. They disappear once we use another representation of the p-adic numbers $f = \sum_{\nu=0}^{\infty} a_\nu p^\nu$, viewing them not as sequences of sums of integers

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu \in \mathbb{Z},$$

V=O

but rather as sequences of **residue** classes

$$\bar{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

The terms of such a sequence lie in different rings $\mathbb{Z}/p^n\mathbb{Z}$, but these are related by the canonical projections

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \cdots$$

and we find

$$\lambda_n(\bar{s}_{n+1}) = \bar{s}_n.$$

In the direct product

$$\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z}\}$$

we now consider all elements $(x_n)_{n\in\mathbb{N}}$ with the property that

$$\lambda_n(x_{n+1}) = x_n \quad \text{for all } n = 1, 2, \ldots.$$

This set is called the **projective limit** of the rings $\mathbb{Z}/p^n\mathbb{Z}$ and is denoted by $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. In other words, we have

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \Big\{(x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \;\Big|\; \lambda_n(x_{n+1}) = x_n,\ n = 1, 2, \ldots\Big\}.$$

The modified representation of the p-adic numbers alluded to above now follows from the

(1.3) Proposition. *Associating to every p-adic integer*

$$f = \sum_{\nu=0}^{\infty} a_\nu p^\nu$$

the sequence $(\bar{s}_n)_{n\in\mathbb{N}}$ of residue classes

$$\bar{s}_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z},$$

yields a bijection

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

The proof is an immediate consequence of proposition (1.2). The projective limit $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ offers the advantage of being clearly a ring. In fact, it is a subring of the direct product $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ where addition and multiplication are defined componentwise. We identify $\mathbb{Z}_p$ with $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ and obtain the ring of p-adic integers $\mathbb{Z}_p$.

Since every element $f \in \mathbb{Q}_p$ admits a representation

with $g \in \mathbb{Z}_p$, addition and multiplication extend from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ and $\mathbb{Q}_p$ becomes the field of fractions of $\mathbb{Z}_p$.

In $\mathbb{Z}_p$, we found the rational integers $a \in \mathbb{Z}$ which were determined by the congruences

$$a \equiv a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \bmod p^n,$$

$0 \le a_i < p$. Making the identification

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

the subset $\mathbb{Z}$ is taken to the set of tuples

$$(a \bmod p,\ a \bmod p^2,\ a \bmod p^3,\ \ldots) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$$

and thereby is realized as a subring of $\mathbb{Z}_p$. We obtain $\mathbb{Q}$ as a subfield of the field $\mathbb{Q}_p$ of p-adic numbers in the same way.

Despite their origin in function-theoretic ideas, the p-adic numbers live up to their destiny entirely within arithmetic, more precisely at its classical heart, the Diophantine equations. Such an equation

$$F(x_1, \ldots, x_n) = 0$$

is given by a polynomial $F \in \mathbb{Z}[x_1, \ldots, x_n]$, and the question is whether it admits solutions in integers. This difficult problem can be weakened by considering, instead of the equation, all the congruences

$$F(x_1, \ldots, x_n) \equiv 0 \bmod m.$$

By the Chinese remainder theorem, this amounts to considering the congruences

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^\nu$$

modulo all prime powers. The hope is to obtain in this way information about the original equation. This plethora of congruences is now synthesized again into a single equation by means of the p-adic numbers. In fact, one has the

(1.4) Proposition. *Let $F(x_1, \ldots, x_n)$ be a polynomial with integer coefficients, and fix a prime number p. The congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^\nu$$

is solvable for arbitrary $\nu \geq 1$ if and only if the equation

$$F(x_1, \ldots, x_n) = 0$$

is solvable in p-adic integers.

Proof: As established above, we view the ring $\mathbb{Z}_p$ as the projective limit

$$\mathbb{Z}_p = \varprojlim_\nu \mathbb{Z}/p^\nu\mathbb{Z} \subseteq \prod_{\nu=1}^{\infty} \mathbb{Z}/p^\nu\mathbb{Z}.$$

Viewed over the ring on the right, the equation $F = 0$ splits up into components over the individual rings $\mathbb{Z}/p^\nu\mathbb{Z}$, namely, the congruences

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^\nu .$$

If now

$$(x_1, \ldots, x_n) = (x_1^{(\nu)}, \ldots, x_n^{(\nu)})_{\nu \in \mathbb{N}} \in \mathbb{Z}_p^n,$$

with $(x_i^{(\nu)})_{\nu \in \mathbb{N}} \in \mathbb{Z}_p = \prod \mathbb{Z}/p^\nu\mathbb{Z}$, is a p-adic solution of the equation $F(x_1, \ldots, x_n) = 0$, then the congruences are solved by

$$F(x_1^{(\nu)}, \ldots, x_n^{(\nu)}) \equiv 0 \bmod p^\nu, \quad \nu = 1, 2, \ldots .$$

Conversely, let a solution $(x_1^{(\nu)}, \ldots, x_n^{(\nu)})$ of the congruence

$$F(x_1, \ldots, x_n) \equiv 0 \bmod p^\nu$$

be given for every $\nu \geq 1$. If the elements $(x_i^{(\nu)})_{\nu \in \mathbb{N}} \in \prod \mathbb{Z}/p^\nu\mathbb{Z}$ are already in $\varprojlim \mathbb{Z}/p^\nu\mathbb{Z}$, for all $i = 1, \ldots, n$, then we have a p-adic solution of the equation $F = 0$. But this is not automatically the case. We will therefore extract a subsequence from the sequence $(x_1^{(\nu)}, \ldots, x_n^{(\nu)})$ which fits our needs. For simplicity of notation we only carry this out in the case $n = 1$, writing $x_\nu = x_1^{(\nu)}$. The general case follows exactly the same pattern.

In what follows, we view (x_ν) as a sequence in $\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is finite, there are infinitely many terms x_ν which mod p are congruent to the same element $y_1 \in \mathbb{Z}/p\mathbb{Z}$. Hence we may choose a subsequence $\{x_\nu^{(1)}\}$ of $\{x_\nu\}$ such that

$$x_\nu^{(1)} \equiv y_1 \bmod p \quad \text{and} \quad F\big(x_\nu^{(1)}\big) \equiv 0 \bmod p .$$

Likewise, we may exuac1 from lx�11} a suhsequence Jxt2>1such lhat

$$x�}) = }'1 \bmod p\text{-:. and } F\{.t�^2 l) = 0 \bmod p.^1,$$

where _\'2 E Z/ p^2Z evidently satisfies)'2 = y1 mod p. Continuing in this way, we obtain for each k 2: l a subsequence {x�kl j of [x;,t-I l} the 1erms of which satisfy the congruences

$$\text{rtk/} = YA \bmod Ji' \quad \text{und} \quad F(x;,^0) = 0 \bmod 1/$$

for some Jl E Z/ pkz such 1ha1

$$Yk :=y4. \ 1 \bmod,\text{-/}' \ 1.$$

They, define a p-adic integer y = (yJJAE:"I E ll!!! Z/;iZ = Zp satisfying

$$F(y1:) = 0 \bmod 1l$$

for all $k?:.$I. In other words, $F(y) = 0$. □

10:xerci....e I. fl. p-adic numher a = L�..,a,,p'' E QP is a rational numher if and only if the sequence of digils is periodic (possibly with a fini1e siring before 1he first pcrit�.I).

Hint: Write $pma = h + c$ 1 � p''' O � /1 < p', 0 =:cc< p''.

Exercise 2. A p-adic integer a= a1, + a1 p + a2/l2 + ··· is a unit in the ring Z/1 if and only if 011 #- 0

F.xt:n.:ise 3. Show that the equation $x^2 = 2$ ha'> a solution in Z_7.

Excn:ise 4. Write the numher.- � and - � as 5-adic nurnhcrs.

t-::urci� S. The field QP of ,,-111Jic numbers has no aulomorphb,ms excepl lhc identity.

Exercise {i. How is the addition, suhtractioo. multiplication and division of rational numbers rdlected in the representation by p-adic digits"1

§ 2. The p-adic Absolute Value

The representation of a p-adk: inlcgcr

(I) $$a_0 + a_1 p + a_2 p^2 + \cdots$$

resembles very much the decimal frnction represcmation

$$<l\{,+a,(\frac{I}{10})+a,(\frac{I}{10})^2+ \quad , \quad O<:a;<l0,$$

of a real number between O and 10, But it does not converge as the decimal fraction docs. Nonetheless, the field *Qr>* of p-adic numbers can be constructed from the field Q in the same fashion as the tield of real numbers IR. The key to this is to ruplm.:e the ordinary absolute value by a new '·p-adic" absolute value I Ip with rcsper...:t to which the series (I) converge so rh:H the p-adic numbers appear in the usual manner as limirs of Cauchy sequences of rational numbers. This ap11roach was proposed hy the Hungarian mathematician *J. KORSCffA.K.* The p-adic absolute value I Ip is defined as follows.

Let $a = \mathrm{i}.h, c$ E Z be a nonzero rational number. We extract from *h* and from *c* as high a power of the prime number *p* as possible,

$$a=p^{111}!! \; \dot{:}\, \dot{\_}, \quad (b'c'.p)=l. \tag{2}$$

and we put

$$lalp= \frac{I}{pm}$$

Thus the p-adic value no longer measures the siz.e of a number $a \in$ N. Instead it becomes small if the number is divisible by a high power of *p*. This elahorates on the idea suggested in (1.4) that an integer has to be O if it is infinitely divisible by *p*. In particular, the summands of a *p-�dic* series $a_0+(1_1p+a2p^2+\cdot$ fonn a sequence converging to O wilh respec! to I I,,.

The exponem *m* in tOC representation (2) of the number *a* is denoted by *l!p(a).* am.I one puls fonnally $11_1,(0) =$ oo. This gives the funelion

$$v_{1,} :Q\text{----}+ ZUloo),$$

which is easily checked to satisfy 1he propcnics

I) $vp((I) =$ oo $<=> a = 0$,

2) $v,,(ah) = v_1,(a) + v_1,(b)$,

3) $vp(a+$ h) :=:: min{vp(a), l'p{h)},

where .r + oo = oo, oc + oo = :xi and oo > *x*, for all *x* E Z. The funcrion *vp* is called lhc p-adic exponentia,l•aluation of IQ. The p-adic absolute value is given by

$$I \; I,, : Q � \quad R, \quad a \; \text{i-----+} \; lalp = p \; \text{•'�<u>}.$$

In view of I), 2), 3), it satisfies the conditions of a *norm* on Q:

1) $|a|_p = 0 \iff a = 0$,
2) $|ab|_p = |a|_p|b|_p$,
3) $|a+b|_p \le \max\{|a|_p, |b|_p\} \le |a|_p + |b|_p$.

One can show that the absolute values $|\ |_p$ and $|\ |$ essentially exhaust all norms on $\mathbb{Q}$: any further norm is a power $|\ |_p^s$ or $|\ |^s$, for some real numbers $s > 0$ (see (3.7)). The usual absolute value $|\ |$ is denoted in this context by $|\ |_\infty$. The good reason for this will be explained in due course. In conjunction with the absolute values $|\ |_p$, it satisfies the following important **product formula:**

(2.1) Proposition. *For every rational number $a \neq 0$, one has*

$$\prod_p |a|_p = 1,$$

where p varies over all prime numbers as well as the symbol ∞.

Proof: In the prime factorization

$$a = \pm \prod_{p \neq \infty} p^{v_p}$$

of a, the exponent v_p of p is precisely the exponential valuation $v_p(a)$ and the sign equals $\frac{a}{|a|_\infty}$. The equation therefore reads

$$a = \frac{a}{|a|_\infty} \prod_{p \neq \infty} \frac{1}{|a|_p},$$

so that one has indeed $\prod_p |a|_p = 1$. □

The notation $|\ |_\infty$ for the ordinary absolute value is motivated by the analogy of the field of rational numbers $\mathbb{Q}$ with the rational function field $k(t)$ over a finite field k, with which we started our considerations. Instead of $\mathbb{Z}$, we have inside $k(t)$ the polynomial ring $k[t]$, the prime ideals $\mathfrak{p} \neq 0$ of which are given by the monic irreducible polynomials $p(t) \in k[t]$. For every such $\mathfrak{p}$, one defines an absolute value

$$|\ |_{\mathfrak{p}} : k(t) \to \mathbb{R}$$

as follows. Let $f(t) = \frac{g(t)}{h(t)}$, $g(t), h(t) \in k[t]$ be a nonzero rational function. We extract from $g(t)$ and $h(t)$ the highest possible power of the irreducible polynomial $p(t)$,

$$f(t) = p(t)^m \frac{\tilde{g}(t)}{\tilde{h}(t)}, \quad (\tilde{g}\tilde{h}, p) = 1,$$

and put

$$v_\mathfrak{p}(f) = m, \quad |f|_\mathfrak{p} = q_\mathfrak{p}^{-v_\mathfrak{p}(f)},$$

where $q_\mathfrak{p} = q^{d_\mathfrak{p}}$, $d_\mathfrak{p}$ being the degree of the residue das� field of p over k and q a fixed real number> I. Furthermore we put $v_\mathfrak{p}(0) = \infty$ and $|0|_\mathfrak{p} = 0$, and obtain for $v_\mathfrak{p}$ and $|\ |_\mathfrak{p}$ the same conditions I), 2). 3) as for v_p and $|\ |_p$ above. In the case $\mathfrak{p} = (t - a)$ for $a \in k$, the valuation $v_\mathfrak{p}(f)$ is dearly the order of the zero, resp. pole, of the function $f = f(t)$ at $t = a$.

But for the function field t..(1). there i5 one more exponential valuation

$$v_\infty : k(t) \to \mathbb{Z} \cup \{\infty\},$$

namely

$$v_\infty(f) = \deg(h) - \deg(g),$$

where $f = \frac{g}{h} \neq 0$, $g, h \in k[t]$. It describes the order of zero, resp. pole, of $f(t)$ at the point at inllnity ∞, i.e., the order of zero, resp. pole, of the function $f(1/t)$ at the point $t = 0$. ll is associated to the prime ideal $\mathfrak{p} = (1/t)$ of the ring $k[1/t] \subseteq k(t)$ in the same way as the exponential valuations $v_\mathfrak{p}$ are associated to the prime ideals p of A.[t]. Putting

$$|f|_\infty = q^{-v_\infty(f)}$$

the unique factorization in $k(t)$ yields, as in (2.1) above, the fonnula

where p varie5 over the prime ideals of kit] a� well a� the symbol co, which now denote" the point at infinity (sec chap, I, g 14, p. 95).

In view of the product fonnula (2.1), the above consideration shows that the ordinary absolute value $|\ |$ of $\mathbb{Q}$ �hould be thought of as being associated to a virtual point at infinity. This point of view justifies the notation $|\ |_\infty$ obey� our constant *leitmotiv* to study number" as function°' from a geometric per�pective, and it will fulfill the expectations thus raised in an ever growing and ama.dng manner. The decisive difference between the absolute value $|\ |_\infty$ and the ab�olute value $|\ |_\infty$ of $k(t)$ is, however, that the fom1er i� not from any exponential valuation v_p attached to a prime ideal.

Having introduced the p-adic absolute value $|\ |_p$ on the field :JJ!, let u� now give a new definition of the field of p-adic number�. imitating the construction of the field of real numbeVi. will verify afterwards that thb new, analytic construction does agree with Hensel'� definition, which was motivated by function theory.

A **Cauchy sequence** with respect to I I,, is by definition a sequence *{xn)* of rational numbcr5 such that for every f > 0, there exists a positive integer n_0 satir,fying

$$lxn-Xmlp <F \quad \text{forall} \quad n,m \ :'::no.$$

Example: Every formal series

$$\underset{V=O}{L} a1,p'', \quad 0 :Sa,, < p,$$

provides a Cauchy r,,cquence via its partial sum�

$$Xn = \overset{s-1}{,�}avp''.$$

because for $n > m$ one has

$$|x_n - x_m|_p = \Big| \sum_{v=m}^{n-1} a_v p^v \Big|_p \le \max_{m \le v < n} \{ |a_v p^v|_p \} \le \frac{1}{p^m}$$

A sequence */xn* in Q is called a **nullsequence** with respect to I II' if *lxn* If! is a sequence converging to O in the usual sense.

Example: I. p, p^2, p'_

The Cauchy sequencer, fom1 a ring *R*, the nullsequenccs fom1 a maximal ideal m, and we define afresh the field of p-adic numbers to be the residue class field

$$Q,, ,�RJm.$$

We embed Q in 1Q-i,, by associating to every element *a* E Q the residue class of the constant sequence (a, *a*, *a*. .). The p-adic absolute value I lp on Q is extended to Q// by giving lhc clement x = *lxnl* mod m E *R/m* the absolute value

$$lxlp := \}��lxnlp \ E \ IR.$$

This limit exists hecause { $lx_{11}lp$] is a Cauchy sequence in IR, and it is independent of the choice of lhc sequence *lxn)* within it� cla�s mod m because any p-adic nullsequence {_y,,} Em satisfies of course}�� *IYn* If! = 0.

The p-adic exponential valuation *Vp* on Q extends to an exponential valuation

$$vp : Q,, \text{-----+} Z \cup \{oo).$$

In fact, if $x \in \mathbb{Q}_p$ is the class of the Cauchy sequence $\{x_n\}$ where $x_n \neq 0$, then

$$v_p(x_n) = -\log_p |x_n|_p$$

either diverges to ∞ or is a Cauchy sequence in $\mathbb{Z}$ which eventually must become constant for large n because $\mathbb{Z}$ is discrete. We put

$$v_p(x) = \lim_{n \to \infty} v_p(x_n) = v_p(x_n) \quad \text{for } n \geq n_0 .$$

Again we find for all $x \in \mathbb{Q}_p$ that

$$|x|_p = p^{-v_p(x)} .$$

As for the field of real numbers one proves the

(2.2) **Proposition.** *The field $\mathbb{Q}_p$ of p-adic numbers is* **complete** *with respect to the absolute value $|\ |_p$, i.e., every Cauchy sequence in $\mathbb{Q}_p$ converges with respect to $|\ |_p$.*

As well as the field $\mathbb{R}$, we thus obtain for each prime number p a new field $\mathbb{Q}_p$ with equal rights and standing, so that $\mathbb{Q}$ has given rise to the infinite family of fields

$$\mathbb{Q}_2,\ \mathbb{Q}_3,\ \mathbb{Q}_5,\ \mathbb{Q}_7,\ \mathbb{Q}_{11},\ \ldots,\ \mathbb{Q}_\infty = \mathbb{R} .$$

An important special property of the *p-adic* absolute values $|\ |_p$ lies in the fact that they do not only satisfy the usual triangle inequality, but also the stronger version

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} .$$

This yields the following remarkable proposition, which gives us a new definition of the *p-adic integers*.

(2.3) **Proposition.** *The set*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

is a subring of $\mathbb{Q}_p$. It is the closure with respect to $|\ |_p$ of the ring $\mathbb{Z}$ in the field $\mathbb{Q}_p$.

Proof: That $\mathbb{Z}_p$ is closed under addition and multiplication follows from

$$|x+y|_p \le \max\{|x|_p, |y|_p\} \quad \text{and} \quad |xy|_p = |x|_p |y|_p .$$

If $\{x_n\}$ is a Cauchy sequence in $\mathbb{Z}$ and $x = \lim_{n\to\infty} x_n$, then $|x_n|_p \le 1$ implies also $|x|_p \le 1$, hence $x \in \mathbb{Z}_p$. Conversely, let $x = \lim_{n\to\infty} x_n \in \mathbb{Z}_p$, for a Cauchy sequence $\{x_n\}$ in $\mathbb{Q}$. We saw above that one has $|x|_p = |x_n|_p \le 1$ for $n \ge n_0$, i.e., $x_n = \frac{a_n}{b_n}$ with $a_n, b_n \in \mathbb{Z}$, $(b_n, p) = 1$. Choosing for each $n \ge n_0$ a solution $y_n \in \mathbb{Z}$ of the congruence $b_n y_n \equiv a_n \bmod p^n$ yields $|x_n - y_n|_p \le \frac{1}{p^n}$ and hence $x = \lim_{n\to\infty} y_n$, so that x belongs to the closure of $\mathbb{Z}$. □

The group of units of $\mathbb{Z}_p$ is obviously

$$\mathbb{Z}_p^* = \{ x \in \mathbb{Z}_p \mid |x|_p = 1 \}.$$

Every element $x \in \mathbb{Q}_p^*$ admits a unique representation

$$x = p^m u \quad \text{with } m \in \mathbb{Z} \text{ and } u \in \mathbb{Z}_p^* .$$

For if $\quad = m \in \mathbb{Z}$, then $\quad) = 0$, hence $|xp^{-m}|_p = 1$, i.e., $u = \quad \in \mathbb{Z}_p^*$. Furthermore we $\quad$ the

(2.4) Proposition. *The nonzero ideals of the ring $\mathbb{Z}_p$ are the principal ideals*

$$p^n\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \mid v_p(x) \ge n \},$$

with $n \ge 0$, and one has

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Proof: Let $\mathfrak{a} \ne (0)$ be an ideal of $\mathbb{Z}_p$ and $x = p^m u$, $u \in \mathbb{Z}_p^*$, an element of $\mathfrak{a}$ with smallest possible m (since $\quad \le 1$, one has $m \ge 0$). Then $\mathfrak{a} = \quad$ because $\quad = p^n u' \in \mathfrak{a}$, $\quad \in \mathbb{Z}_p^*$, implies $n \ge m$, hence $y = \quad$ The homomorphism

$$\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p, \quad a \mapsto a \bmod p^n\mathbb{Z}_p,$$

has kernel $p^n\mathbb{Z}$ and is surjective. Indeed, for every $x \in \mathbb{Z}_p$, there exists by (2.3) an $a \in \mathbb{Z}$ such that

$$|x - a|_p \leq \frac{1}{p^n},$$

i.e., $v_p(x-a) \geq n$, therefore $x - a \in p^n\mathbb{Z}_p$ and hence $x \equiv a \bmod p^n\mathbb{Z}_p$. So we obtain an isomorphism

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}. \qquad \square$$

We now want to establish the link with Hensel's definition of the ring $\mathbb{Z}_p$ and the field $\mathbb{Q}_p$ which was given in §1. There we defined the p-adic integers as formal series

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu, \quad 0 \leq a_\nu < p,$$

which we identified with sequences

$$x_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1, 2, \ldots,$$

where s_n was the partial sum

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu.$$

These sequences constituted the projective limit

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \Big\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \;\Big|\; x_{n+1} \mapsto x_n \Big\}.$$

We viewed the p-adic integers as elements of this ring. Since

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z},$$

we obtain, for every $n \geq 1$, a surjective homomorphism

$$\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}.$$

It is clear that the family of these homomorphisms yields a homomorphism

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

It is now possible to identify both definitions given for $\mathbb{Z}_p$ (and therefore also for $\mathbb{Q}_p$) via the

(2.5) **Proposition.** *The homomorphism*

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

is an isomorphism.

Proof: If $x \in \mathbb{Z}_p$ is mapped to zero, this means that $x \in p^n\mathbb{Z}_p$ for all $n \ge 1$, i.e., $|x|_p \le \frac{1}{p^n}$ for all $n \ge 1$, so that $|x|_p = 0$ and thus $x = 0$. This shows injectivity.

An element of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is given by a sequence of partial sums

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu, \quad 0 \le a_\nu < p.$$

We saw above that this sequence is a Cauchy sequence in $\mathbb{Z}_p$ and thus converges to an element

$$x = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p.$$

Since

$$x - s_n = \sum_{\nu=n}^{\infty} a_\nu p^\nu \in p^n\mathbb{Z}_p,$$

one has $x \equiv s_n \mod p^n$ for all n, i.e., x is mapped to the element of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, which is defined by the given sequence $(s_n)_{n\in\mathbb{N}}$. This shows surjectivity. $\square$

We emphasize that the elements on the right hand side of the isomorphism

$$\mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

are given formally by sequences of partial sums

$$s_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu, \quad n = 1, 2, \dots.$$

On the left, however, these sequences converge with respect to the absolute value and yield the elements of $\mathbb{Z}_p$ in the familiar way, as convergent infinite series

$$x = \sum_{\nu=0}^{\infty} a_\nu p^\nu.$$

Yet another, very elegant method to introduce the p-adic numbers comes about as follows. Let $\mathbb{Z}[[X]]$ denote the ring of all formal power series $\sum_{\nu=0}^{\infty} a_\nu X^\nu$ with integer coefficients. Then one has the

(2.6) Proposition. There is a canonical isomorphism

$$\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X - p).$$

Proof: Consider the visibly surjective homomorphism $\mathbb{Z}[[X]] \to \mathbb{Z}_p$ which to every formal power series $\sum_{\nu=0}^{\infty} a_\nu X^\nu$ associates the convergent series $\sum_{\nu=0}^{\infty} a_\nu p^\nu$. The principal ideal $(X-p)$ clearly belongs to the kernel of this mapping. In order to show that it is the whole kernel, let $f(X)=\sum_{\nu=0}^{\infty} a_\nu X^\nu$ be a power series such that $f(p)=\sum_{\nu=0}^{\infty} a_\nu p^\nu = 0$. Since $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, this means that

$$a_0+a_1p+\cdots+a_{n-1}p^{n-1} \equiv 0 \mod p^n$$

for all n. We put, for $n \geq 1$,

$$b_{n-1} = -\frac{1}{p^n}(a_0+a_1p+\cdots+a_{n-1}p^{n-1}).$$

Then we obtain successively

$$a_0 = -pb_0,$$

$$a_1 = b_0 - pb_1,$$

$$a_2 = b_1 - pb_2, \quad \text{etc.}$$

But this amounts to the equality

$$(a_0+a_1X+a_2X^2+\cdots) = (X-p)(b_0+b_1X+b_2X^2+\cdots),$$

i.e., $f(X)$ belongs to the principal ideal $(X-p)$. $\square$

Exercise 1. $|x-y|_p \geq \big||x|_p - |y|_p\big|$.

Exercise 2. Let n be a natural number, $n=a_0+a_1p+\cdots+a_{r-1}p^{r-1}$ its p-adic expansion, with $0 \leq a_i < p$, and $s = a_0+a_1+\cdots+a_{r-1}$. Show that $v_p(n!) = \frac{n-s}{p-1}$.

Exercise 3. The sequence $1, \frac{1}{10}, \frac{1}{100}, \frac{1}{1000}, \dots$ does not converge in $\mathbb{Q}_p$ for any p.

Exercise 4. Let $\varepsilon \in 1+p\mathbb{Z}_p$, and let $\alpha = a_0+a_1p+a_2p^2+\cdots$ be a p-adic integer, and write $s_n = a_0+a_1p+\cdots+a_{n-1}p^{n-1}$. Show that the sequence ε^{s_n} converges to a number ε^α in $1+p\mathbb{Z}_p$. Show furthermore that $1+p\mathbb{Z}_p$ is thus turned into a multiplicative $\mathbb{Z}_p$-module.

Exercise 5. For every $a \in \mathbb{Z}$, $(a,p)=1$, the sequence $\{a^{p^n}\}_{n\in\mathbb{N}}$ converges in $\mathbb{Q}_p$.

Exercise 6. The fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic, unless $p=q$.

Exercise 7. The algebraic closure of $\mathbb{Q}_p$ has infinite degree.

Exercise 8. In the ring $\mathbb{Z}_p[[X]]$ of formal power series $\sum_{\nu=0}^{\infty} a_\nu X^\nu$ over $\mathbb{Z}_p$, one has the following division with remainder. Let $g \in \mathbb{Z}_p[[X]]$ and let $f(X) = a_0+a_1X+\cdots$ such that $p \mid a_\nu$ for $\nu = 0, \dots, n-1$, but $p \nmid a_n$. Then one may write in a unique way

$$g = qf + r,$$

where q E Z,,IIX]], and IE Z1,[XI is a polynomial of degree� 11- I.

Hint: Let τ be the operator $\tau(\sum_{\nu=0}^{\infty} b_\nu X^\nu) = \sum_{\nu=n}^{\infty} b_\nu X^{\nu-n}$. Show that $U(X) = \tau(f(X))$ is a unit in $\mathbb{Z}_p[[X]]$ and write $f(X) = pP(X) + X^n U(X)$ with a polynomial $P(X)$ of degree $\leq n-1$. Show that

$$q(X) = \frac{1}{U(X)} \sum_{i=0}^{\infty} (-1)^i p^i \left(\tau \circ \frac{P}{U}\right)^i \tau(g)$$

is a well-defined power series in $\mathbb{Z}_p[[X]]$ such that $\tau(qf) = \tau(g)$.

Exercise 9 (p-adic Weierstrass Preparation Theorem). Every nonzero power series

$$f(X) = \qquad \in \mathbb{Z}_p[[X]]$$

admits a unique representation

$$f(X) = p^\mu P(X) U(X),$$

where $U(X)$ is a unit in $\mathbb{Z}_p[[X]]$ and $P(X) \in \mathbb{Z}_p[X]$ is a monic polynomial satisfying $P(X) \equiv X^n \bmod p$.

§ 3. Valuations

The procedure we performed in the previous section with the field $\mathbb{Q}$ in order to obtain the p-adic numbers can be generalized to arbitrary fields using the concept of (multiplicative) valuation.

(3.1) Definition. *A* valuation of a *field K* is *a function*

enjoying the properties

(i) $|x| \geq 0$, *and* $|x| = 0 \iff x = 0$,

(ii) $|xy| = |x||y|$,

(iii) $|x+y| \leq |x| + |y|$ *"triangle inequality".*

We tacitly exclude in the sequel the case where $|\ |$ is the trivial valuation of K which satisfies $|x| = 1$ for all $x \neq 0$. Defining the distance between two points $x, y \in K$ by

$$d(x,y) = |x-y|$$

makes K into a metric space, and hence in particular a topological space.

(3.2) Definition. *Two valuations* of K are called equivalent if *they* define *the* same *topology on* K.

(3.3) Proposition. *Two* valuations I I1 and I 12 on *K* are *equivalent* if and *only* if *there* exists a *real numbers* > 0 *such Iha/ one has*

forallx EK.

Proof: If I I1 = I 11, *withs* > 0, then I I1 and I 12 are obviomly equivalent. For an arbitrary valuation I I on *K,* the inequality Ix I < I is tantamount to the condition that *\xn)"""l* converges to zero in the topology defined by I I. Therefore if I 11 and I 12 are equivalent, one has the implication

$$|x|_1 < 1 \Longrightarrow |x|_2 < 1$$

Now let E *K* be a fixed element satisfying lyl1 > I. Lett EK, *x f.* 0. Then = IYl'i' for �ome *a* E JR. Let *m,/n;* be a sequence of rational numbers (with > 0) which converges to *a* from above. Then we have lxl1 = lylf < hence

I *xn,* < I ===} *xn,* 12< I,

so that lxl2 ::S IYl;',1111, and thu� lxl2 ::S IY12- Using a sequence *m,/n,* which converge<, lo *a* from below(*) tells us that lxl2 :::_ lyl�- So we have lxl2 = lyl�. For all *x* E *K, x f.* 0, we therefore get

loglxl1 logl_vl1
log lxl2= log IYl2 =: *s,*

hence l.tl1 = ltl;. But ly11 > I implies IYl2 >!,hences> 0. r:J

The proof shows that the equivalence of I 11 and I 12 is abo equivalent to the condition

$$|x|_1 < 1 \Longrightarrow |x|_2 < 1$$

We use this for the proof of the following approximation theorem, which may be considered a variant of the Chinese remainder theorem.

(3.4) Approximation Theorem. *Let* I 11, ... I 111 *be* pairwise *inequivalent valuations* of *the* field *K and Jet* a1, ... , *an* E *K be given elemcms. Then* for every *c* > 0 *there exists* an *x* E *K such that*

I\ - *a,* I; < f for aJJ i = I,

Proof: By the above remark, since $|\ |_1$ and $|\ |_n$ are inequivalent, there exists $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_n \geq 1$. By the same token, there exists $\beta \in K$ such that $|\beta|_n < 1$ and $|\beta|_1 \geq 1$. Putting $y = \beta/\alpha$, one finds $|y|_1 > 1$ and $|y|_n < 1$.

We now prove by induction on n that there exists $z \in K$ such that

$$|z|_1 > 1 \quad \text{and} \quad |z|_j < 1 \quad \text{for } j = 2, \dots, n.$$

We have just done this for $n = 2$. Assume we have found $z \in K$ satisfying

$$|z|_1 > 1 \quad \text{and} \quad |z|_j < 1 \quad \text{for } j = 2, \dots, n-1.$$

If $|z|_n \leq 1$, then $z^m y$ will do, for m large. If however $|z|_n > 1$, the sequence $t_m = z^m/(1+z^m)$ will converge to 1 with respect to $|\ |_1$ and $|\ |_n$, and to 0 with respect to $|\ |_2, \dots, |\ |_{n-1}$. Hence, for m large, $t_m y$ will suffice.

The sequence $z^m/(1+z^m)$ converges to 1 with respect to $|\ |_1$ and to 0 with respect to $|\ |_2, \dots, |\ |_n$. For every i we may construct in this way a z_i which is very close to 1 with respect to $|\ |_i$ and very close to 0 with respect to $|\ |_j$, for $j \neq i$. The element

$$x = a_1 z_1 + \cdots + a_n z_n$$

then satisfies the statement of the approximation theorem. $\square$

(3.5) Definition. *The valuation* $|\ |$ *is called* **nonarchimedean** *if* $|n|$ *stays bounded, for all* $n \in \mathbb{N}$. *Otherwise it is called* **archimedean.**

(3.6) Proposition. *The valuation* $|\ |$ *is nonarchimedean if and only if it satisfies the* **strong triangle inequality**

$$|x + y| \leq \max\{|x|, |y|\}.$$

Proof: If the strong triangle inequality holds, then one has

$$|n| = |1 + \cdots + 1| \leq 1.$$

Conversely, let $|n| \leq N$ for all $n \in \mathbb{N}$. Let $x, y \in K$ and suppose $|x| \geq |y|$. Then $|x|^\nu |y|^{n-\nu} \leq |x|^n$ for $\nu \geq 0$ and one gets

$$|x+y|^n \leq \sum_{\nu=0}^{n} \left|\binom{n}{\nu}\right| |x|^\nu |y|^{n-\nu} \leq N(n+1)|x|^n,$$

hence

$$|x+y| \leq N^{1/n}(1+n)^{1/n}|x| = N^{1/n}(1+n)^{1/n}\max\{|x|, |y|\},$$

and thus $|x+y| \leq \max\{|x|, |y|\}$ by letting $n \to \infty$. $\square$

Remark: The strong triangle inequality immediately implies that

$$|x| \neq |y| \implies |x+y| = \max\{|x|,|y|\}.$$

One may extend the nonarchimedean valuation $|\ |$ of K to a valuation of the function field $K(t)$ in a canonical way by setting, for a polynomial $f(t) = a_0 + a_1 t + \cdots + a_n t^n$,

$$|f| = \max\{|a_0|, \ldots, |a_n|\}.$$

The triangle inequality $|f+g| \le \max\{|f|,|g|\}$ is immediate. The proof that $|fg| = |f||g|$ is the same as the proof of Gauss's lemma for polynomials over factorial rings once we replace the **content** of f in this lemma by the absolute value $|f|$.

For the field $\mathbb{Q}$, we have the usual absolute value $|\ |_\infty = |\ |$, this being the archimedean valuation, and for each prime number p the nonarchimedean valuation $|\ |_p$. As a matter of fact:

(3.7) **Proposition.** *Every valuation of* $\mathbb{Q}$ *is equivalent to one of the valuations* $|\ |_p$ or $|\ |_\infty$.

Proof: Let $\|\ \|$ be a nonarchimedean valuation of $\mathbb{Q}$. Then $\|n\| = \|1 + \cdots + 1\| \le 1$, and there is a prime number p such that $\|p\| < 1$ because, if not, unique prime factorization would imply $\|x\| = 1$ for all $x \in \mathbb{Q}^*$. The set

$$\mathfrak{a} = \{a \in \mathbb{Z} \mid \|a\| < 1\}$$

is an ideal of $\mathbb{Z}$ satisfying $p\mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$, and since $p\mathbb{Z}$ is a maximal ideal, we have $\mathfrak{a} = p\mathbb{Z}$. If now $a \in \mathbb{Z}$ and $a = bp^m$ with $p \nmid b$, so that $b \notin \mathfrak{a}$, then $\|b\| = 1$ and hence

$$\|a\| = \|p\|^m = |a|_p^s$$

where $s = -\log\|p\|/\log p$. Consequently $\|\ \|$ is equivalent to $|\ |_p$.

Now let $\|\ \|$ be archimedean. Then one has, for every two natural numbers $n, m > 1$,

$$\|m\|^{1/\log m} = \|n\|^{1/\log n}.$$

In fact, we may write

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

where $a_i \in \{0, 1, \ldots, n-1\}$ and $n^r \le m$. Hence, observing that $r \le \log m/\log n$ and $\|a_i\| \le \|1\| + \cdots + \|1\| \le a_i\|1\| \le n$, one gets the inequality

$$\|m\| \le \sum \|a_i\|\|n\|^i \le \sum \|a_i\|\|n\|^r \le \Big(1 + \frac{\log m}{\log n}\Big)\, n\, \|n\|^{\log m/\log n}.$$

Substituting here n^l for m, taking k-th roots on both sides, and letting k tend to ∞, one finally obtains

$$\|m\| \le \|n\|^{\log m/\log n} \quad \text{or} \quad \|m\|^{1/\log m} \le \|n\|^{1/\log n}.$$

Swapping m with n gives the identity (*). Putting $c = \|n\|^{1/\log n}$ we have $\|n\| = c^{\log n}$, and putting $c = e^s$ yields, for every positive rational number $x = a/b$,

$$\|x\| = e^{s \log |x|} = |x|^s.$$

Therefore $\|\ \|$ is equivalent to the usual absolute value $|\ |$ on $\mathbb{Q}$. □

Let $|\ |$ be a nonarchimedean valuation of the field K. Putting

$$v(x) = -\log|x| \quad \text{for } x \neq 0, \quad \text{and } v(0) = \infty,$$

we obtain a function

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

verifying the properties

(i) $v(x) = \infty \iff x = 0$,

(ii) $v(xy) = v(x) + v(y)$,

(iii) $v(x + y) \ge \min\{v(x), v(y)\}$,

where we fix the following conventions regarding elements $a \in \mathbb{R}$ and the symbol ∞: $a < \infty$, $a + \infty = \infty$, $\infty + \infty = \infty$.

A function v on K with these properties is called an **exponential valuation** of K. We exclude the case of the trivial function $v(x) = 0$ for $x \neq 0$, $v(0) = \infty$. Two exponential valuations v_1 and v_2 of K are called **equivalent** if $v_1 = s v_2$, for some real number $s > 0$. For every exponential valuation v we obtain a valuation in the sense of (3.1) by putting

$$|x| = q^{-v(x)},$$

for some fixed real number $q > 1$. To distinguish it from v, we call $|\ |$ an associated **multiplicative valuation, or absolute value.** Replacing v by an equivalent valuation sv (i.e., replacing q by $q' = q^s$) changes $|\ |$ into the equivalent multiplicative valuation $|\ |^s$. The conditions (i), (ii), (iii) immediately imply the

(3.8) **Proposition.** *The subset*

$$\mathfrak{o} = \{x \in K \mid v(x) \ge 0\} = \{x \in K \mid |x| \le 1\}$$

is a ring with group of units

$$\mathfrak{o}^* = \{x \in K \mid v(x) = 0\} = \{x \in K \mid |x| = 1\}$$

and the unique maximal ideal

$$\mathfrak{p} = \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x| < 1\}.$$

o is an integral domain with field of fractions K and has the property that, for every $x \in K$, either $x \in o$ or $x^{-1} \in o$. Such a ring is called a valuation ring. Its only maximal ideal is $\mathfrak{p} = \{x \in o \mid x^{-1} \notin o\}$. The field $o/\mathfrak{p}$ is called the residue class field of o. A valuation ring is always integrally closed. For if $x \in K$ is integral over o, then there is an equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with $a_i \in o$ and the hypothesis $x \notin o$, so that $x^{-1} \in o$, would imply the contradiction $x = -a_1 - a_2 x^{-1} - \cdots - a_n (x^{-1})^{n-1} \in o$.

An exponential valuation v is called discrete if it admits a smallest positive value s. In this case, one finds

$$v(K^*) = s\mathbb{Z}.$$

It is called normalized if $s = 1$. Dividing by s we always pass to a normalized valuation without changing the invariants. Having done so, an element

$$\pi \in o \quad \text{such that} \quad v(\pi) = 1$$

is a prime element, and every element $x \in K^*$ admits a unique representation

with $m \in \mathbb{Z}$ and $u \in$ For if $v(x) = m$, then $v(x\pi^{-m}) = 0$, hence $u = x\pi^{-m} \in$

(3.9) Proposition. *If v is a discrete exponential valuation of K, then*

$$o = \{x \in K \mid v(x) \geq 0\}$$

is a principal ideal domain, hence a discrete valuation ring (see I, (11.3)).

Suppose v is normalized. Then the nonzero ideals of o are given by

$$\mathfrak{p}^n = \pi^n o = \{x \in K \mid v(x) \geq n\}, \quad n \geq 0,$$

where π is a prime element, i.e., $v(\pi) = 1$. One has

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong o/\mathfrak{p}.$$

Proof: Let $\mathfrak{a} \neq 0$ be an ideal of o and $x \neq 0$ an element in $\mathfrak{a}$ with smallest possible value $v(x) = n$. Then $x = u\pi^n$, $u \in o^*$, so that $\pi^n o \subseteq \mathfrak{a}$. If $y = \varepsilon\pi^m \in \mathfrak{a}$ is arbitrary with $\varepsilon \in o^*$, then $m = v(y) \geq n$, hence $y = (\varepsilon\pi^{m-n})\pi^n \in \pi^n o$, so that $\mathfrak{a} = \pi^n o$. The isomorphism

$$p^n/p^{n+1} \cong \mathfrak{o}/p$$

remits from the correspondence $a\pi^n \mapsto a \bmod p$. □

In a discretely valued field K the chain

$$\mathcal{o} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \cdots$$

consisting of the ideals of the valuation ring $\mathcal{o}$ forms a basis of neighbourhoods of the zero element. Indeed, if v is a normalized exponential valuation and $|\ | = q^{-v}$ $(q > 1)$ an associated multiplicative valuation, then

$$\mathfrak{p}^n = \left\{x \in K \;\Big|\; |x| < \frac{1}{q^{n-1}}\right\}.$$

As a basis of neighbourhoods of the element 1 of K^*, we obtain in the same way the descending chain

$$\mathcal{o}^* = U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots$$

of subgroups

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{x \in K^* \;\Big|\; |1-x| < \frac{1}{q^{n-1}}\right\}, \qquad n > 0,$$

of $\mathcal{o}^*$. (Observe that $1 + \mathfrak{p}^n$ is closed under multiplication and that, if $x \in U^{(n)}$, then so is x^{-1} because $|1 - x^{-1}| = |x|^{-1}|x - 1| = |1 - x| < \frac{1}{q^{n-1}}$.) $U^{(n)}$ is called the n-th **higher unit group** and $U^{(1)}$ the group of **principal units.** Regarding the successive quotients of the chain of higher unit groups, we have the

(3.10) Proposition. $\mathcal{o}^*/U^{(n)} \cong (\mathcal{o}/\mathfrak{p}^n)^*$ *and* $U^{(n)}/U^{(n+1)} \cong \mathcal{o}/\mathfrak{p}$, *for* $n \geq 1$.

Proof: The first isomorphism is induced by the canonical and obviously surjective homomorphism

$$\mathcal{o}^* \longrightarrow (\mathcal{o}/\mathfrak{p}^n)^*, \quad u \longmapsto u \bmod \mathfrak{p}^n,$$

the kernel of which is $U^{(n)}$. The second isomorphism is given, once we choose a prime element π, by the surjective homomorphism

$$U^{(n)} = 1 + \pi^n \mathcal{o} \longrightarrow \mathcal{o}/\mathfrak{p}, \qquad 1 + \pi^n a \longmapsto a \bmod \mathfrak{p},$$

which has kernel $U^{(n+1)}$. □

Exercise 1. Show that $|z| = (z\bar{z})^{1/2} =$ JIN.c1IR(z)I is the only valuation of C which extends the absolute value | | of ℝ

Exercise 2. What i� the relation between the Chinese remainder theorem and the approximation theorem (3.4)?

Exerci�e 3. Let k be a field and $K = k(t)$ the function field in one variahle. Show that the valuation� Vp as�ociated to the prime ideals p = (p(tJ) of $k[t]$, together with the degree valuation v.,._,. are lhe only valuations of K. up to eqrnvalenee. What are the residue das� field�?

Exercise 4. Let o he an arbitrary valuat10n rmg with field of fraction� K, and let $I' =$ Then r becomes a totally ordered group if we define rmodo*:::y o•tomean.x/yEO.

Write r additively and show that the function

v:K------'>- I'U{cx:::},

v(O) = ex::. v(.t) = x mod o• for x EK', satisfies the conditions

I) v{x) =ex::-==} $x = 0$,

2) v(ry) = $v(x)$ + v(r),

3) v(r + y) ;=:- min{v(r), v(y)).

v is called a Krull valuation.

§ 4. Completions

(4.1) Definition. *A valued* field *(K,* I I) *is called* complete if *every Cauchy* .�*equencc [a*$_{11}$lnect� *in* K converges *to an element a* E K, i.e.,

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Here, as usual. we call {a$_{11}$}$_{11}$Er, a Cauchy sequence if for every F > 0 there exists N E N such that

la$_{11}$*-aml<F* forall *n.m:=:N.*

From any valued field *(K,* I I) we get a complete valued field (R.1 I) by the process of completion. Thi� completion is obtained in the same way as the field of real numbers i� com,tructed from the field of rational numbers.

Take the ring R of all Cauchy sequences of *(K,* I I), consider therein the maximal ideal m of all nulbequem:es with respect to I I, and define

fi�*R/m.*

One embeds the tield K inlo f by sending every a E K to the class of the constant Cauchy sequence *(a.a.a, ...).* The valuation I I is extended from K to f by giving the clement a E R which is represented by lhc Cauchy sequence {an}nEN the absolute value

$$|a| = }�mx\ |a_n|.$$

This limit exisb because I $|a_{11}|$ - $|am_{11}|$.:S $|a_{11}$- $am|$ implies that $|an|$ is a Cauchy sequence of real numbers. As in the case of the field of real numbers, one proves that f is complete with respect lo the extended I I, and that each a E f is a limit of a sequence *{au)* in K. Finally one proves the uniqueness of the completion cR. I I): if cf'.I n is another complete valued field that contains *(K,* 1 I) a" a dense subfield, then mapping

gives a K-isomorphi5m *o:* R -+ R^1 such that $|a| = |aa|'$

The fields IR and C are the most familiar examples of complete fields. They are complete with rc5pccl to an archimedean valuation. Amazingly enough, there are no others of this type. More precisely we have the

(4.2) Theorem (Osrnowm). Let *K be a field which* i.� *complete with* respect to *an* an:himcdean valuation I I. *Then* there *is* cm isomorphism *er* from *K onto* IR or C *satisfying*

$$|a| = |aa|' \quad fora/J \quad a \in K.$$

for some *fixed s* E (0, I].

Proof: We may assume without l0'-5 of generality that R <:; K and that the valuat'.on I I of K i� an exten�ion of the usual absolute value of IR. In fact, replacing I I by I I�^{1} for a 5UJtable $s > 0$, we may assume by (3.7) that the restriction of I I lo Q is equal to the usual absolute value. Then taking the closure Q in K we find that ij is complete with to the restriction of I I to ij, in other words, it is a completion of I I). In of the uniqueness of completions, there is an isomorphi<;m a : IR -+ such that $|a| = |(Ja|$ as required.

In order to prove that K = IR or = C we 5how that each � E K satisfies a quadratic equation over R.. For this, consider the continuous function f : C -+ IR defined by

$$f(z) = |\xi^2 - (z + \bar{z})\xi + z\bar{z}|$$

Note here that $z+\bar z,\ z\bar z \in \mathbb{R} \subseteq K$. Since $\lim_{|z|\to\infty} f(z)=\infty$, $f(z)$ has a minimum m. The set

$$S=\{z\in\mathbb{C}\mid f(z)=m\}$$

is therefore nonempty, bounded, and closed, and there is a $z_0\in S$ such that $|z_0|\ge|z|$ for all $z\in S$. It suffices to show that $m=0$, because then one has the equation $z_0^2-(z_0+\bar z_0)z_0+z_0\bar z_0=0$.

Assume $m>0$. Consider the real polynomial

$$g(x)=x^2-(z_0+\bar z_0)x+z_0\bar z_0+\varepsilon,$$

where $0<\varepsilon<m$, with the roots $z_1,\bar z_1\in\mathbb{C}$. We have $z_1\bar z_1=z_0\bar z_0+\varepsilon$, hence $|z_1|>|z_0|$ and thus

$$f(z_1)>m.$$

For fixed $n\in\mathbb{N}$ consider on the other hand the real polynomial

$$G(x)=[g(x)-\varepsilon]^n-(-\varepsilon)^n=\prod_{i=1}^{2n}(x-\alpha_i)=\prod_{i=1}^{2n}(x-\bar\alpha_i)$$

with roots $\alpha_1,\dots,\alpha_{2n}\in\mathbb{C}$. It follows that $G(z_1)=0$; say, $z_1=\alpha_1$. We may substitute $x\in K$ into the polynomial

$$G(x)^2=\prod_{i=1}^{2n}\big(x^2-(\alpha_i+\bar\alpha_i)x+\alpha_i\bar\alpha_i\big)$$

and get

$$|G(x)|^2=\prod_{i=1}^{2n} f(\alpha_i)\ge f(\alpha_1)m^{2n-1}.$$

From this and the inequality

$$|G(x)|\le|x^2-(z_0+\bar z_0)x+z_0\bar z_0|^n+\varepsilon^n=f(z_0)^n+\varepsilon^n=m^n+\varepsilon^n,$$

it follows that $f(\alpha_1)m^{2n-1}\le(m^n+\varepsilon^n)^2$ and hence

$$\frac{f(\alpha_1)}{m}\le\left(1+\left(\frac{\varepsilon}{m}\right)^n\right)^2.$$

For $n\to\infty$ we have $f(\alpha_1)\le m$, which contradicts the inequality $f(\alpha_1)>m$ proved before. □

In view of Ostrowski's theorem, we will henceforth restrict attention to the case of nonarchimedean valuations. In this case it is usually expedient – both with regard to the substance and to practical technique – to work with the exponential valuations ꜀ rather than the multiplicative valuation5. So let v

be an exponential valuation of the field K. It is canonically continued to an exponential valuation $\hat{v}$ of the completion $\hat{K}$ by setting

$$\hat{v}(a) = \lim_{n\to\infty} v(a_n),$$

where $a = \lim_{n\to\infty} a_n$, $a_n \in K$. Observe here that the sequence $v(a_n)$ has to become stationary (provided $a \neq 0$) because, for $n \geq n_0$, one has $\hat{v}(a - a_n) > \hat{v}(a)$, so that it follows from the remark on p. 119

$$v(a_n) = \hat{v}(a_n - a + a) = \min\{\hat{v}(a_n - a), \hat{v}(a)\} = \hat{v}(a).$$

Therefore it follows that

$$v(K^*) = \hat{v}(\hat{K}^*),$$

and if v is discrete and normalized, then so is the extension $\hat{v}$. In the nonarchimedean case, for a sequence $\{a_n\}_{n\in\mathbb{N}}$ to be a Cauchy sequence, it suffices that $a_{n+1} - a_n$ be a nullsequence. In fact, $v(a_m - a_n) \geq \min_{n\leq i<m}\{v(a_{i+1} - a_i)\}$. By the same token an infinite series $\sum_{\nu=0}^{\infty} a_\nu$ converges in $\hat{K}$ if and only if the sequence of its terms a_ν is a nullsequence. The following proposition is proved exactly as its analogue, proposition (2.4), in the special case $(\mathbb{Q}, v_p)$.

(4.3) Proposition. *If $\mathcal{O} \subseteq K$, resp. $\hat{\mathcal{O}} \subseteq \hat{K}$, is the valuation ring of v, resp. of $\hat{v}$, and $\mathfrak{p}$, resp. $\hat{\mathfrak{p}}$, is the maximal ideal, then one has*

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$$

and, if v is discrete, one has furthermore

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n \quad \text{for } n \geq 1.$$

Generalizing the p-adic expansion to the case of an arbitrary discrete valuation v of the field K, we have the

(4.4) Proposition. *Let $R \subseteq \hat{\mathcal{O}}$ be a system of representatives for $\kappa = \hat{\mathcal{O}}/\hat{\mathfrak{p}}$ such that $0 \in R$, and let $\pi \in \mathcal{O}$ be a prime element. Then every $x \neq 0$ in $\hat{K}$ admits a unique representation as a convergent series*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

where $a_i \in R$, $a_0 \neq 0$, $m \in \mathbb{Z}$.

Proof: Let $x = \pi^{m}u$ with $u \in \mathcal{O}^*$. Since $\mathcal{O}/\mathfrak{p} \cong \mathfrak{o}/\mathfrak{p}$, the class $u \bmod \mathfrak{P}$ has a unique representative $a_0 \in R$, $a_0 \neq 0$. We thm have $u = a_0 + \pi b_1$, for some $b_1 \in \mathcal{O}$. Assume now that $a_0, \dots, a_{n-1} \in R$ have been found, safo,fying

$$u = a_0 + a_1\pi + \dots + a_{n-1}\pi^{n-1} + \pi^{n} b_n$$

for some $b_n \in \mathcal{O}$, and that the a_i are uniquely detennined by this equation. Then the representative $a_n \in R$ of $b_n \bmod \pi\mathcal{O} \in$;:: uniquely detennined by u and we have $b_n =$ E 3. Hence

$$u = a_0 + a_1\pi + \dots + a_{n-1}\pi^{n-1} + a_n\pi^{n} + \pi^{n+1}b_{n+1}$$

In this way we find an infinite series $\sum a_\nu \pi^\nu$ which is uniquely detennined by u. It converges to u because the remainder tenn $\pi^{n+1} b_{n+1}$ tends to zero. □

In the case of the field of rational numbers $\mathbb{Q}$ and the p-adic valuation v_p with its completion $\mathbb{Q}_p$, the numbers $0, 1, \dots, p-1$ fonn a sy5tem of repre�entatives R for the residue class field $\mathbb{Z}/p\mathbb{Z}$ of the valuation, and we gel back the representation of p-adic numbers which has already been discussed in §2:

$$x = p^{m}(a_0 + a_1p + a_2p^2 + \cdots),$$

where $0 \le a_i < p$ and $m \in \mathbb{Z}$.

In the case of the rational function field $k(t)$ and the valuation $v_\mathfrak{p}$ attached to a prime ideal $\mathfrak{p} = (t-a)$ of $k[t]$ (see S2), we may take as a system of representatives R the field of coefficients k itself. The completion then turns out to be the **field of formal power series** $k((x))$, $x = t - a$, consisting of all fonnal Laurent 5crics

$$f(t) = (t-a)^m(a_0 + a_1(t-a) + a_2(t-a)^2 + \cdots),$$

with $a_i \in k$ and $m \in \mathbb{Z}$. The motivating analogy of the beginning of thi� chapter, between power serie� and p-adic numbers. thus appears as two �pccial instances of the same concrete mathematical situation.

In § 1 we identified the ring $\mathbb{Z}_p$ of *p-adic* integers as being the projective limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. We obtain a similar result **in** the general setting of valuation theory. To explain thi�, let K be complete with respect to a discrete valuation. Let $\mathcal{O}$ be the valuation ring with the maximal ideal $\mathfrak{p}$. We then have for every $n \ge 1$ the canonical homomorphisms

$$\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}^n$$

and

$$\mathfrak{o}/\mathfrak{p} \leftarrow \mathfrak{o}/\mathfrak{p}^2 \leftarrow \mathfrak{o}/\mathfrak{p}^3 \leftarrow \cdots.$$

This gives us a homomorphism

$$\mathfrak{o} \longrightarrow \varprojlim_n \mathfrak{o}/\mathfrak{p}^n$$

into the projective limit

$$\varprojlim_n \mathfrak{o}/\mathfrak{p}^n = \Big\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathfrak{o}/\mathfrak{p}^n \;\Big|\; \lambda_n(x_{n+1}) = x_n \Big\}.$$

Considering the rings $\mathfrak{o}/\mathfrak{p}^n$ as topological rings for the discrete topology, gives us the product topology on $\prod_{n=1}^{\infty} \mathfrak{o}/\mathfrak{p}^n$ and the projective limit $\varprojlim_n \mathfrak{o}/\mathfrak{p}^n$ becomes a topological ring in a canonical way, being a closed subset of the product (see chap. IV, §2).

(4.5) Proposition. *The canonical mapping*

$$\mathfrak{o} \longrightarrow \varprojlim_n \mathfrak{o}/\mathfrak{p}^n$$

is an isomorphism and a homeomorphism. The same is true for the mapping

$$\mathfrak{o}^* \longrightarrow \varprojlim_n \mathfrak{o}^*/U^{(n)}.$$

Proof: The map is injective since its kernel is $\bigcap_{n=1}^{\infty} \mathfrak{p}^n = (0)$. To prove surjectivity, let $\mathfrak{p} = \pi\mathfrak{o}$ and let $R \subseteq \mathfrak{o}$, $R \ni 0$, be a system of representatives of $\mathfrak{o}/\mathfrak{p}$. We saw in the proof of (4.4) (and in fact already in (1.2)) that the elements $a \bmod \mathfrak{p}^n \in \mathfrak{o}/\mathfrak{p}^n$ can be given uniquely in the form

$$a \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \bmod \mathfrak{p}^n,$$

where $a_i \in R$. Each element $x \in \varprojlim_n \mathfrak{o}/\mathfrak{p}^n$ is therefore given by a sequence

$$s_n = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}, \quad n = 1, 2, \ldots,$$

with fixed coefficients $a_i \in R$, and it is thus the image of the element $x = \lim_{n\to\infty} s_n = \sum_{\nu=0}^{\infty} a_\nu \pi^\nu \in \mathfrak{o}$.

The sets $P_n = \prod_{\nu \geq n} \mathfrak{o}/\mathfrak{p}^\nu$ form a basis of neighbourhoods of the zero element of $\prod_{\nu=1}^{\infty} \mathfrak{o}/\mathfrak{p}^\nu$. Under the bijection the basis of neighbourhoods $\mathfrak{p}^n$ of zero in $\mathcal{O}$ is mapped onto the basis of neighbourhoods $P_n \cap \varprojlim \mathcal{O}/\mathfrak{p}^\nu$ of zero in $\varprojlim \mathcal{O}/\mathfrak{p}^\nu$. Thus the bijection is a homeomorphism. It induces an isomorphism and homeomorphism on the group of units

$$\mathcal{O}^* \cong (\varprojlim \mathcal{O}/\mathfrak{p}^n)^* \cong \varprojlim (\mathcal{O}/\mathfrak{p}^n)^* \cong \varprojlim \mathcal{O}^*/U^{(n)}. \qquad \square$$

One of our chief concerns will be to study the finite extensions $L|K$ of a complete valued field K. This means that we have to turn to the question of factoring algebraic equations

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

over complete valued fields. For this, Hensel's seminal "lemma" is of fundamental importance. Let K again be a field which is complete with respect to a nonarchimedean valuation $|\ |$. Let $\mathcal{O}$ be the corresponding valuation ring with maximal ideal $\mathfrak{p}$ and residue class field $\kappa = \mathcal{O}/\mathfrak{p}$. We call a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathcal{O}[x]$ primitive if $f(x) \not\equiv 0 \mod \mathfrak{p}$, i.e., if

$$|f| = \max\{|a_0|, \ldots, |a_n|\} = 1.$$

(4.6) Hensel's Lemma. *If a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits modulo $\mathfrak{p}$ a factorization*

$$f(x) \equiv \bar{g}(x)\bar{h}(x) \mod \mathfrak{p}$$

into relatively prime polynomials $\bar{g}, \bar{h} \in \kappa[x]$, then $f(x)$ admits a factorization

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}[x]$ such that $\deg(g) = \deg(\bar{g})$ and

$$g(x) \equiv \bar{g}(x) \mod \mathfrak{p} \quad \text{and} \quad h(x) \equiv \bar{h}(x) \mod \mathfrak{p}.$$

Proof: Let $d = \deg(f)$, $m = \deg(\bar{g})$, hence $d - m \geq \deg(\bar{h})$. Let $g_0, h_0 \in \mathcal{O}[x]$ be polynomials such that $g_0 \equiv \bar{g} \mod \mathfrak{p}$, $h_0 \equiv \bar{h} \mod \mathfrak{p}$ and $\deg(g_0) = m$, $\deg(h_0) \leq d - m$. Since $(\bar{g}, \bar{h}) = 1$, there exist polynomials $a(x), b(x) \in \mathcal{O}[x]$ satisfying $ag_0 + bh_0 \equiv 1 \mod \mathfrak{p}$. Among the coefficients of the two polynomials $f - g_0 h_0$ and $ag_0 + bh_0 - 1 \in \mathfrak{p}[x]$ we pick one with minimum value and call it π.

Lel m, look for the polynomials g and h in the following fonn:

$$g=go+p1n+p2n^2+$$
$$h = ho +q1n +t12n^2 + \cdot$$

where p_{1}, q, E o[x] are polynomials of degree < m. resp. :'.::: d - m. We then determine successively the polynomials

!?n-1 =Ro+ P1JT + · · · + Pn 1Jfn-l,

hn-1 =ho+ q1n +· · · + q,,_1nn-l,

in such a way that one has

$$f \equiv g_{n-1} h_{n-1} \bmod \pi^n$$

Passing lo the limit as n --+ oo, we will finally obtain the identity $f = gh$. For $n = 1$ the congruence is satisfied in view of our choice of ;r. Lel us aswme thal it is already e�tablished for some n �I. Then, in view of the relation

$$g_n = g_{n-1} + p_n \pi^n, \quad h_n = h_{n-1} + q_n \pi^n,$$

lhe condition on g,,.h11reduces to

$$f - g_{n-1} h_{n-1} \equiv (g_{n-1} q_n + h_{n-1} p_n) \pi^n \bmod \pi^{n+1}$$

Dividing by n", this meam

$$g_{n-1} q_n + h_{n-1} p_n \equiv g_0 q_n + h_0 p_n \equiv f_n \bmod \pi,$$

where j� = Jf-IIu- ffo-1hn- i) E oLxJ. Since goa + hoh = I mod Jr, has

Roaf�+ hoh/11 = fn mod IT.

At this point we would like lo put qn = af;, and p11= hf;,, but the degrees might be too big. For this reason, we write

h(x)fn(.r) = q(.,),:o(x) + P11(x),

where deg(p11) < deg(i;:-0) = m. Since = 8 mod p and deg(Ro) = deg(!{), the highest cocfllcient of ,:₀ i� a unit: q(r) E o[x] and we obtain the congruence

go(afn + hoq) + hoJJ11 = !11 mod Jf.

Omitting now from the polynomial af11+ h0q all coefficients divisible by :rr, we get a polynomial q11such that g0q11+ h0p11= f,, mod ;r and which, in view of deg(.f�) :'.::: d, deg(g = m and deg(hp < (d - m) + m = d, has degree :'.::: d - m as required. □

Example: The polynomial $x^{p-1}-1 \in \mathbb{Z}_p[x]$ splits over the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ into distinct linear factors. Applying (repeatedly) Hensel's lemma, we see that it also splits into linear factors over $\mathbb{Z}_p$. We thus obtain the astonishing result that the field $\mathbb{Q}_p$ of p-adic numbers contains the $(p-1)$-th roots of unity. These, together with 0, even form a system of representatives for the residue class field, which is closed under multiplication.

(4.7) Corollary. *Let the field K be complete with respect to the nonarchimedean valuation $|\ |$. Then, for every irreducible polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ such that $a_0a_n \neq 0$, one has*

$$|f| = \max\{|a_0|, |a_n|\}.$$

In particular, $a_n = 1$ and $a_0 \in \mathcal{O}$ imply that $f \in \mathcal{O}[x]$.

Proof: After multiplying by a suitable element of K we may assume that $f \in \mathcal{O}[x]$ and $|f| = 1$. Let a_r be the first one among the coefficients $a_0, \dots, a_n$ such that $|a_r| = 1$. In other words, we have

$$f(x) \equiv x^r(a_r + a_{r+1}x + \cdots + a_nx^{n-r}) \bmod \mathfrak{p}.$$

If one had $\max\{|a_0|,|a_n|\} < 1$, then $0 < r < n$ and the congruence would contradict Hensel's lemma. □

From this corollary we can now deduce the following theorem on extensions of valuations.

(4.8) Theorem. *Let K be complete with respect to the valuation $|\ |$. Then $|\ |$ may be extended in a unique way to a valuation of any given algebraic extension $L|K$. This extension is given by the formula*

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|},$$

when $L|K$ has finite degree n. In this case L is again complete.

Proof: If the valuation $|\ |$ is archimedean, then by Ostrowski's theorem, $K = \mathbb{R}$ or $\mathbb{C}$. We have $N_{\mathbb{C}|\mathbb{R}}(z) = z\bar{z} = |z|^2$ and the theorem is part of classical analysis. So let $|\ |$ be nonarchimedean. Since every algebraic extension $L|K$ is the union of its finite subextensions, we may assume that the degree $n = [L:K]$ is finite.

Existence of the extended valuation: let $\mathfrak{o}$ be the valuation ring of K and $\mathcal{O}$ its integral closure in L. Then one has

$$\mathcal{O} = \{\alpha \in L \mid N_{L|K}(\alpha) \in \mathfrak{o}\}. \quad (*)$$

The implication $\alpha \in \mathcal{O} \Rightarrow N_{L|K}(\alpha) \in \mathfrak{o}$ is evident (see chap. I, § 2, p. 12). Conversely, let $\alpha \in L^*$ and $N_{L|K}(\alpha) \in \mathfrak{o}$. Let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$$

be the minimal polynomial of α over K. Then $N_{L|K}(\alpha) = \pm a_0^m \in \mathfrak{o}$, so that $|a_0| \le 1$, i.e., $a_0 \in \mathfrak{o}$. By (4.7) this gives $f(x) \in \mathfrak{o}[x]$, i.e., $\alpha \in \mathcal{O}$.

For the function $|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|}$, the conditions $|\alpha| = 0 \Leftrightarrow \alpha = 0$ and $|\alpha\beta| = |\alpha||\beta|$ are obvious. The strong triangle inequality

$$|\alpha + \beta| \le \max\{|\alpha|, |\beta|\}$$

reduces, after dividing by α or β, to the implication

$$|\alpha| \le 1 \Rightarrow |\alpha + 1| \le 1,$$

and then, by (*), to $\alpha \in \mathcal{O} \Rightarrow \alpha + 1 \in \mathcal{O}$, which is trivially true. Thus the formula $|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|}$ does define a valuation of L, and, restricted to K, it clearly gives back the given valuation. Equally obviously it has $\mathcal{O}$ as its valuation ring.

Uniqueness of the extended valuation: let $|\ |'$ be another extension with valuation ring $\mathcal{O}'$. Let $\mathfrak{P}$, resp. $\mathfrak{P}'$, be the maximal ideal of $\mathcal{O}$, resp. $\mathcal{O}'$. We show that $\mathcal{O} \subseteq \mathcal{O}'$. Let $\alpha \in \mathcal{O} \setminus \mathcal{O}'$ and let

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$$

be the minimal polynomial of α over K. Then one has $a_1, \dots, a_d \in \mathfrak{o}$ and $\alpha^{-1} \in \mathfrak{P}'$, hence $1 = -a_1\alpha^{-1} - \cdots - a_d(\alpha^{-1})^d \in \mathfrak{P}'$, a contradiction. This shows the inclusion $\mathcal{O} \subseteq \mathcal{O}'$. In other words, we have that $|\alpha| \le 1 \Rightarrow |\alpha|' \le 1$ and this implies that the valuations $|\ |$ and $|\ |'$ are equivalent. For if they were not, then the approximation theorem (3.4) would allow us to find an $\alpha \in L$ such that $|\alpha| \le 1 \Rightarrow |\alpha|' > 1$. Thus $|\ |$ and $|\ |'$ are equal because they agree on K.

The fact that L is again complete with respect to the extended valuation is deduced from the following general result. □

(4.9) Proposition. *Let K be complete with respect to the valuation $|\ |$ and let V be an n-dimensional normed vector space over K. Then, for any basis $v_1, \dots, v_n$ of V the maximum norm*

$$\|x_1 v_1 + \cdots + x_n v_n\| = \max\{|x_1|, \dots, |x_n|\}$$

is *equivalent to the given norm on \I. In* parlicufar, *\I* is *complete and the i.mmorp/Jism*

$$K^n \longrightarrow V\,, \quad (x_1, \dots, x_n) \longmapsto x_1v_1 + \cdots + x_nv_n\,,$$

is a *homeomorphism.*

Proof: Let v1. . *Vn* be a basi5 and II II be the corre�ponding maximum norm on *\I.* It suffices to show that, for every nonn I l on *V,* there exist constants *p, p'* > 0 such that

Pllxll :':: lxl :':: p'llxll for all .t EV.

Then the norm I I defines the same topology on *V* m, the norm II II. and we obtain the topological isomorphism K^{11} ➔ *V,* (x1, ... *Xn)*r--?' x1v1 +· ·+*x11vn.* In fact. II II b transformed intotbemaximum norm on *Kn.*

For *p'* we may obviously take lv11 + •·· + lv,,I. The existence of pis proved by induction on *n.* For *n* = l we may take *p* = Iv11- Suppose that everything is proved for *(n* - [)-dimensional vector spaces. Let

V1=Kv1+ +Kv,_1+Kv1r1+ +Kv,,.

so that *V* = V1 + *Kv,.* Then *V,* i5 complete with respect to the restriction of I I by induction, hence it is clo�cd in *V.* Thus *V,* + *v,* is also closed. Since Of/. LJ�=l (\/; + 1•1), there exists a neighbourhood of O which is disjoint from U;1=l*W1* + *V1),* i.e., there exbb *p* > 0 such that

Ill.'1 + *v,* I 2:. *p* for all *w,* E *V;* and all i = 1.

For *x* = x1v1 + • +.1,,v,, -=*I*- 0 and Ix, l= max{lx11}, one finds

+*v,* + 2:. *p.*

�o that one has lxl 2:. *pix,* I= Pllxll. □

The fact that an exponential valuation *v* on *K* a%ociatcd with I I extends uniquely to *L* is a trivial consequence of theorem (4.8). The extension *w* is given by the formula

$$w(\alpha) = \frac{1}{n}\,v\big(N_{L|K}(\alpha)\big)$$

ifn = [L: Kl< oc.

Exercise 1. An infinite algebrail'. cxtcn�ion of a complete field K is never complete.

Exercise 2. Lct $X_0, X_1, \ldots$ be an infinite sequence of unknowns, p a fixed prime number and 0. Show that there exist polynomial� ... I �uch that

W''(Sn.S1,)=W,,(Xo.X,.. J+Wn(Yo,Y1 ......).

W/)(Po, P1, ...) = Wn(Xu,X1 ....) W,,(Yo. Y1,.

Exerci�e 3. Let A he a commutative ring. For $a=$ $(a_0,a_1\cdot\ldots).h=(h_0.h_1\cdot\cdot)$, a,,h,EA,put

$$a+h=(S_0(a,h).8_1(a,h),\ldots),\quad a\cdot h=(Po(a,h).P_1(a.h),\ldots\ldots).$$

Show that with the\e operation\ the vectors $a=(a_0,$ ll$_1,$ form a commutat1ve ring $W(A)$ with I. It is rnllcd the ring of Witt vectors over

Exercise 4. Assume $pA=0$. For every Will vector $a=(a_0,a_1,\ldots)$ E $W(A)$ consider the "gho�t component�"

a1,,1 = W,,(a) =a{+ pa(·'+ ··+ p/)a''

a� well as the mapping\ V.F: $W(A)$----+ $W(A)$ defined hy

Va= (0,an,l/1, ...) and Fu= (u(;.u('.......),

called re�pectively "trnm,fer" ("Ver�chiebung" in German) and "Frobeniu5" Show that

(Va/'''= pa'''-11 and a'''1 = (Fa)'''1 + p''a11.

Exercise 5. Let A be a field of charactcristJC p. Then V 1� a homomorphism of the additive group of $W(A)$;-iml Fis ;-iring homomorphism, and one ha\

\!Fa= F\la = pa.

Exercise 6. If A 1� a perfect field of charactens11c p, then $W(k)$ 1� a complete 1.facrelc valuat10n ring with residue cla�� field L

§ 5. Local Fields

Among all complete (nonarchimedean) valued field5, tho�e arising as completions of a global field, i.e., of a finite extension of either IQ or l�'p(t), have the most eminent relevance for number theory. The valuation on rnch a completion is discrete and has a finite residue da�� field, as we shall see �hortly. In contrast to the global field5. all field� which are complete with respect to a discrete valuation and have a finite residue cla�� field are called local fields. For such a local field. the normalized exponential valuation is denoted by l'p, and I Ip denote� the absolute value normalized by

\x\p = (/-l'µh) _

where q is the cardinality of the residue class field.

(5.1) Proposition. *A local field K is locally compact. Its valuation ring $\mathcal{O}$ is compact.*

Proof: By (4.5) we have $\mathcal{O} \cong \varprojlim_n \mathcal{O}/\mathfrak{p}^n$, both algebraically and topologically. Since $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$ (see (3.9)), the rings $\mathcal{O}/\mathfrak{p}^n$ are finite, hence compact. Being a closed subset of the compact product $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$, it follows that the projective limit $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$, and thus $\mathcal{O}$, is also compact. For every $a \in K$, the set $a + \mathcal{O}$ is an open, and at the same time compact neighbourhood, so that K is locally compact. □

In happy concord with the definition of global fields as the finite extensions of $\mathbb{Q}$ and $\mathbb{F}_p(t)$, we now obtain the following characterization of local fields.

(5.2) Proposition. *The local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.*

Proof: A finite extension K of $k = \mathbb{Q}_p$ or $k = \mathbb{F}_p((t))$ is again complete, by (4.8), with respect to the extended valuation $|\alpha| = |N_{K|k}(\alpha)|^{1/n}$, which itself is obviously again discrete. Since $K|k$ is of finite degree, so is the residue class field extension: for if $\bar{x}_1, \dots, \bar{x}_n \in \kappa$ are linearly independent, then any choice of preimages $x_1, \dots, x_n \in K$ is linearly independent over k. Indeed, dividing any nontrivial k-linear relation $\lambda_1 x_1 + \dots + \lambda_n x_n = 0$, $\lambda_i \in k$, by the coefficient λ_i with biggest absolute value, yields a linear combination with coefficients in the valuation ring of k with 1 as i-th coefficient, from which we obtain a nontrivial relation $\bar{\lambda}_1 \bar{x}_1 + \dots + \bar{\lambda}_n \bar{x}_n = 0$ by reducing to κ. Therefore K is a local field.

Conversely, let K be a local field, v its discrete exponential valuation, and p the characteristic of its residue class field κ. If K has characteristic 0, then the restriction of v to $\mathbb{Q}$ is equivalent to the p-adic valuation v_p of $\mathbb{Q}$ because $v(p) > 0$. In view of the completeness of K, the closure of $\mathbb{Q}$ in K is the completion of $\mathbb{Q}$ with respect to v_p, in other words $\mathbb{Q}_p \subseteq K$. The fact that $K|\mathbb{Q}_p$ is of finite degree results from the local compactness of the vector space K, by a general theorem of topological linear algebra (see [18], chap. I, §2, no. 4, th. 3), but it also follows from (6.8) below. If on the other hand the characteristic of K is not equal to zero, then it has to equal p. In this case we find $K = \kappa((t))$, for a prime element t of K (see p.127), hence $\mathbb{F}_p((t)) \subseteq K$. In fact, if $\kappa = \mathbb{F}_p(\alpha)$ and $p(X) \in \mathbb{F}_p[X] \subseteq K[X]$ is the minimal polynomial of α over $\mathbb{F}_p$, then, by Hensel's lemma, $p(X)$ splits over K into linear factors. We may therefore view κ as a subfield of K, and then the elements of K turn out to be, by (4.4), the Laurent series in t with coefficients in κ. □

Remark: One can show that a field K which is locally compact with respect to a nondiscrete topology is isomorphic either to $\mathbb{R}$ or $\mathbb{C}$, or to a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, i.e., to a local field (see [137], chap. I, §3).

We have just seen that the local fields of characteristic p are the power series fields $\mathbb{F}_q((t))$, with $q = p^f$. The local fields of characteristic 0, i.e., the finite extensions $K|\mathbb{Q}_p$ of the fields of p-adic numbers $\mathbb{Q}_p$, are called p-adic number fields. For them one has an *exponential function* and a *logarithm function*. In contrast to the real and complex case, however, the former is not defined on all of K, whereas the latter is given on the whole multiplicative group K^*. For the definition of the logarithm we make use of the following fact.

(5.3) Proposition. *The multiplicative group of a local field K admits the decomposition*

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)}.$$

Here π is a prime element, $(\pi) = \{\pi^k \mid k \in \mathbb{Z}\}$, $q = \#\kappa$ is the number of elements in the residue class field $\kappa = \mathcal{O}/\mathfrak{p}$, and $U^{(1)} = 1 + \mathfrak{p}$ is the group of principal units.

Proof: For every $a \in K^*$, one has a unique representation $a = \pi^n u$ with $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$, so that $K^* = (\pi) \times \mathcal{O}^*$. Since the polynomial $X^{q-1} - 1$ splits into linear factors over $\mathcal{O}$ by Hensel's lemma, $\mathcal{O}^*$ contains the group μ_{q-1} of $(q-1)$-th roots of unity. The homomorphism $\mathcal{O}^* \to \kappa^*$, $u \mapsto u \bmod \mathfrak{p}$, has kernel $U^{(1)}$ and maps μ_{q-1} bijectively onto κ^*. Hence $\mathcal{O}^* = \mu_{q-1} \times U^{(1)}$. $\square$

(5.4) Proposition. For a p-adic *number field K* there *is* a *uniquely determined continuous homomorphism*

$$\log : K^* \to K$$

such that $\log p = 0$ *which on principal units* $(1+x) \in U^{(1)}$ *is* given *by the series*

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots.$$

Proof: By §4, we can think of the p-adic valuation v_p of $\mathbb{Q}_p$ as extended to K. Observing that $v_p(x) > 0$, so that $c = p^{v_p(x)} > 1$, and $p^{v_p(\nu)} \le \nu$, giving $vp(v)$,:S ? (with the w,ual logarithm), we compute the valuation of the tenm, x''/v of the series,

$$v_p(\frac{x^{1'})}{-;} = vv_{P(X)-} \quad 1!,,(v) ? \; v \; \frac{\text{Inc}}{\text{In}_p} - \frac{Inv}{?} = \frac{\ln(c''/v)}{} \; = Inp.$$

This show<, that xv/v is a nullsequcnce, i.e., the logarithm series converges. It defines a homomorphi?m because

$$\log((! +x)(l + y)) ? \log(! +x)+\log(l +y)$$

is an identity of fonnal power series and all serie? in it converge provided l+x,l+yEU(ll_

For every a E K^*, choo,;ing a prime element TC, we have a unique representation

$$a= TC^{1'}p(a)w(a)(O!),$$

where $v_p = evf'$ is the nonnalized valuation of K. $w(a)$ E /1--q-l, (a) E u(IJ. As sugge?ted by the equation $p = TCew(p)(p)$, we define log $TC = -\}$ log (p) and thus obtain the homomorphism log: K^* --+ K by

$$\log a= v_p(U') \log TC+ \log (a).$$

Il is obviously continuous and has the property that log $p = 0$. If A: K^* ---+ K is any continuation of log : ij(ll --+ K such that $A(p) = 0$, then we find that A(s'') = ?A(t'' ^{1}) = 0 for each t E /.L$_{11}$_1. It follows that 0 = $eA(TC)$ + A((p)) = eA(TC) + log(p), so that A(TC) = log TC, and thus A(a) = vp(a)A(TC) +A({a)) = 1Jp(a) log TC+ log {a) = \oga, for all a E K^*. log is therefore uniquely detennined and independent of the choice of TC. LJ

(5.5) **Proposition.** *Let K* $|Q_1$, *be* a p-adic number *field with valuation* ring *o and maximal ide:il* p, and let *po=* i-,''. *Then the* power .?eries

$$\exp(x)= l+x+\frac{x2}{2!}+\frac{.\backslash}{3!}+\cdots,\text{md} \quad \log(!+,)?,-\frac{?2}{2}+\frac{7}{3}- -$$

yield, for n > -,;-=:-T, *two mutually* inverse *isomorphi.?ms* (and *homeomorphisms)*

$$\mathfrak{p}^n \underset{\longleftarrow}{\overset{\exp}{\longrightarrow}} U^{(n)}$$

We prepare the proof by the following elementary lemma.

(5.6) Lemma. Let $\nu = \sum_{i=0}^{r} a_i p^i$, $0 \le a_i < p$, be the p-adic expansion of the natural number $\nu \in \mathbb{N}$. Then

$$v_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^{r} a_i(p^i - 1).$$

Proof: Let $[c]$ signify the biggest integer $\le c$. Then we have

$$\begin{aligned}[\nu/p] &= a_1 + a_2 p + \cdots + a_r p^{r-1},\\ [\nu/p^2] &= a_2 + \cdots + a_r p^{r-2},\\ &\ \ \vdots\\ [\nu/p^r] &= a_r.\end{aligned}$$

Now we count how many numbers $1, 2, \dots, \nu$ are divisible by p, and then by p^2, etc. We find

$$v_p(\nu!) = [\nu/p] + \cdots + [\nu/p^r] = a_1 + (p+1)a_2 + \cdots + (p^{r-1} + \cdots + 1)a_r,$$

and hence

$$(p-1)v_p(\nu!) = (p-1)a_1 + (p^2-1)a_2 + \cdots + (p^r - 1)a_r = \sum_{i=0}^{r} a_i(p^i - 1).$$

$\square$

Proof of (5.5): We again think of the p-adic valuation v_p of $\mathbb{Q}_p$ as being extended to K. Then $v_{\mathfrak{p}} = e v_p$ is the normalized valuation of K. For every natural number $\nu > 1$, one has the estimate

$$\frac{v_p(\nu)}{\nu - 1} \le \frac{1}{p-1}.$$

For if $\nu = p^a \nu_0$, with $(\nu_0, p) = 1$ and $a > 0$, then

$$\frac{v_p(\nu)}{\nu-1} = \frac{a}{p^a\nu_0 - 1} \le \frac{a}{p^a - 1} = \frac{1}{p-1}\cdot\frac{a}{p^{a-1} + \cdots + 1} \le \frac{1}{p-1}.$$

For $v_p(z) > \frac{1}{p-1}$, $z \neq 0$, i.e., $v_{\mathfrak{p}}(z) > \frac{e}{p-1}$, this yields

$$v_p\Big(\frac{z^\nu}{\nu}\Big) - v_p(z) = (\nu - 1)v_p(z) - v_p(\nu) > (\nu - 1)\Big(\frac{1}{p-1} - \frac{v_p(\nu)}{\nu - 1}\Big) \ge 0,$$

and thus $v_p(\log(1+z)) = v_p(z)$. For $n > \frac{e}{p-1}$, log therefore maps $U^{(n)}$ into $\mathfrak{p}^n$.

For the exponential series $\sum_{\nu=0}^{\infty} \frac{z^\nu}{\nu!}$ we compute the valuations $v_p(\frac{z^\nu}{\nu!})$ as follows. Writing, for $\nu > 0$,

$$\nu = a_0 + a_1 p + \cdots + a_r p^r, \quad 0 \le a_i < p,$$

we get from (5.6) that

$$v_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^{r} a_i(p^i-1) = \frac{1}{p-1}\big(\nu-(a_0+a_1+\cdots+a_r)\big).$$

Putting $s_\nu = a_0+\cdots+a_r$, this becomes

$$v_p\Big(\frac{x^\nu}{\nu!}\Big) = \nu v_p(x) - \frac{\nu-s_\nu}{p-1} = \nu\Big(v_p(x)-\frac{1}{p-1}\Big)+\frac{s_\nu}{p-1}.$$

For $v_p(x) > \frac{1}{p-1}$, i.e., $v_\mathfrak{p}(x) > \frac{e}{p-1}$, this implies the convergence of the exponential series. If furthermore $x \neq 0$ and $\nu > 1$, then one has

$$v_\mathfrak{p}\Big(\frac{x^\nu}{\nu!}\Big) - v_\mathfrak{p}(x) = (\nu-1)v_\mathfrak{p}(x) - e\frac{\nu-s_\nu}{p-1} > (\nu-1)\frac{e}{p-1} - e\frac{\nu-s_\nu}{p-1} = e\frac{s_\nu-1}{p-1} \geq 0.$$

Therefore $v_\mathfrak{p}(\exp(x)-1) = v_\mathfrak{p}(x)$, i.e., for $n > \frac{e}{p-1}$, exp maps the group $\mathfrak{p}^n$ into $U^{(n)}$. Furthermore, one has for $v_\mathfrak{p}(x), v_\mathfrak{p}(z) > \frac{e}{p-1}$ that

$$\exp\log(1+z) = 1+z \quad\text{and}\quad \log\exp x = x,$$

for these are identities of formal power series and all of the series converge. This proves the proposition. □

For an arbitrary local field K, the group of principal units $U^{(1)}$ is a $\mathbb{Z}_p$-module (where $p = \operatorname{char}(\kappa)$) in a canonical way, i.e., for every $1+x \in U^{(1)}$ and every $z \in \mathbb{Z}_p$, one has the power $(1+x)^z \in U^{(1)}$. This is a consequence of the fact that $U^{(1)}/U^{(n+1)}$ has order q^n for all n (where $q = \#\mathcal{O}/\mathfrak{p}$ — the reason for this is that $U^{(i)}/U^{(i+1)} \cong \mathcal{O}/\mathfrak{p}$, by (3.10), so that $U^{(1)}/U^{(n+1)}$ is a $\mathbb{Z}/q^n\mathbb{Z}$-module) and of the formulas

$$U^{(1)} = \varprojlim_n U^{(1)}/U^{(n+1)} \quad\text{and}\quad \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/q^n\mathbb{Z}.$$

This obviously extends the $\mathbb{Z}$-module structure of $U^{(1)}$. The function

$$f(z) = (1+x)^z$$

is continuous because the congruence $z \equiv z' \bmod q^n\mathbb{Z}_p$ implies $(1+x)^z \equiv (1+x)^{z'} \bmod U^{(n+1)}$, so that the neighbourhood $z + q^n\mathbb{Z}_p$ of z is mapped to the neighbourhood $(1+x)^z U^{(n+1)}$ of $f(z)$. In particular, $(1+x)^z$ may be expressed as the limit

$$(1+x)^z = \lim_{k\to\infty}(1+x)^{z_k}$$

of ordinary powers $(1+x)^{z_k}$, $z_k \in \mathbb{Z}$, if $z = \lim_{k\to\infty} z_k$.

After this discussion we can now determine explicitly the structure of the locally compact multiplicative group K^* of a local field K.

(5.7) Proposition. *Let K be a local field and $q = p^f$ the number of elements in the residue class field. Then the following hold.*

(i) *If K has characteristic 0, then one has (both algebraically and topologically)*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

where $a \geq 0$ and $d = [K:\mathbb{Q}_p]$.

(ii) *If K has characteristic p, then one has (both algebraically and topologically)*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}.$$

Proof: By (5.3) we have (both algebraically and topologically)

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)} \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus U^{(1)}.$$

This reduces us to the computation of the $\mathbb{Z}_p$-module $U^{(1)}$.

(i) Assume $char(K) = 0$. For n sufficiently big, (5.5) gives us the isomorphism

$$\log : U^{(n)} \longrightarrow \mathfrak{p}^n = \pi^n \mathcal{O} \cong \mathcal{O}.$$

Since log, exp, and $f(z) = (1+z)^\alpha$ are continuous, this is a topological isomorphism of $\mathbb{Z}_p$-modules. By chap. I, (2.9), $\mathcal{O}$ admits an integral basis $\alpha_1, \ldots, \alpha_d$ over $\mathbb{Z}_p$, i.e., $\mathcal{O} = \mathbb{Z}_p\alpha_1 \oplus \cdots \oplus \mathbb{Z}_p\alpha_d \cong \mathbb{Z}_p^d$. Therefore $U^{(n)} \cong \mathbb{Z}_p^d$. Since the index $(U^{(1)} : U^{(n)})$ is finite and $U^{(n)}$ is a finitely generated $\mathbb{Z}_p$-module of rank d, so is $U^{(1)}$. The torsion subgroup of $U^{(1)}$ is the group μ_{p^a} of roots of unity in K of p-power order. By the main theorem on modules over principal ideal domains, there exists in $U^{(1)}$ a free, finitely generated, and therefore closed, $\mathbb{Z}_p$-submodule V of rank d such that

$$U^{(1)} = \mu_{p^a} \times V \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

both algebraically and topologically.

(ii) If $char(K) = p$, we have $K \cong \mathbb{F}_q((t))$ (see p. 127) and

$$U^{(1)} = 1 + \mathfrak{p} = 1 + t\mathbb{F}_q[[t]].$$

The following argument is taken from the book [79] of *K. Iwasawa*.

Let $\omega_1, \ldots, \omega_f$ be a basis of $\mathbb{F}_q|\mathbb{F}_p$. For every natural number n relatively prime to p we consider the continuous homomorphism

$$g_n : \mathbb{Z}_p^f \to U^{(n)}, \quad g_n(a_1, \ldots, a_f) = \prod_{i=1}^{f} (1 + \omega_i t^n)^{a_i}.$$

This function has the following properties. If $m = np^s$, $(n,p)=1$, $s \geq 0$, then

(1) $$U^{(m)} = g_n(p^s\mathbb{Z}_p^f)\,U^{(m+1)}$$

and, for $\alpha = (\alpha_1, \dots, \alpha_f) \in \mathbb{Z}_p^f$,

(2) $$\alpha \notin p\mathbb{Z}_p^f \iff g_n(p^s\alpha) \notin U^{(m+1)}.$$

Indeed, for $\omega = \sum_{i=1}^f a_i\omega_i$, $a_i \in \mathbb{Z}$, $a_i \equiv \alpha_i \bmod p$, we have

$$E_n(\alpha) \equiv \prod_{i=1}^f (1+\omega_i\pi^n)^{a_i} \equiv 1+\omega\pi^n \bmod \mathfrak{p}^{n+1}$$

and hence, since we are in characteristic p,

$$g_n(p^s\alpha) = g_n(\alpha)^{p^s} \equiv 1 + \omega^{p^s}\pi^m \bmod \mathfrak{p}^{m+1}.$$

As α varies over the elements of $\mathbb{Z}_p^f$, ω, and thus also ω^{p^s}, varies over the elements of $\mathbb{F}_q$, and we get (1). Furthermore one has $g_n(p^s\alpha) \equiv 1 \bmod \mathfrak{p}^{m+1} \iff \omega = 0 \iff a_i \equiv 0 \bmod p$, for $i = 1, \dots, f$ $\iff \alpha_i \equiv 0 \bmod p$, for $i = 1, \dots, f$ $\iff \alpha \in p\mathbb{Z}_p^f$, and this amounts to (2).

We now consider the continuous homomorphism of $\mathbb{Z}_p$-modules

$$g = \prod_{(n,p)=1} g_n : A = \prod_{(n,p)=1} \mathbb{Z}_p^f \longrightarrow U^{(1)},$$

where the product $\prod_{(n,p)=1} \mathbb{Z}_p^f$ is taken over all $n \geq 1$ such that $(n,p)=1$, each factor being a copy of $\mathbb{Z}_p^f$. Observe that the product $g(\alpha) = \prod g_n(\alpha_n)$ converges because $g_n(\alpha_n) \in U^{(n)}$. Let $m = np^s$, with $(n,p)=1$, be any natural number. As $g_n(\mathbb{Z}_p^f) \subseteq g(A)$, it follows from (1) that each coset of $U^{(m)}/U^{(m+1)}$ is represented by an element of $g(A)$. This means that $g(A)$ is dense in $U^{(1)}$. Since A is compact and g is continuous, g is actually surjective.

On the other hand, let $\alpha = (\dots, \alpha_n, \dots) \in A$, $\alpha \neq 0$, i.e., $\alpha_n \neq 0$ for some n. Such an α_n is of the form $\alpha_n = p^{s_n}\beta_n$, with $s_n = v_p(\alpha_n) \geq 0$, and $\beta_n \in \mathbb{Z}_p^f \smallsetminus p\mathbb{Z}_p^f$. It now follows from (2) that

$$g_n(\alpha_n) \in U^{(m)}, \quad g_n(\alpha_n) \notin U^{(m+1)} \quad \text{for} \quad m = m(\alpha_n) = np^{s_n}.$$

Since the n are prime to p, all the $m(\alpha_n)$ have to be distinct, for all $\alpha_n \neq 0$. Let n be the natural number, prime to p and such that $\alpha_n \neq 0$, which satisfies $m(\alpha_n) < m(\alpha_{n'})$, for all $n' \neq n$ such that $\alpha_{n'} \neq 0$. Then one has, for all $n' \neq n$, that

$$g_{n'}(\alpha_{n'}) \in U^{(m+1)} \quad \text{where} \quad m = m(\alpha_n) < m(\alpha_{n'}).$$

Consequently

$$g(\alpha) \equiv g_n(\alpha_n) \not\equiv 1 \bmod U^{(m+1)},$$

and so g(�) #-I. This �how� the injectivity of g. Since $A=$ Z;;, this proves the claim (ii). D

(5.8) Corollary. *If the natural number n* is *not divisible by the characteristic* of *K. then* one *finds the following* indices *for the subgroup.�* of *n-th* power.� *K*" and un in the multiplicative group K* and in the* unit *group U:*

$$(K^*: K^{*11}) = n(U: U^{11}) = \frac{!!\quad \#;111(K).}{|n|,}$$

Proof: The first equality is a consequence of $K^* =$ (rr) x U. By (5.7), we have

$$U \;;;:: fl(K) \times Z1,, \quad \text{resp.} \quad U \text{ �} 11(K) \times Z\text{�},$$

when char $(K) = 0$, resp. $p > 0$. From the exact sequence

$$I\text{------}+ 11_{11}(K)\text{-+} \quad \mu(K) \text{ �} \quad \mu(K)\text{------}+ \mu(K)/\mu(K)'1\text{------}+ I,$$

one has $\#\mu_{11}(K) = \#\mu(K)/\mu(K)^{11}$. When char(K) $= 0$, this gives:

$$(U: 1/^{11}) = \#ft,,(K)\#(Z,,/nZp/ = \#11,1(K)pd,\cdot,,(u) = \#\mu n(K)/|n|p,$$

and when char(K) =pone gets simply (U : $1/^{11}) = \#\mu_{11}(K) = \#\mu_{11}(K)/|n|p$ becau'>c $(n.\ p) = 1$, i.e., $nZp = Z,,.$ n

Exercise **1.** The logarithm function can he continued to a continuou� homomorphi�m log : ij;, --+ � and the exponential f��c11on to a cuntmuous ho.momorphism exp: p-.------;; → Q\,, where p-.------;; = E Qr I $vp(A) >$ 2-r} and *vi'* \ the umque extenq1on of the normalized valuation on Qr.

Exercise 2, Let *K* IQ,, be a p-adJC number field. For I+ ,1 E U\i1 and : E 2₁, one ha�

$$(I + xf \quad =$$

The .\erie\ converges even for ,1 EK �uch that vp(x) > �

Exercise 3. Under the ahove hypothe�e� one has

$$(I + x)' = \exp(z\log(l + 1)) \quad \text{and} \quad \log(l +.d = z \log(! + r).$$

Exercise **4.** For a p-adic number field *K,* every �uhgroup ot finite index in K^* is both open and dosed.

Exercise 5. If *K* 1� a p-adJC number field, then the groupq *Ky",* for *n* EN, form a ba�is of neighbourhood� of I in K^*.

Exercise 6. Let *K* be a p-adic number field, v_p the normalized exponential valuation of *dt* the Haar measure on the locally compact additive group *K,* �calcd �o that *d,1* = I. Then one haq Vp(u) = ,/�CJ *dx.* Furthermore.

$$!(fl\text{�}\int_{K'-101} dx$$

i� a Haar mea�ure on the locally compact group K^*

§ 6. Henselian Fields

Mo1-t results on complete valued fields can be derived from Hensel's lemma alone, without the full strength of completene�s. This lemma is valid in a much bigger class of nonarchimedean valued fields than the com_rlete ones. For example, let *(K, v)* be a nonarchimedean valued field and *(K,* f,) its completion. Leto, resp. 3, be the valuation rings of *K,* resp. *K.* We then consider the separable closure *K,,* of *K* in *K,* and the valuation ring *o,,* £ *K1'* with maximal ideal p1.. which is as<,ociated to the restriction of *fj* to *Ki,,*

K£KV£f<, o<;ov<;O.

Then Hensel\ lemma hold5 in the ring ol' as well as in the ring 3 even though *Ki,* will not, as a rule, be complete. When *Kv* is algebraically closed in *R* - hence in particular char(K) = 0 - this it. immediately obvious (otherwise it follows from (6.6) and §6, exerci5e 3 below). Indeed, by (4.3) we have

o/p = o,,/p,, = O;p,

and if a primitive polynomial *f(x)* E Oi-[x] splil1- over *o,.jp,,* into relatively prime factors]I(.:i).h(t), then we have by Hensel's lemma (4.6) a factorization in 3

/(x) � *g(x)h(x)*

such that x = g" modp', *h* = *1i* modp', deg(g) = deg(!{). But thi� factori?ation already takei,, place over *o,,* once the highest coefficient of,-; is chosen to be in *o:,*. because the coefficients off, and therefore also those of *g* and *h* are algebraic over *K.*

The valued field *K,,* is called the **henselization** of the field *K* with re�pect to *v.* It enjoys all the relevant algebraic properties of the completion *R,* but offer<, the advantage of being itself an algebraic extension of *K* which can also be obtained in a purely algebraic manner, without the analytic recourse to the completion (see §9. exercise 4). The consequence is that taking the henselization of an infini1e algebraic extension LI *K* is possible within the category of algebraic exten1-ions. Let us define in general:

(6.1) Definition. *A* **henselian field** i.� a *field with* a *1101wrchimedcan* valua1ion *v* whose *wilu:-1.tion ring o* sati.,lic1, *Hensel's lemma in the* sense of (4.6). *One* also *calls the valuation v or the wllu,1tion ring o henselian.*

(6.2) Theorem. Let K *be a henselian field with respect to the valuation* $|\ |$. *Then* $|\ |$ *admits one and only one extension to any given algebraic extension* $L|K$. *It is given by*

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|},$$

if $L|K$ *has finite degree* n. *In any case, the valuation ring of the extended valuation is the integral closure of the valuation ring of* K *in* L.

The proof of this theorem is *verbatim* the same as in the case of a complete field (see (4.8)). What is remarkable about our current setting is that, conversely, the unique extendability also characterizes henselian fields. In order to prove this, we appeal to a method which allows us to express the valuations of the roots of a polynomial in terms of the valuations of the coefficients. It relies on the notion of **Newton polygon,** which arises as follows.

Let v be an arbitrary exponential valuation of the field K and let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$$

be a polynomial satisfying $a_0a_n \neq 0$. To each term a_ix^i we associate a point $(i, v(a_i)) \in \mathbb{R}^2$, ignoring however the point (i, ∞) if $a_i = 0$. We now take the lower convex envelope of the set of points

$$\{(0, v(a_0)), (1, v(a_1)), \ldots, (n, v(a_n))\}.$$

This produces a polygonal chain which is called the **Newton polygon** of $f(x)$.

(.1.1·(0,J)

The polygon consists of a sequence of line segments $S_1, S_2, \ldots$ whose slopes are strictly increasing, and which are subject to the following

(6.3) Proposition. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_0a_n \neq 0$, be a polynomial over the field K, v an exponential valuation of K, and w an extension to the splitting field L of f.

If $(r, v(a_r)) \leftrightarrow (s, v(a_s))$ is a line segment of slope $-m$ occurring in the Newton polygon of f, then $f(x)$ has precisely $s - r$ roots $\alpha_1, \dots, \alpha_{s-r}$ of value

$$w(\alpha_1) = \cdots = w(\alpha_{s-r}) = m.$$

Proof: Dividing by a_n only shifts the polygon up or down. Thus we may assume that $a_n = 1$. We number the roots $\alpha_1, \dots, \alpha_n \in L$ of f in such a way that

$$\begin{aligned} w(\alpha_1) &= \cdots = w(\alpha_{s_1}) = m_1, \\ w(\alpha_{s_1+1}) &= \cdots = w(\alpha_{s_2}) = m_2, \\ &\ \ \vdots \\ w(\alpha_{s_t+1}) &= \cdots = w(\alpha_n) = m_{t+1}, \end{aligned}$$

where $m_1 < m_2 < \cdots < m_{t+1}$. Viewing the coefficients a_i as elementary symmetric functions of the roots α_i, we immediately find

$$\begin{aligned} v(a_n) &= v(1) = 0, \\ v(a_{n-1}) &\geq \min_i \{w(\alpha_i)\} = m_1, \\ v(a_{n-2}) &\geq \min_{i<j} \{w(\alpha_i\alpha_j)\} = 2m_1, \\ &\ \ \vdots \\ v(a_{n-s_1}) &= \min_{i_1<\cdots<i_{s_1}} \{w(\alpha_{i_1}\dots\alpha_{i_{s_1}})\} = s_1m_1, \end{aligned}$$

the latter because the value of the term $\alpha_1 \dots \alpha_{s_1}$ is smaller than that of all the others,

$$\begin{aligned} v(a_{n-s_1-1}) &\geq \min_{i_1<\cdots<i_{s_1+1}} \{w(\alpha_{i_1}\dots\alpha_{i_{s_1+1}})\} = s_1m_1 + m_2, \\ v(a_{n-s_1-2}) &\geq \min_{i_1<\cdots<i_{s_1+2}} \{w(\alpha_{i_1}\dots\alpha_{i_{s_1+2}})\} = s_1m_1 + 2m_2, \\ &\ \ \vdots \\ v(a_{n-s_2}) &= \min_{i_1<\cdots<i_{s_2}} \{w(\alpha_{i_1}\dots\alpha_{i_{s_2}})\} = s_1m_1 + (s_2 - s_1)m_2, \end{aligned}$$

and so on. From this result one concludes that the vertices of the Newton polygon, from right to left, are given by

$$(n, 0), \quad (n - s_1, s_1m_1), \quad (n - s_2, s_1m_1 + (s_2 - s_1)m_2),$$

The slope of the extreme right-hand line segment is

$$\frac{0 - s_1 m_1}{n - (n - s_1)} = -m_1 ,$$

and, proceeding further to the left,

$$\frac{(s_1m_1 + \cdots + (s_t - s_{t-1})m_t) - (s_1m_1 + \cdots + (s_{t+1} - s_t)m_{t+1})}{(n - s_t) - (n - s_{t+1})} = -m_{t+1} .$$

□

We emphasize that, according to the preceding proposition, the Newton polygon consists of precisely one segment if and only if the roots $\alpha_1, \dots, \alpha_n$ of f all have the same value. In general, $f(x)$ factors into a product according to the slopes $-m_r < \cdots < -m_1$,

$$f(x) = a_n \prod_{j=1}^{r} f_j(x),$$

where

$$f_j(x) = \prod_{w(\alpha_i)=m_j} (x - \alpha_i).$$

Here the factor f_j corresponds to the $(r - j + 1)$-th segment of the Newton polygon, whose slope equals minus the value of the roots of f_j.

(6.4) Proposition. *If the valuation v admits a unique extension w to the splitting field L of f, then the factorization*

$$f(x) = a_n \prod_{j=1}^{r} f_j(x)$$

is defined already over K, i.e., $f_j(x) = \prod_{w(\alpha_i)=m_j} (x - \alpha_i) \in K[x]$.

Proof: We may clearly assume that $a_n = 1$. The statement is obvious when $f(x)$ is irreducible because then one has $\alpha_i = \sigma_i\alpha_1$ for some $\sigma_i \in G(L|K)$, and since, for any extension w of v, $w \circ \sigma_i$ is another one, the uniqueness implies that $w(\alpha_i) = w(\sigma_i\alpha_1) = m_1$, hence $f_1(x) = f(x)$.

The general case follows by induction on n. For $n = 1$ there is nothing to show. Let $p(x)$ be the minimal polynomial of α_1 and $g(x) =$ … $K[x]$. Since all roots of … have the same value m_1, $p(x)$ … a … of $f_1(x)$. Let $g_1(x) =$ … The factorization of $g(x)$ according to the slopes is

$$g(x) = g_1(x) \prod_{j=2}^{r} f_j(x).$$

Since $\deg(g) < \deg(f)$, it follows that $f_j(x) \in K[x]$ for all $j = 1, \dots, r$. □

If the polynomial f is irreducible, then, hy the above factori.wtion result, there is only *one* slope, i.e., the Newton polygon consists of a single segment. The values of all coefficients lie on or above this line segment and we get the

(6.S) **Corollary.** *Let* $j(x) = a_0+a_1x+\cdot \cdot +ant.ti$ E $K[x)$ be,m *irreducible polynomial with an* i- 0. *Then,* if | | i.� *a nonan:himedean valu:ition* of K *with a unique extension* to *the splilling* field, one has

111 � **max{** |a.,|, |a,|},

In (4.7) we deduced thi<s rc�ult for complete fields from Hensel's lemma and thus obtained the uniqueness of the extended valuation. Here we oblain it, by contrast, as a consequence of the uniqueness of the extended valuation. We now proceed to deduce Heme!'� lemma from the unique extendability.

(6.6) Theorem. *A nonarchimedean valued field (K,* | I) is *hensc/ian* if *and only* if *the valuation* | | can *be uniquely extended to any illgebr.iic extension.*

Proof: The fact that a henselian valuation | | extend& uniquely wa� dealt with in (6.2). Let us assume conversely that || admih one and only one extension to any given algebraic extension. We first show:

Let $f(x) = a_0 +a_1t +$ $+anrn$ E v[x] be a primitive, irreducible polynomial such that a_0an i- 0, and let $J(x) = f(x)$ mod p E K[x]. Then we have deg(!) = 0 or deg(J) = deg(f), and we find

$$J(x) =Gip(x)''',$$

for�ome irreducible polynomial $ip(x)$ E K[..t] and a comtant a.

As f i� irreducible, the Newton polygon is a ,_jngle line segment and thu& lfl = max{luol, lanl\. We may assume that *an* is a unit, becau�e othemi"e the Newton polygon is a �egment which does not lie on the x-axi& and this means that $.f(,) = Go$.

Let L IK be the splitting field of f(x) over K and O the valuation ring of the unique extension I I to L, with maximal ideal �- For an arbitrary K-automorphism a E G = G(LIK), we have lrral = lal for all a EL, because I | and the composite | | o a extend the same valuation. This shows that $aO = 0$, a�=�- If a is a zero off(;,.) and *11.* ih multiplicity. then aa E O for all a E C. Indeed, if $a'¢$ ('J, then n()" laal1, =In()" aal^{1}, > I would imply that the constant coefficient a_0 could not belong to o. Thu& every a E G induces a K-automorphi&m a of 0/\l]. and the ;,eroc:-. *i.'fa* = *rici* of $f(x)$ are all conjugate over K. It follows that $.f(x) =$ if 'rp(x) is the minimal polynomial of ii over K. Since $a,$, E we furthermore that deg(]) � deg(f).

Let now $f(x)$ E olx] be an arbitrary primitive polynomial, and let

$$f(x) \text{ � } .f,(x) \quad \bullet \text{ /; } (x)$$

be it5 factorization into irreduciblcs over K. Since I = lfl = **n** lJ;l, multiplying the $/_1$ by suitable constants yields If; l = 1. The $J;(x)$ are therefore primitive, irreducible polynomials in $o[x]$. It follows that

$$]tx) \text{ � } 1,(x) \cdots 1,(x),$$

where deg(_f,) = 0 or deg({1}) = deg(/;), and $.1_1$ is, up lo a constant factor. the power of an irreducible polynomial. If $T = g\,h$ is a factorization into relatively prime polynomiab "ji,h E $K[x]$, then we must have

$$g \text{ � } a \prod_{iEcl} [1\ ],\ .\quad h \text{ � } h \prod_{/E./} [1\ 1_1$$

where tl,h EK and {I, ... $r\backslash = I$ U J and deg(J,) = deg(J;) for i E /. We now put

$$g \text{ � } a \prod_{rEI} [1\_/;.\quad h \text{ � } h \prod_{JEcJ} f1fi-$$

for a. h E such that $a=$ $(I,\ h = h$ mod p and $.f = gh$. [J

We have introduced henselian flelds by a condition of which the reader will find weaker versions in the literature, restricted to *monic polvnomials* only. Both are equivalent as is shown by the following

(6.7) Proposition. *A nonarchimedean* field $(K.$ v) is hensc/ian if *any manic polynomial* /"(x) E *o[x] which split.�* over *the* residue cfa.�.� *field* K = o/p *as*

$$fCt) = j(:i)li(x) \text{ mod } p$$

with relatively prime manic factors"$ji(\_\backslash)$, $Ti(x)$ E Klx], *admits itself* a .�*plitling*

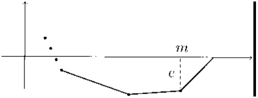
$$f(x) \text{ � } g(x)h(x)$$

into manic factors g(x),h(x) E o[xJ *8uch 1hat*

$$g(,t) = j(x) \bmod p \quad and \quad h(x) = Ti(x) \bmod p.$$

Proof *(H. NART):* We have just seen that the property of K to be henselian follows from the condition that the Newton polygon of every irreducible polynomial $f(x) = a_0 + a_1 \backslash'' + \quad + a_{11}x^{11}$ E $K[x]$ is a 5ingle line segment. It i5 therefore sufficient to �how this. We may assume that $an = $ I. Let $LI K$ he the &plitting field *off.* Then there is always an extension w of v to $L.$ It is obtained for example by taking the completion R of $K,$ extending the valuation of R in a unique way to a valuation V of the algebraic closure K of $R,$ embedding L into $K,$ and restricting V to L It is also pm,sible to get the extension w directly, without passing through the completion. For this we refer to [93], chap. XII, §4, th. I.

Assume now that the Newton polygon of f consist:- of more than one segment:



Let the last segment be given by the points (m, e) and $(n, 0)$. If $e = 0$, we immediately have a contradiction. Becau5c then we have $v(a,) :=: 0$, so that E Cl[x], and $a_0 = \quad = am\text{-}I = 0$ mod p, am "I- 0 mod p. Therefore $= (Xo\text{-}m + \bullet\bullet\bullet + an,)X'''$ mod p, with $m > 0$ because there i� more than one segment. In view of the condition of the proposition this contradict� the irreducibility of *f.*

We will now reduce to $e = 0$ by a tran�formation. Let a E L be a root of $f(x)$ of minimum value $w(a)$ and let a E K such that $v(a) = e.$ We consider the charncteristic polynomial $i(x)$ of $o\text{-}^1cl$ EK $(a), r = n - m.$ If $= n'.^1_{=l}(x - a;),$ then $M(X) = n:^1_{=]}(x - a;''a^{-1})$, Propo�ition (6.3) that the Newlon polygon of i(x) also has more than one segment the last one of slope

$$-w(a\ ^1a') = v(a) - rw(a) = e - rf \ = 0.$$

Since $i(x)$ i5 a power of the minimal polynomial of $a\text{-}^1a'$, hence of an irreducible polynomial, this produces the same contradiction as before. D

Let K be a field which is hemelian with respect to the exponential valuation $v.$ If $LI K$ is a finite extension of degree $n,$ then 1• extends uniquely to an exponential valuation w of $L,$ namely

$$w(a) = lv(NL_1K(a))$$

This follows from (6.2) by taking the logarithm. For the value groups and residue class fields of v and w, one gets the inclusions

$$v(K^*) \subseteq w(L^*) \quad \text{and} \quad \kappa \subseteq \lambda.$$

The index

$$e = e(w\,|\,v) = (w(L^*) : v(K^*))$$

is called the **ramification index** of the extension $L|K$ and the degree

$$f = f(w\,|\,v) = [\lambda : \kappa]$$

is called the **inertia degree.** If v, and hence $w = \frac{1}{n} v \circ N_{L|K}$, is discrete and if $\mathfrak{o}$, $\mathfrak{p}$, π, resp. $\mathcal{O}$, $\mathfrak{P}$, Π, are the valuation ring, the maximal ideal and a prime element of K, resp. L, then one has

$$e = (w(\Pi)\mathbb{Z} : v(\pi)\mathbb{Z}),$$

so that $v(\pi) = e\,w(\Pi)$, and we find

$$\pi = \varepsilon \Pi^e,$$

for some unit $\varepsilon \in \mathcal{O}^*$. From this one deduces the familiar (see chap. I) interpretation of the ramification index: $\mathfrak{p}\mathcal{O} = \pi\mathcal{O} = \Pi^e\mathcal{O} = \mathfrak{P}^e$, or

(6.8) Proposition. *One has* $[L : K] \geq ef$ and *the* **fundamental identity**

$$[L : K] = ef,$$

if v is *discrete* and $L|K$ is *separable.*

Proof: Let $\omega_1, \dots, \omega_f$ be representatives of a basis of $\lambda|\kappa$ and let $\pi_0, \dots, \pi_{e-1} \in L^*$ be elements the values of which represent the various cosets in $w(L^*)/v(K^*)$ (the finiteness of e will be a consequence of what follows). If v is discrete, we may choose for instance $\pi_i = \Pi^i$. We show that the elements

$$\omega_j \pi_i, \quad j = 1, \dots, f, \quad i = 0, \dots, e-1,$$

are linearly independent over K, and in the discrete case form even a basis of $L|K$. Let

$$\sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{ij}\omega_j \pi_i = 0$$

with $a_{ij} \in K$. Assume that not all $a_{ij} = 0$. Then there exist nonzero sums $S_i = \sum_j a_{ij}\omega_j$, and each time that $S_i \neq 0$ we find $w(S_i) \in v(K^*)$. In fact, dividing s, by the coefficient a,� of minimum value, we get a linear combination of the w1, ... , *c.vr* with coefficients in the valuation ring o _c; K one of which equab I. This linear combination is¢ 0 mod 1}, hence a unit, so that w(s1) = E $v(K^*)$.

In the sum $\sum_{i=0}^{e-1} s_i\pi_i$, two nonzero summands must have the same value, say $w(s_i\pi_i) = w(s_j\pi_j)$, i -/=- because otherwi:;.c it could not be zero (observe that $w(x) \neq w(y)$ =} = min{u•(x). w(y))). It follows that

$$u\bullet(rr,) = U'(n_1) + w(sj) � w(s;) == w(nJ) \bmod v(K^*).$$

a contradiction. This shows the linear independence of the *(JJJJf*,. In particular, wehaveef-::::[L:KJ.

Assume now that v, and thus also w, b discrete and let n be a prime element in the valuation ring O of w. We consider the o-module

$$M = \sum_{1=0;=1}^{e-1\ J} Low_1 rr,$$

where $77_1 = TT'$ and show that $M = 0$, i.e., {w $_1$n$_1$) i1- even an integral basis of O over o. We put

$$N = \sum_{/=1}^{j} Low,,$$

sothat $M = N + nN + \cdots + n''^{-1} N$. We find that

$$\mathcal{O} = N + \Pi\mathcal{O},$$

because. for a E 0, we have $a == a_1w_1 + \bullet\bullet + a1wr$ mod nO, a_1 E o. This implies

$$0= N + n(N + TTO) = - =N + TTN + \cdots + TT''^{-1}N + nec:J,$$

so that $O = M + 13e = M +$ pO. Since LIK is separable, 0 is a finitely generated o-modulc (1-ee chap. L (2.11)). and we conclude $O = M$ from Nakayama\ lemma (chap. I, S 11, exercise 7). □

Remark: We had already proved the idemity f $L : K$ J $= cf$ in a somewhat different way in chap. I, (8.2), also in the case where ı• wa1- discrete and LIK separable. Both hypotheses are actually needed. But, strangely enough, the separability condition can be dropped once K is complete with respect to the discrete valuation. In this case, one deduces the equality $O = M$ in the above proof from $O = M +$ pO, not by means of Nakayama's lemma, but rather like this: asp' M S; M, we get successively

$$O � M + p(M+pO) � M + p'O � \quad � M + p''O$$

forall v 2: 1, and since {pvO}�EN is a basis of neighbourhoods of *Lero* in CJ, Mis dense in 0. Since o i� closed in K, (4.9) implies that Mis closed m 0, so that $M = 0$.

Exercise l. In a hcn�elian field the zeroes ot a polynomial are continuou� functions of its cocffo.:1ents. More preci�cly, one ha">: let f(x) E: $K\x]$ be a monic polynomial of degree n <-ind

$$f(x) = \text{IbI(A -air}$$

ild\ecompO\ition into linear factor�, with ::-_ I, $a,\#- a_1$ for 1 #- . If the monic polynomial J;(t) of degree 11 has all sufficiently dose to hose of $f(x)$, then it has r roots $fi_1, ..$ /J, which approximate the $a_1, \ldots, \alpha_r$ to any previously given prec1s1on.

Exercise 2 (Krasner's l,emma). Let a E K be \eparahlc over K and let a = $a_1, ..., a''$ be it� conJugate� over K. If fl E K i� �uch that

$$|a-/J| < |a-a,| \quad \text{for } i = 2 \ldots ,n,$$

then one ha\ $K(a)$ � K(/J).

Exercise 3. A field which 1� 1ensellan ' with re�pect lo two inc4uivalcnt valuations i� scp<1rably clo�ed (Theorem of F.K. SCHMIDT).

Exercise 4. A �eparably closed lield K J\ hen�clian v.ith re�pect to any nonarchimedean valuation.

More generally, valu<1t1on of K admit� a unique cxten�mn to any purely in�cparable extension

Hint: If $a^{1'} = a$ EK, one is forced lo put w(a) = $fiv(a)$.

Exercise 5. Lc1 K a nonan.:himedean valued field, o the valuation ring, and K is hensehan if and only if every polynomial $= x'' + \cdots + a_0$ E ci[x l such that a_0 E p and a_1 *1.* p ha\ a *Lero u* E p.

Hint: The Newton polygon.

Remark: A local rmg o with maximal ideal pis called *hemelian* if Hen\el's lemma in the sense of (6.7) hold� for it. A characterization of these rmg\ which i.\ important in algebraic geometry i"' the tollowing:

A local ring tl i� hensclian 1f and only if every finite commutative o-algcbra A spliN into a direct product $A = n'._1 A$, of local rings J\I•

The proof i� not straightforv.ard, we refer to [ltn], chap. I, �4, th. 4.2.

§ 7. Unramified and Tamely Ramified Extensions

In this section we fix a base field K which is hcn'ielian with respect to a nonarchimedcan valuation v or I 1- As before, we denote the valuation ring, the maximal ideal and the residue class field by o. p, κ, re:c.pectively. if LI K is an algebraic extcn�ion, then the corresponding invariants are labelled $w, 0,$ q:3, A, respectively. An especially important r6lc among these extensions is played by the unramificd extensions, which are defined as follows.

(7.1) Definition. *A finite extension $L|K$ is called* unramified *if the extension $\lambda|\kappa$ of the residue class field is separable and one has*

$$[L:K] = [\lambda:\kappa].$$

An arbitrary algebraic extension $L|K$ is called unramified if it is a union of finite unramified subextensions.

Remark: This definition does not require K to be henselian; it applies in all cases, where v extends uniquely to L.

(7.2) Proposition. *Let $L|K$ and $K'|K$ be two extensions inside an algebraic closure $\bar{K}|K$ and let $L' = LK'$. Then one has*

$$L|K \ \textit{unramified} \implies L'|K' \ \textit{unramified}.$$

Each subextension of an unramified extension is unramified.

Proof: The notations $\mathfrak{o}, \mathfrak{p}, \kappa$; $\mathfrak{o}', \mathfrak{p}', \kappa'$; $\mathcal{O}, \mathfrak{P}, \lambda$; $\mathcal{O}', \mathfrak{P}', \lambda'$ are self-explanatory. We may assume that $L|K$ is finite. Then $\lambda|\kappa$ is also finite and, being separable, is therefore generated by a primitive element $\bar{\alpha}$, $\lambda = \kappa(\bar{\alpha})$. Let $\alpha \in \mathcal{O}$ be a lifting, $f(x) \in \mathfrak{o}[x]$ the minimal polynomial of α and $\bar{f}(x) = f(x) \bmod \mathfrak{p} \in \kappa[x]$. Since

$$[\lambda:\kappa] \le \deg(\bar{f}) = \deg(f) = [K(\alpha):K] \le [L:K] = [\lambda:\kappa],$$

one has $L = K(\alpha)$ and $\bar{f}(x)$ is the minimal polynomial of $\bar{\alpha}$ over κ.

We thus have $L' = K'(\alpha)$. In order to prove that $L'|K'$ is unramified, let $g(x) \in$ be the minimal polynomial of α over K' and $\bar{g}(x) = g(x) \bmod \mathfrak{p}' \in$ Being a factor of $\bar{f}(x)$, $\bar{g}(x)$ is separable and hence irreducible , because otherwise $g(x)$ is reducible by Hensel's lemma. We obtain

$$[\lambda':\kappa'] \le [L':K'] = \deg(g) = \deg(\bar{g}) = [\kappa'(\bar{\alpha}):\kappa'] \le [\lambda':\kappa'].$$

This implies $[L':K'] = [\lambda':\kappa']$, i.e., $L'|K'$ is unramified.

If $L|K$ is a subextension of the unramified extension $L'|K$, then it follows from what we have just proved that $L'|L$ is unramified. Hence so is $L|K$, by the formula for the degree. □

(7.3) Corollary. *The composite of two unramified extensions of K is again unramified.*

Proof': It suffices to show this for two finite extensions *L[K* and *L'IK, LIK* is unramified, hence soi" *LL'IL'*, by (7.2). This implie� that *LL'IK* i'> unramified as well becau:-e separability is tran:-itive and the degree:- of field (and residue field) extensions are multiplicative. LJ

(7.4) Definition. *Let L* IK *he an algebraic* extension. *Then the* composite TI *K* of *all unramilicd* rnbextensions *is called the* **maximal unramitied subextension** of Ll *K.*

(7.5) Proposition. *The residue class* field of *T is the* sep,irab/e *c/w,urc* A, of *K in the residue clm,s field* extemion AIK of *LIK, whereas the* value *group* of *T* equal.'> *thal of K.*

Proof: Let).,$_0$ be the residue class field of *T* and assume *ii* E A i:-separahle over *K.* We have to show that *ii* E Ao. Let *f(x)* E *K\xj* he the minimal polynomial of *ii* and *.f(x)* E o[xj a monic polynomial such that *J* = *f* mod).J. Then f(r) is irreducible and hy Hcnse\'s lemma has a root *a* in *L* wch that *ci* = *a* mod q}, i.e., LK (a) : K] = *[K(ci) : K* J. This implies that *K(a)IK* is unramified, so that *K(a)* S; *T,* and thu:-. *ii* E J...$_0$.

In order to prove *w(T*)* = *v(K*)* we may suppo:-e *LIK* to be finite. The claim then follows from

[Tc *Kl* 2' (w(T') c v(K'))J1'o c K] � (w(T') c *v(K'))IT* c KJ. □

The composite of all unramified extensions inside the algebraic closure *K* of *K* is simply called the maximal unramified extension *K* $_{ni}$ IK of *K* *(nr* = 'non ramifiee'). lt5 residue class field is the separable closure K,.!1c *K* $_{nr}$ contains all roob of unity of order *m* not divisible by the characteristic of *K* because the 5eparable polynomial *x"'* - I splits over *K.,* and hence also over $K_{111,}$ by Hensel's lemma. If *K* is a finite field, then the extension *Km* IK is even generated by these roots of unity because they generate *K,* IK.

If the ch;uacterl5tic *p* = char(K) of the residue class field is po�itive. then one ha5 the following weaker notion accompanying that of an unramified extension.

(7.6) Definition. *An algebraic extension LIK i.� called* **tamely ramified** if *the extern.ion* AIK of *the residue* clas., *fields i.'> separable and one has (lL : T].* p) = I. *In the infinite ca.�e thi� latter condition* is *taken to mean that the* degree of *each finite subextension* of *LIT* is *prime* lop.

As before, in this definition K need not be henselian. We apply it whenever the valuation v of K has a unique extension to L. When the fundamental identity $ef = [L:K]$ holds and $\lambda|\kappa$ is separable, to say that the extension is unramified, resp. tamely ramified, simply amounts to saying that $e = 1$, resp. $(e,p) = 1$.

(7.7) **Proposition.** *A finite extension $L|K$ is tamely ramified if and only if the extension $L|T$ is generated by radicals*

$$L = T(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r})$$

such that $(m_i, p) = 1$. In this case the fundamental identity always holds:

$$[L:K] = ef.$$

Proof: We may assume that $K = T$ because $L|K$ is obviously tamely ramified if and only if $L|T$ is tamely ramified, and if this is the case, then $[L:K] = [L:T][T:K] = [L:T]f$. Let $L|K$ be tamely ramified, so that $\kappa = \lambda$ and $([L:K], p) = 1$. We first show that $e = 1$ implies $L = K$. Let $\alpha \in L \setminus K$. Writing $\alpha = \alpha_1, \dots, \alpha_m$ for the conjugates and $a = Tr(\alpha) = \sum_{i=1}^m \alpha_i$, the element $\beta = \alpha - \frac{1}{m}a \in L \setminus K$ has trace $Tr(\beta) = \sum_{i=1}^m \beta_i = 0$. Since $v(K^*) = w(L^*)$ we may choose $b \in K^*$ such that $v(b) = w(\beta)$ and obtain a unit $\varepsilon = \beta/b \in L \setminus K$ with trace $\sum_{i=1}^m \varepsilon_i = 0$. But the conjugates ε_i have the same residue classes $\bar{\varepsilon}$, mod λ, because $\lambda = \kappa$. Hence $0 = \sum_{i=1}^m \bar{\varepsilon}_i = m\bar{\varepsilon}$, and thus $m \equiv 0 \bmod p$, which contradicts $p \nmid [L:K]$ and $m \mid [L:K]$.

Now let $\omega_1, \dots, \omega_r \in w(L^*)$ be a system of representatives for the quotient $w(L^*)/v(K^*)$ and m_i the order of $\omega_i \bmod v(K^*)$. Since $w(L^*) = \frac{1}{n}v(N_{L|K}(L^*)) \subseteq \frac{1}{n}v(K^*)$, where $n = [L:K]$, we have $m_i | n$, so that $(m_i, p) = 1$. Let $\gamma_i \in L^*$ be an element such that $w(\gamma_i) = \omega_i$. Then $v(\gamma_i^{m_i}) = v(c_i)$, with $c_i \in K$, so that $\gamma_i^{m_i} = c_i\varepsilon_i$ for some unit ε_i in L. As $\lambda = \kappa$ we may write $\varepsilon_i = b_i u_i$, where $b_i \in K$ and u_i is a unit in L which tends to 1 in λ. By Hensel's lemma the equation $x^{m_i} - u_i = 0$ has a solution $\beta_i \in L$. Putting $\alpha_i = \gamma_i\beta_i^{-1} \in L$, we find $w(\alpha_i) = \omega_i$ and

$$\alpha_i^{m_i} = a_i, \quad i = 1, \dots, r,$$

where $a_i = c_i b_i \in K$, i.e., we have $K(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r}) \subseteq L$. By construction, both fields have the same value group and the same residue class field. So, by what we proved first, we have

$$L = K(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r}).$$

The inequality $[L:K] \geq e$ and thus, in view of (6.8), the equality $[L:K] = e$, now follows by induction on r. If $L_1 = K(\sqrt[m_1]{a_1})$, then

w_1 E $w(Lj)$ yields

$$e(L1IK) = (w(L;): v(K^*)) \geq m_1 \geq [L1: Kl.$$

Aboe(/,lli) 2: [L: *Lil,* because *w(L*)/w(Lj)* is generated by the residue dai'>f>e<, of *t1>2, ., Wr.* Thus

$$e \, e(LIL,)c(L,IK) \geq [L, L, III,, Kl [L,K\.$$

In order to prove lhat an extem,ion /, $= K$ ("'.y;Ti, . if> tamely ramified, it <;uftices to look at the caf>e $r = 1$, i.e., $= K(";fa)$, where $(m, p) = 1$. The general case then follows hy induclion. We may assume without loss of generality that *1<* if> separahly dosed. This is seen by passing to the maximal unramified extension $K_1 = K,,,.,$ which haf> the separable closure $1<_1 = K_1$. of *k* as ih residue class held. We obtain the following diagram

$$L -- L,$$

$$K -- K,,$$

where $L \cap K_1 = T = K$ and $L_1 = K_1(\sqrt{G})$. If now $L_1 I K_1$ is tamely ramified, then ,\1 11<1 is separable; hence $A_1 = 1<_1$ and *pf* $[L_1 : Kil = [L:K] =$ jl: *TJ,* i.e., *LIK* i<; also tamely ramified.

Let $a = 7/a$. We may assume that $[L : Kl = [K(\sqrt{G}) : Kl = m$. In fact. if *d* if> the greatest divisor of *m* such that $a = a'^{d}$ for <;ome $a' \in K^*$, and if $m' = m/d$, then $a=$ "'j":;i and $[K(,(/2): K] = m'$. Now let $n =$ ord(w(a) mod $v(K^*))$. Since $mw(ct) = v(a)$ E $v(K^*)$, we have $m = dn$. Consequently $w(a") = 1\cdot$(h), *h* E *K*, and $v(h") = w(ctm) = v(a);$ thus *am*= *a*= Eh^{11} for some unit *f* in *K.* A<; $(d.p) = 1$, the equation $xd - c = 0$ splits over the <;cparably dm,ed residue field *1<* into distinct linear factors, hence also over K by Henf>el '<; lemma. Therefore $am = li = a$ for some new h E K^*. Since $xm - a$ is irreducible, we have $d = 1$, and hence $m = n$. Thus

$$e \geq n = |I, : Kl \geq el \geq e,$$

in other words $j = 1$, and so A= *1<* and *pf* $n = e$. This shows that *LIK* i tamely ramified. D

(7.8) Corollary. *Let LIK* and *K'IK be two* extemiom *imidc the algebraic* closure *i<IK,* and $L' = LK'$. *Then* we have:

f,IK tamely ramified===} L'IK' tamely ramified.

Every suhextew,ion of *a tamely ramified* exten.ion is *tamely* ramified.

Proof: We may assume without loss of generality that $L|K$ is finite and con<;klcr the diagram

$$\begin{array}{ccc} L & - & L' \\ | & & | \\ T & - & T' \\ | & & | \\ K & - & K'. \end{array}$$

The inclusion T S; T' follows from (7.2). If $L|K$ is tamely ramified, then $L =$ .. ,"':,/a:), $(m,,p) =$ I; hence $L' = LK' = LT' =$ $T'('''Fi.$ �o that $L'|K'$ is also tamely ramified. by (7.7).

The claim conccmmg the subextemions follows exactly as in the unramified case. □

(7.9) Corollary. *The* composite of tamely ramified extensions is *tamely* ramified.

Proof: This follows from (7.8), exactly a!, (7.3) followed from (7.2) in the unramified case. n

(7.10) Definition. Lei $L|K$ *be an algebraic extension. Then the composite* $V|K$ *of all tamely ramified subextemions is called the* maximal tamely ramified *1,ubextension* of $L|K$.

Let $w(L^*)^{1}1$\ denote the subgroup of all clements $w \in w(L^*)$ such that $mw \in v(K^*)$ for some m sati!,fying $(m. p) =$ I. The quotient group 11'(/.*)(l'l $/v(K^*)$ then consists of all elements of $w(L^*)/v(K$�$)$ whose order is prime *top.*

(7.11) Proposition. *The maximal tamely* rnmified *subextension* $V|K$ of L IK *h;.is value group* w(\/�) = $w(L^*/$Pl *and* re.\id11e da.�s *field* equal *lO the separable* closure A., *ofK in* AIK.

Proof: We may restrict to the case of a finite extension $L|K$. By passing from K to the maximal unramified subextension. we may assume by (7.5) that A, = k. As *pf* e(\/IK) = we certainly Conversely we find. a!, in proof of (7.7), for $w \in$ a radical α = ?:./a EL such that $a \in K$. $(m,$ p) = I and = w, so that one has $\alpha \in V$, and $w \in w(V^*)$. □

The results obtained in this section may be summarized in the following picture:

$$\begin{array}{ccccccc} K & \subseteq & T & \subseteq & V & \subseteq & L \\ \kappa & \subseteq & \lambda_s & = & \lambda_s & \subseteq & \lambda \\ v(K^*) & = & w(T^*) & \subseteq & w(L^*)^{(p)} & \subset & w(L^*). \end{array}$$

If $L|K$ is finite and $e = e'p^a$ where $(e',p) = 1$, then $[V:T] = e'$. The extension $L|K$ is called **totally** (or **purely**) **ramified** if $T = K$, and **wildly ramified** if it is not tamely ramified, i.e., if $V \neq L$.

Important Example: Consider the extension $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ for a primitive n-th root of unity ζ. In the two cases $(n,p) = 1$ and $n = p^\nu$, this extension behaves completely differently. Let us first look at the case $(n,p) = 1$ and choose as our base field, instead any discretely valued complete field K with finite residue class field $\kappa =$ with $q = p^f$.

(7.12) Proposition. *Let $L = K(\zeta)$, and let $\mathcal{O}|\mathfrak{o}$, resp. $\lambda|\kappa$, be the extension of valuation rings, resp. residue class fields, of $L|K$. Suppose that $(n,p) = 1$. Then one has:*

(i) *The extension $L|K$ is unramified of degree f, where f is the smallest natural number such that $q^f \equiv 1 \bmod n$.*

(ii) *The Galois group $G(L|K)$ is canonically isomorphic to $G(\lambda|\kappa)$ and is generated by the automorphism $\varphi : \zeta \mapsto \zeta^q$.*

(iii) $\mathcal{O} = \mathfrak{o}[\zeta]$.

Proof: (i) If $\phi(X)$ is the minimal polynomial of ζ over K, then the reduction $\bar\phi(X)$ is the minimal polynomial of $\bar\zeta = \zeta \bmod \mathfrak{P}$ over κ. Indeed, being a divisor of $X^n - 1$, $\bar\phi(X)$ is separable and by Hensel's lemma cannot split into factors. ϕ and $\bar\phi$ have the same degree, so that $[L:K] = [K(\zeta):K] = [\kappa(\bar\zeta):\kappa] = [\lambda:\kappa]$. $L|K$ is therefore unramified. The polynomial $X^n - 1$ splits over $\mathcal{O}$ and thus, (because $(n,p) = 1$) over λ into distinct linear factors, so that $\lambda = \mathbb{F}_{q^f}$ contains the group μ_n of n-th roots of unity and is generated by it. Consequently f is the smallest number such that $\mu_n \subseteq \mathbb{F}_{q^f}^*$, i.e., such that $n \mid q^f - 1$. This shows (i). (ii) results trivially from this.

(iii) Since $L|K$ is unramified, we have $p\mathcal{O} = \mathfrak{P}$, and since $1, \zeta, \dots, \zeta^{f-1}$ represent a basis of $\lambda|\kappa$, we have $\mathcal{O} = \mathfrak{o}[\zeta] + \mathfrak{P}\mathcal{O}$, and $\mathcal{O} = \mathfrak{o}[\zeta]$ by Nakayama's lemma. □

(7.13) Proposition. *Let ζ be a primitive p^m-th root of unity. Then one has:*

(i) *$\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ is totally ramified of degree $\varphi(p^m) = (p-1)p^{m-1}$.*

(ii) *$G(\mathbb{Q}_p(\zeta)|\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^*$.*

(iii) *$\mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\zeta)$.*

(iv) *$1-\zeta$ is a prime element of $\mathbb{Z}_p[\zeta]$ with norm p.*

Proof: $\xi = \zeta^{p^{m-1}}$ is a primitive p-th root of unity, i.e.,

$$\xi^{p-1} + \xi^{p-2} + \cdots + 1 = 0, \quad \text{hence}$$

$$\zeta^{(p-1)p^{m-1}} + \zeta^{(p-2)p^{m-1}} + \cdots + 1 = 0.$$

Denoting by ϕ the polynomial on the left, $\zeta - 1$ is a root of the equation $\phi(X+1) = 0$. But this is irreducible because it satisfies Eisenstein's criterion: $\phi(1) = p$ and $\phi(X) = (X^{p^m}-1)/(X^{p^{m-1}}-1) \equiv (X-1)^{p^m - p^{m-1}} \bmod p$. It follows that $[\mathbb{Q}_p(\zeta):\mathbb{Q}_p] = \varphi(p^m)$. The canonical injection $G(\mathbb{Q}_p(\zeta)|\mathbb{Q}_p) \to (\mathbb{Z}/p^m\mathbb{Z})^*$, $\sigma \mapsto n(\sigma)$, where $\sigma\zeta = \zeta^{n(\sigma)}$, is therefore bijective, since both groups have order $\varphi(p^m)$. Thus

$$N_{\mathbb{Q}_p(\zeta)|\mathbb{Q}_p}(1-\zeta) = \prod_\sigma (1-\sigma\zeta) = \phi(1) = p.$$

Writing w for the extension of the normalized valuation v_p of $\mathbb{Q}_p$ to $\mathbb{Q}_p(\zeta)$, we find furthermore that $\varphi(p^m)w(1-\zeta) = v_p(p) = 1$, i.e., $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ is totally ramified and $\zeta - 1$ is a prime element of $\mathbb{Q}_p(\zeta)$. As in the proof of (6.8), it follows that $\mathbb{Z}_p[\zeta-1] = \mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\zeta)$. This concludes the proof. □

If ζ_n is a primitive n-th root of unity and $n = n'p^m$, with $(n',p) = 1$, then propositions (7.12) and (7.13) yield the following result for the maximal unramified and the maximal tamely ramified extension:

$$\mathbb{Q}_p \subseteq T = \mathbb{Q}_p(\zeta_{n'}) \subseteq V = T(\zeta_p) \subseteq \mathbb{Q}_p(\zeta_n).$$

Exercise 1. The maximal unramified extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity of order prime to p.

Exercise 2. Let K be henselian and $K_{nr}|K$ the maximal unramified extension. Show that the subextensions of $K_{nr}|K$ correspond 1-1 to the subextensions of the separable closure $\bar\kappa|\kappa$.

Exercise 3. Let $L|K$ be totally and tamely ramified, and let Γ_L, resp. Γ_K, be the value group of L, resp. K. Show that the intermediate fields of $L|K$ correspond 1-1 to the suhgrour� of d / /'

§ 8. Extensions of Valuations

Having seen that the henselian valuations extend uniquely to algebraic extensions we will now study lhe que<;tion of how a valuation 11 of a field K extends to an algebraic extem,ion in general. So let v be an arbitrary archimedean or nonarchimedean valuation. There is a little di�crepancy in notation here, because archimedean valuations manifest themselves only as absolute values while the letter u has hitherto been used for nonarchimedean exponential valuation�. In �pite of this, it will prove advantageous. and agrees with current usage, to employ the letter 1J simultaneou�ly for both types of valuations, to denote the corre<;ponding multiplicative valuation in both case� by I Iv and the completion by K�· Where confusion lurks, we will supply clarifying remarks.

For every valuation v of K we consider the completion K_v and an algebraic clornre K_1, of K,,. The canonical extension of 1• to Kr i<; again denoted by 1· and the unique cxlemion of this latter valualion to K_1, by V.

Let LI K be an algebraic cxten"ion. Choosing a K-embedding

$$\tau : L \longrightarrow \overline{K}_v\,,$$

we obtain by restriction of V to r L an exten�ion

$$w = 1/o\tau$$

of the valuation 1• to L In other words. if v, re�p. V, are given by the absolute values I I,. re�p. I Iv, on K, Kv, resp. K,., where I Iv extends precisely the absolute value I I,, of K_{1},, then we obtain on L the multiplicative valuation

$$|x|_w = |\tau x|_{\bar{v}}\,.$$

The mapping r : L --+ K, is obviously continuous with respect to thi<; valuation. It extends in a unique way to a continuous K-embedding

$$\tau : Lw \dashrightarrow f<,,.$$

where, in the case of an infinite extension LI K, L.,, does not mean the completion of L with respect to w, but the union Lu, = LJ, $L_{11}r$ of the completion<; /.$_{1}$,;, of all finite subexten<;ion<; L,IK of LJK. This union will be henceforth called the **localization** of /. with respect to w. When fl: Kl< co. r is given by the rule

$$x = w\text{-}\lim_{n\to\infty} x_n \quad := \bar{v}\text{-}\lim_{n\to\infty} \tau x_n$$

where is aw-Cauchy sequence in L, and hence {rx,$_1$}nEH a ii-Cauchy �cquence m Note here that the ,;equcnec $T\11$ converges in the finite complete extension rL Kv of K_{1}. We consider the diagram of fields

L-------------- L,.,

|

| K_{v}

K

The canonical exten�ion of the valuation w from L to Lu, j._ precisely the unique extension of the valuation v from K,, to the extension $L_{11},IK"$. We have

$$Lw=LKv,$$

because if LIK is finite, then the field LK,, � L,,. is complete hy (4.8). contains the field Land therefore ha,; to be it� completion. If L,,.$[K_1$, has degree n < oo, then, by (4.8), the ab,;olute values corresponding to v and w satisfy the relation

$$|x|_w = \sqrt[n]{|N_{L_w|K_v}(x)|_v}$$

The !ield diagram(*) is of central importance for algebraic number theory. It show5 the pa,;,,;age from the "global extension" LIK to the "local extension" L_{11}, I K_1, and thm represent� one of the most important method,; of algebraic number theory, the so-called **local-to-global principle.** This tenninology arises from the case of a function lleld K, for example K = :C(!), where the elemenb of the extension L arc algebraic function� on a Riemann surface, hence on a *?,lohal* object, whereas pasf>ing to Kv and L.,, �ignifies looking at power series expansions, i.e., the *local* study of functions. The diagram (*) thus cxprc,;scs in an abstract manner our original goal. to provide methods of function theory for use in the theory of numbers by mean� of valuation�.

We saw that every K-embedding r : L ---+ K_1, gave u� an extcn�ion w =Vo r of v. For every automorphi�m a E $G(i<_1$ IK_1,) of Kv over $K v$, we obtain with the composite

$$L \xrightarrow{\tau} \overline{K}_v \xrightarrow{\sigma} \overline{K}$$

a new K-embedding r' = a or of L. It will be f>aid to be *to T* *m·cr Ku*• The following result gives us a complete description pos�ible exten5ions of v to L.

(8.1) Extension Theorem. Lei LIK be an *algebraic field extension* and v a valuation of K. *Then one has:*

(i) *Every extension* w *of the valuation* v *arises as the composite* $w = \bar{v} \circ \tau$ *for some* K-*embedding* $\tau : L \to \bar{K}_v$.

(ii) *Two extensions* $\bar{v} \circ \tau$ *and* $\bar{v} \circ \tau'$ *are equal if and only if* τ *and* τ' *are conjugate over* K_v.

Proof: (i) Let w be an extension of v to L and L_w the localization of the canonical valuation, which is again denoted by w. This is the unique extension of the valuation v from K_v to L_w. Choosing any K_v-embedding $\tau : L_w \to \bar{K}_v$, the valuation $\bar{v} \circ \tau$ has to coincide with w. The restriction of τ to L is therefore a K-embedding $\tau : L \to \bar{K}_v$ such that $w = \bar{v} \circ \tau$.

(ii) Let τ and $\sigma \circ \tau$, with $\sigma \in G(\bar{K}_v|K_v)$, be two embeddings of L conjugate over K_v. Since $\bar{v}$ is the only extension of the valuation v from K_v to $\bar{K}_v$, one has $\bar{v} = \bar{v} \circ \sigma$, and thus $\bar{v} \circ \tau = \bar{v} \circ (\sigma \circ \tau)$. The extensions induced to L by τ and by $\sigma \circ \tau$ are therefore the same.

Conversely, let $\tau, \tau' : L \to \bar{K}_v$ be two K-embeddings such that $\bar{v} \circ \tau = \bar{v} \circ \tau'$. Let $\sigma : \tau L \to \tau' L$ be the K-isomorphism $\sigma = \tau' \circ \tau^{-1}$. We can extend σ to a K_v-isomorphism

$$\sigma : \tau L \cdot K_v \to \tau' L \cdot K_v .$$

Indeed, τL is dense in $\tau L \cdot K_v$, so every element $x \in \tau L \cdot K_v$ can be written as a limit

$$x = \lim_{n \to \infty} \tau x_n$$

for some sequence x_n which belongs to a finite subextension of L. As $\bar{v} \circ \tau = \bar{v} \circ \tau'$, the sequence $\tau' x_n = \sigma \tau x_n$ converges to an element

$$\sigma x := \lim_{n \to \infty} \sigma \tau x_n$$

in $\tau' L \cdot K_v$. Clearly the correspondence $x \mapsto \sigma x$ does not depend on the choice of a sequence $\{x_n\}$, and yields an isomorphism $\tau L \cdot K_v \to \tau' L \cdot K_v$ which leaves K_v fixed. Extending σ to a K_v-automorphism $\sigma \in G(\bar{K}_v|K_v)$ gives $\tau' = \sigma \circ \tau$, so that τ and τ' are indeed conjugate over K_v. □

Those who prefer to be given an extension $L|K$ by an algebraic equation $f(X) = 0$ will appreciate the following concrete variant of the above extension theorem.

Let $L = K(\alpha)$ be generated by the zero α of an irreducible polynomial $f(X) \in K[X]$ and let

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r}$$

be the decomposition of $f(X)$ into irreducible factors $f_1(X), \dots, f_r(X)$ over the completion K_v. Of course, the m_i are one if f is separable. The K-embeddings $\tau : L \to \bar{K}_v$ are then given by the zeroes β of $f(X)$ which lie in $\bar{K}_v$:

$$\tau : L \longrightarrow \bar{K}_v, \quad \tau(\alpha) = \beta.$$

Two embeddings τ and τ' are conjugate over K_v if and only if the zeroes $\tau(\alpha)$ and $\tau'(\alpha)$ are conjugate over K_v, i.e., if they are zeroes of the same irreducible factor f_i. With (8.1), this gives the

(8.2) **Proposition.** *Suppose the extension $L|K$ is generated by the zero α of the irreducible polynomial $f(X) \in K[X]$.*

Then the valuations $w_1, \dots, w_r$ extending v to L correspond 1-1 to the irreducible factors $f_1, \dots, f_r$ in the decomposition

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r}$$

of f over the completion K_v.

The extended valuation w_i is explicitly obtained from the factor f_i as follows: let $\alpha_i \in \bar{K}_v$ be a zero of f_i, and let

$$\tau_i : L \longrightarrow \bar{K}_v, \quad \alpha \mapsto \alpha_i,$$

be the corresponding K-embedding of L into $\bar{K}_v$. Then one has

$$w_i = \bar{v} \circ \tau_i.$$

τ_i extends to an isomorphism

$$\tau_i : L_{w_i} \longrightarrow K_v(\alpha_i)$$

on the completion L_{w_i} of L with respect to w_i.

Let $L|K$ be again an arbitrary finite extension. We will write $w|v$ to indicate that w is an extension of the valuation v of K to L. The inclusions $L \hookrightarrow L_w$ induce homomorphisms $L \otimes_K K_v \to L_w$, via $a \otimes b \mapsto ab$, and hence a canonical homomorphism

$$\varphi : L \otimes_K K_v \longrightarrow \prod_{w|v} L_w.$$

To begin with, the tensor product is taken in the sense of vector spaces, i.e. the K-vector space L is lifted to a K_v-vectorspace $L \otimes_K K_v$. This latter, however, is in fact a K_v-algebra, with the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$, and φ is a homomorphism of K_v-algebras. This homomorphism is the subject of the

(8.3) Proposition. *If $L|K$ is separable, then* $L \otimes_K K_v \cong \prod_{w|v} L_w$.

Proof: Let α be a primitive element for $L|K$, so that $L = K(\alpha)$, and let $f(x) \in K[x]$ be its minimal polynomial. To every $w|v$, there corresponds an irreducible factor $f_w(x) \in K_v[x]$ of $f(x)$, and in view of the separability, we have $f(x) = \prod_{w|v} f_w(x)$. Consider all the L_w as embedded into an algebraic closure $\bar{K}_v$ of K_v, and denote by α_w the image of α under $L \to L_w$. Then we find $L_w = K_v(\alpha_w)$ and $f_w(x)$ is the minimal polynomial of α_w over K_v. We now get a commutative diagram

$$\begin{tikzcd} K_v[x]/(f) \arrow[r] \arrow[d] & \prod_{w|v} K_v[x]/(f_w) \arrow[d] \\ L \otimes_K K_v \arrow[r] & \prod_{w|v} L_w \end{tikzcd}$$

where the top arrow is an isomorphism by the Chinese remainder theorem. The arrow on the left is induced by $x \mapsto \alpha \otimes 1$ and is an isomorphism because $K[x]/(f) \cong K(\alpha) = L$. The arrow on the right is induced by $x \mapsto \alpha_w$ and is an isomorphism because $K_v[x]/(f_w) \cong K_v(\alpha_w) = L_w$. Hence the bottom arrow is an isomorphism as well. □

(8.4) Corollary. *If $L|K$ is separable, then one has*

$$[L : K] = \sum_{w|v} [L_w : K_v]$$

and

$$N_{L|K}(\alpha) = \prod_{w|v} N_{L_w|K_v}(\alpha), \quad Tr_{L|K}(\alpha) = \sum_{w|v} Tr_{L_w|K_v}(\alpha).$$

Proof: The first equation results from (8.3) since $[L : K] = \dim_K(L) = \dim_{K_v}(L \otimes_K K_v)$. On both sides of the isomorphism

$$L \otimes_K K_v \cong \prod_{w|v} L_w$$

let us consider the endomorphism: multiplication by α. The characteristic polynomial of α on the K_v-vector space $L \otimes_K K_v$ is the same as that on the K-vector space L. Therefore

$$\text{char. polynomial}_{L|K}(\alpha) = \prod_{w|v} \text{char. polynomial}_{L_w|K_v}(\alpha).$$

This implies immediately the identities for the norm and the trace. □

If v is a nonarchimedean valuation, then we define, as in the henselian case, the ramification index of an extension $w|v$ by

$$e_w = (w(L^*) : v(K^*))$$

and the inertia degree by

$$f_w = [\lambda_w : \kappa],$$

where λ_w, resp. κ, is the residue class field of w, resp. v. From (8.4) and (6.8), we obtain the fundamental identity of valuation theory:

(8.5) Proposition. *If v is discrete and $L|K$ separable, then*

$$\sum_{w|v} e_w f_w = [L:K].$$

This proposition repeats what we have already seen in chap. I, (8.2), working with the prime decomposition. If K is the field of fractions of a Dedekind domain $\mathcal{o}$, then to every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{o}$ is associated the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ of K defined by $v_\mathfrak{p}(a) = \nu_\mathfrak{p}$, where $(a) = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$ (see chap. I, § 11, p. 67). The valuation ring is the localization $\mathcal{o}_\mathfrak{p}$. If $\mathcal{O}$ is the integral closure of $\mathcal{o}$ in L and if

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

is the prime decomposition of $\mathfrak{p}$ in L, then the valuations $w_i = \frac{1}{e_i} v_{\mathfrak{P}_i}$, $i = 1, \dots, r$, are precisely the extensions of $v = v_\mathfrak{p}$ to L, e_i are the corresponding ramification indices and $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$ the inertia degrees. The fundamental identity

$$\sum_{i=1}^r e_i f_i = [L:K]$$

has thus been established in two different ways. The *raison d'être* of valuation theory, however, is not to reformulate ideal-theoretic knowledge, but rather, as has been stressed earlier, to provide the possibility of passing from the extension $L|K$ to the various completions $L_w|K_v$ where much simpler arithmetic laws apply. Let us also emphasize once more that completions may always be replaced with henselizations.

Exercise 1. Up to equivalence, the valuations of the field $\mathbb{Q}(\sqrt{5})$ are given as follows.

1) $|a+b\sqrt{5}|_1 = |a+b\sqrt{5}|$ and $|a+b\sqrt{5}|_2 = |a-b\sqrt{5}|$ are the archimedean

2) If $p = 2$ or 5 or a prime number $p \neq 2, 5$ such that $\left(\frac{5}{p}\right) = -1$, then there is exactly one extension of $|\ |_p$ to $\mathbb{Q}(\sqrt{5})$, namely

$$|a+b\sqrt{5}|_{\mathfrak{p}} = |a^2-5b^2|_p^{1/2}.$$

3) If p is a prime number $\neq 2, 5$ such that $\left(\frac{5}{p}\right) = 1$, then there are two extensions of $|\ |_p$ to $\mathbb{Q}(\sqrt{5})$, namely

$$|a+b\sqrt{5}|_{\mathfrak{p}_1} = |a+by|_p, \quad \text{resp.} \quad |a+b\sqrt{5}|_{\mathfrak{p}_2} = |a-by|_p,$$

where y is a solution of $x^2-5=0$ in $\mathbb{Q}_p$.

Exercise 2. Determine the valuations of the field $\mathbb{Q}(i)$ of the Gaussian numbers.

Exercise 3. How many extensions to $\mathbb{Q}(\sqrt[3]{2})$ does the archimedean absolute value $|\ |$ of $\mathbb{Q}$ admit?

Exercise 4. Let $L|K$ be a finite separable extension, $\mathcal{o}$ the valuation ring of a discrete valuation v, $\mathcal{O}$ its integral closure in L. If $w|v$ varies over the extensions of v to L and $\mathcal{o}_v$, $\mathcal{O}_w$ resp. are the valuation rings of the completions K_v, resp. L_w, then one has

$$\mathcal{o}_v \otimes_{\mathcal{o}} \mathcal{O} \cong \prod_{w|v} \mathcal{O}_w.$$

Exercise 5. How does proposition (8.2) relate to Dedekind's proposition, chap. I, (8.3)?

Exercise 6. Let $L|K$ be a finite field extension, v a nonarchimedean exponential valuation, and w an extension to L. If $\mathcal{O}$ is the integral closure of the valuation ring $\mathcal{o}$ of v in L, then the localization $\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}$ at the prime ideal $\mathfrak{p} = \{a \in \mathcal{O} \mid w(a) > 0\}$ is the valuation ring of w.

§ 9. Galois Theory of Valuations

We now consider Galois extensions $L|K$ and study the effect of the Galois action on the extended valuations $w|v$. This leads to a direct generalization of "Hilbert's ramification theory" - see chap. I, §9, where we studied, instead of valuations v, the prime ideals $\mathfrak{p}$ and their decomposition $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ in Galois extensions of algebraic number fields. The arguments stay the same, so we may be rather brief here. However, we formulate and prove all results for extensions that are not necessarily finite, using infinite Galois theory. The reader who happens not to know this theory should feel free to assume all extensions in this section to be finite. On the other hand, we treat infinite Galois theory also in chap. IV, § 1 below. Its main result can be put in a nutshell like this:

In the case of a Galois extension $L|K$ of infinite degree, the main theorem of ordinary Galois theory, concerning the 1-1 correspondence between the intermediate fields of $L|K$ and the subgroup'> of the Galois group $G(L|K)$ ceases to hold; there are more subgroups than intermediate fields. The corre�pondence can be salvaged, however, by considering a canonical topology on the group $G(L|K)$, the **Krull topology.** It is given by defining, for every $a \in G(L|K)$, as a basis of neighbourhoods the cosets $aG(L|M)$, where $M|K$ varies over the *finite* Galois subextensions of $L|K$. $G(L|K)$ is thus turned into a compact, Hausdorff topological group. The main theorem of Galois theory then has to be modified in the infinite case by the condition that the intermediate fields of $L|K$ corre�pond 1-1 to the *closed* subgroups of $G(l|K)$. Otherwise, everything goes through as in the finite case. So one tacitly restricts attention to *dosed* subgroups, and accordingly to *continuous* homomorphisms of $G(L|K)$.

So let $L|K$ be an arbitrary, finite or infinite, Galois extension with Galois group $G = G(L|K)$. If vis an (archimcdcan or nonarchimcdean) valuation of K and w an extension to L, then, for every $a \in G$, $w \circ a$ also extends v, so that the group G acts on the set of extensions $w|v$.

(9.1) Proposition. *The group G* acts tramitively *on the ·"et* of *extensiom* $w|v$, i.e., every *two extensiom* <JJ"e *conjugate.*

Proof: Let $11'$ and W' he two extensions of v to L. Suppo�e $L|K$ is finite. If w and w' are not conjugate, then the �et�

$$\{w \circ \sigma \mid \sigma \in G\} \quad \text{and} \quad \{w' \circ \sigma \mid \sigma \in G\}$$

would he disjoint. By the approximation theorem (3.4), we would be able to find an _t E L such that

$$|ax|_{11,} < I \quad \text{and} \quad |crtl|_{11,i} > 1$$

for all $a \in G$. Then one would have for the nonn $a = Nr1K(x) = \prod_{rr \in G} a\_t$ that $|a|_{1,} = \prod |a|_{\ldots} < I$ and likewise $|a|_{,,} > I$, a contradiction.

If $L|K$ is infinite, then we let $M|K$ vary over all finite Galois subextensions and consider the �et� $X_M = \{\sigma \in G \mid w \circ \sigma|_M = w'|_M\}$. They arc nonempty, as we have juf.t seen, and also closed because, for $a \in G \setminus X_M$, the whole open neighbourhood $aG(L|M)$ lies in the complement of X_M. We have $\bigcap_M X_M \# 0$. because otherwi�e the compactness of G would yield a relation $\bigcap_{i=1}^{n} X_{M_i} = 0$ with finitely many M_i, and this j5 a comradiction bccau<,c if $M = M_1 \cdots M_n$, then $X_M = \bigcap_{i=1}^{n} X_{M_i}$. □

(9.2) **Definition.** *The* **decomposition group** of *an extension w o(v to L* is *defined by*

$$G_w = G_w(L|K) = \{a \in G(L|K) \mid w \circ a = w\}$$

If *v* is a nonarchimedean valuation, then the decomposition group contains two further canonical subgroups

Gw2fw2Ru,,

which are defined as follow<;. Let 0, resp. *0,* be the valuation ring, p, resp. '13, the maximal ideal, and let *κ* = o/p. resp.).= *0/'l],* be the rc<;idue clas1- field of *v,* resp. *w.*

(9.3) **Definition.** *The* **inertia group** *ofwlv is defined by*

fu,=11!,(LIK)={aEGwlax=xmodq] fora/I xEO)

and the **ramification group** *by*

R,,, = Ru,(LIK) = {a E *Gu,* | *f!.f* = l mod *V* for all *x* EL*).

Observe in this definition that, *fora* E *Gu,,* the identity *woo= w* implic<; that one always ha<; *rrO =0* and *ax/x* E ('.J, for all *x EL*.*

The "ubgroups *Gu,,lw,R11,* of *G* = G(LIK), and in fact all canonical subgroups we will encounter in the sequel, are all *closed* in the Krull topology. The proof of thi� ir, routine in all case�. Let us just illu�trate the model of the argument for the example of the decomposition group.

Let *a* E *G* = G(LIK) be an element which belongs to the do�urc of *G0,.* Thi� means that. in every neighbourhood *aG(LIM),* there is some element *aM* of G.,,. Herc *MIK* varies over all finite Galob subcxtcnsions of *LIK.* Since *aM* E aG(LIM), we have *aMIM* = *alM,* and *woaM* = *w* implies that *W* oal111 = *w* oa111IM = *wlM-* A� Lis the union of all the *M,* we get 11[1] o *a* = *w,* so that *a* E *G0·.* This shows that the subgroup *G,,,* is do�cd inG.

The groups *Gw. lw, Ru-* carry very significant information about the behaviour of the valuation *v* of *K* as it is extended to /,. But before going into this, we will treat the functorial propertie� of the groups *G,,,. I,,, R,,.*

Consider two Galois extension� *LIK* and /,'IK' and a commutative diagram

T T

K � *K'*

with homomorphisms r which will typically be inclusions. They induce a homomorphism

$$T^*: \quad G(L'IK') \text{----+} G(LIK), \quad T^*(a') = T^{-1}a'T.$$

Observe here that. LIK being nonnal, the same is true of $TLITK$, and thus one has $a'TL$ £;; TL, 50 that composing with T^{-1} makc5 sense.

Now let w' be a valuation of L', $v' = w'IK'$ and $w = w'$ or, $v = wIK$• Then we have the

(9.4) Proposition. r*: G(L'IK')-+ G(LIK) induces *homom01phisms*

$$Gw,(L'IK') - \quad G.,,(LIK).$$

$$1,,.,(1.'IK')- \quad I,,,(LIK).$$

$$Rw,(L'IK') - \quad Rw(LIK).$$

In the latter two eci.�e.�, v i� assumed *to* be nonarchimedean.

Proof: Let a' E Gu,,(L'IK') and a= r*(a'). lf.t EL. then one has

$$lxlu,,o = laxlw = \text{Ir} \ ^1a^1Txlw = \text{la'rxlu•'} = \text{lrxlu''} = \text{lxl},,,.$$

so that a E $Gw(LIK)$. If a' E /.,,,(L'IK') and x E 0, then

$$w(ax - x) = w(r^{-1}(a'rx - Tx)\} = w'(o'(rx) - (rx)\} > 0,$$

and a E $I,i,(LIK)$. If a' E $Rw,(L'IK')$ and x EL�, then

$$w(\text{�} - 1) = w(r^{\ 1}(\underline{a::x} \ 1)) = \underline{w'(a::x} \ 1) > 0,$$

�o that a E Ru-(LIK). □

If the two homomorphisms r L -+ L' and r K -+ K' are isomorphisms, then the homomorphisms (9.4) are of course isomorphisms. In particular, in the case $K = K'$. $L = L'$. we find for each r E $G(L$ IK):

$$GwAr = r^{-1}G_{11}\, r, \quad Iw,,=r^{-1}fuT, \quad R_{11}.,=r^{-1}R.,,T,$$

i.e., the decomposition, inertia, and ramification groups of conjugate valuations are conjugate.

Another �pecial case arises from an intermediate field M of LI K by the diagram

$$L \qquad\qquad L$$

$$Kc \_\_\_\_\_ ,,. \ M.$$

r* then becomes the indm,ion G(LIM) "-----c>- G(LIK), and we trivially get the

(9.5) Proposition. *For the extension $K \subseteq M \subseteq L$, one has*

$$G_w(L|M) = G_w(L|K) \cap G(L|M),$$
$$I_w(L|M) = I_w(L|K) \cap G(L|M),$$
$$R_w(L|M) = R_w(L|K) \cap G(L|M).$$

A particularly important special case of (9.4) occurs with the diagram

$$\begin{array}{ccc} L & \text{-------} & L_w \\ & & | \\ & & K_v \\ K & & \end{array}$$

which can be associated to any extension of valuations $w|v$ of $L|K$. If $L|K$ is infinite, then L_w has to be read as the localization in the sense of §8, p. 160. (This distinction is rendered superfluous if we consider, as we may perfectly well do, the henselization of $L|K$.) Since in the local extension $L_w|K_v$ the extension of the valuation is unique, we denote the decomposition, inertia, and ramification groups simply by $G(L_w|K_v)$, $I(L_w|K_v)$, $R(L_w|K_v)$. In this case, the homomorphism τ^* is the restriction map

$$G(L_w|K_v) \longrightarrow G(L|K), \quad \sigma \longmapsto \sigma|_L,$$

and we have the

(9.6) Proposition. $G_w(L|K) \cong G(L_w|K_v)$,

$$I_w(L|K) \cong I(L_w|K_v),$$
$$R_w(L|K) \cong R(L_w|K_v).$$

Proof: The proposition derives from the fact that the decomposition group $G_w(L|K)$ consists precisely of those automorphisms $\sigma \in G(L|K)$ which are continuous with respect to the valuation w. Indeed, the continuity of the $\sigma \in G_w(L|K)$ is clear. For an arbitrary continuous automorphism σ, one has

$$|x|_w < 1 \iff |\sigma x|_w < 1,$$

because $|x|_w < 1$ means that x^n and hence also σx^n is a w-nullsequence, i.e., $|\sigma x|_w < 1$. By §3, p. 117, this implies that w and $w \circ \sigma$ are equivalent, and hence in fact equal because $w|_K = w \circ \sigma|_K$, so that $\sigma \in G_w(L|K)$.

Since L is dense in L_w, every $\sigma \in G_w(L|K)$ extends uniquely to a continuous K_v-automorphism $\hat\sigma$ of L_w, and it is clear that $\hat\sigma \in I(L_w|K_v)$, resp. $\hat\sigma \in R(L_w|K_v)$, if $\sigma \in I_w(L|K)$, resp. $\sigma \in R_w(L|K)$. This proves the bijectivity of the mappings in question in all three cases. □

The above propo�ition reduce,; the problem� concerning a single valuation of *K* to the local �ituation. We identify the decomposition group *G,,* (LIK) with the Galois group of *L w* I*K_I_* and write

G.,,(LIK) � G(L,,,IK,,),

and similarly /,,.(LIK) = /(L,,,IK,,) and *R,,.(LIK)* = *R(L11,IKv).*

We now explain the concrete meaning of the �ubgroups G,,,, */11• R,,.* of *G* = *G*(LI*K)* for the field extension LI*K.*

The **decomposition group** *Gw* consists - as was shown in the proof of (9.6) - of all automorphisms *a* E G that are **continuous** with respecl to the valuation *w.* It controls the extension of *v* to *L* in a group-theoretic manner. Denoting by Gu,\G the set of all right cosets *G,, a,* by *W"* the ,;ct of exten<,ion� of *v* to Land choosing a fixed extension *w,* we obtain a bijection

$$G_w\backslash G \xrightarrow{\sim} W_v\,, \quad G_w\sigma \longmapsto w\sigma\,.$$

In particular, the number *#Wv* of extensions equals the index (G: G,,,). As mentioned already in chap. I, *9 - and left for the reader to verify - the decomposition group also describes the way a valuation 1• extends to an arbitrary separable extension *LIK.* For this. we embed *LIK* into a Galois extension *NIK,* choose an cxtemion *U'* of 1• to *N,* and put *G* = *G(NIK).* *H* = G(NIL), G,,, = *G,,,(NIK),* to get a bijection

G,,.\G/H.....:::,,. W₀- *Gu,aH* f-------+ *woalr*

(9.7) **Definition.** *The fixed field* of *G 11* ,

2₁₁. = Zu,(LIK) = *{x* EL | *ax =x for,Jll a* E G,,,),

i� *called the* **decomposition field** of *w over K.*

The r6le of the decomposition llcld in the extension LI*K* is described by the following proposition.

(9.8) Proposition.

(i) *The restriction WL* ofw *to* Zw extends *uniquely* to *L.*

(ii) *If* 1• j,\ nonarc/Jimedean, *1117* /Jas *the* same residue *das� lic/d* and *the* �ame value *group* as 1•.

(iii) Z.,, = *L n K,,* (1/Jc *inicr�ccrion* i� *wken imide L.,,).*

Proof: (i) An arbitrary extem,ion *w'* of *wz* to *L* is conjugate *tow* over *Zu-;* thw;. *W' = w* o *a,* for some *a* E G(LIZ11.) = *Gu,,* i.e., *w' = w.*

(iii) The identity *Zu,* = *L* n *Kv* follows immediately from *Gu-(LIK)* � *G(L,,,IK,),*

(ii) Since *Kv* has the i,,ame residue class field and the 5ame value group as *K,* the same holds true for Z*w* = *L* n *K*,,. lJ

The **inertia group** *I,,,* is defined only if *w* is a nonarchimedean valuation of *L.* It i5 the kernel of a canonical homomorphism of G.,,. For if *O* is the valuation ring of *w* and ',l3 the maximal ideal, then. since *aO* = CJ and *aq]* = 1], every *a* E G_{11}, induces a K-automorphism

0: CJ/',13------+ 0/1}, *x* mod ',l3 i-------+ *ax* mod 1},

of the residue c\a55 field A, and we obtain a homomorphi<,m

$$G_w \longrightarrow \mathrm{Aut}_\kappa(\lambda)$$

with kernel *I.,,.*

(9.9) **Proposition.** *The residue class field* extension AIK *is* nonnal, *and* we /Jave *an exact* �equence

$$1 \longrightarrow I_w \longrightarrow G_w \longrightarrow G(\lambda|\kappa) \longrightarrow 1.$$

Proof: l11 the case of a finite Galois extension, we have proved thii,, already in chap. I, (9.4). In the infinite cai,,e AIK is normal 5ince *LIK,* and hence also A IK, is the union of the finite nonnal subexten5ions. In order to prove the i,,urjectivity *off: Gw----+* G(AIK) all one ha5 to show ii,, that f(G.,,) is dense in G(AIK) because *j* (Gw), being the continuous image of a compact set, is compact and hence do&ed. Let *cf* E G(AIK) and OG(AIµ) be a neighbourhood of *0,* where *µIK* is a finite Galois subextension of AIK. We have to show that this neighbourhood contains an element of the image *f* (r), r E G1,,. Since *Zu,* has the re5idue class llcld *K,* there exi�ts a finite Galois rnbextension *MIZw* of LIZa, whose residue class field *M* containi,, the field *tL* As G(MIZ0,)----+G(MIK) is surjective. the composite

$$G_w = G(L|Z_w) \longrightarrow G(M|Z_w) \longrightarrow G(\overline{M}|\kappa) \longrightarrow G(\mu|\kappa)$$

is abo &urjective. and if r E G.,, ii,, mapped to01,, then f(r) E irG(AltL),

--� □

(9.10) Definition. *The fixed field* of $/_{11''}$

$$Tw = T_{,,.}(LIK) = \backslash X \text{ EL } | _{(J.I} = \backslash \text{ foraJJ } _{(J} \text{ E } /.,,),$$

i,s *called the* **inertia field** of w over K.

For the inertia field, (9.9) gives u:,. the isomorphism

$$G(T_w|Z_w) \cong G(\lambda|\kappa).$$

It ha:,. the following significance for the extension LIK.

(9.11) Proposition. $T_{,,}$ IZ..,, is *the* maxinrn/ *unramilicd* �ubexrension of LIZ,,,.

Proof: By (9.6), we may asmme that $K = Z_{,,}$ is henselian. Let TIK be the maximal unramilied :,.uhextension of LIK. It i5 Galois, since the conjugate extensions are also unramified. Hy (7.5). T has the residue clas<: field A,, and we have an isomorphism

$$G(T|K) \xrightarrow{\sim} G(\lambda_s|\kappa).$$

Surjectivity follows from (9.9) and the injectivity from 1he fact that TiK is unramillcd: every finite Galois suhexten:;.ion has the <:ame degree as its residue class field extension. An element $_{(J}$ E G(LIK) therefore induces the identity on A,. i.e.. on A, if and only if it belong:,. to G(L IT). Consequently, G(LIT) $=$ Iv-, hence $T = T_{11''}$ □

If in particular K is a henselian field and K, IK its separable closure, then the inertia field of this exten:;.ion is *the* maximal unramified exten:,.ion TI K and has the separable closure K., IK a:,. it:,. residue clas:,. field. The isomorphism

$$G('/'IK) \text{ � } G(K,IK)$$

:,.hows that the unramified exten&ions of K correspond 1-1 to the :,.eparable extensions of κ.

Like the inertia group, the **ramification group** $R_{,,}$ is the kernel of a canonical homomorphbm

$$I_w \to \chi(L|K),$$

where

$$x(I.IK) = \text{Hom}(Ll/r.r).$$

where Ll $=$ *w(L*)*, and r $=$ *v(K*)*. If *a* E /,,,, then the associated homomorphism

$$Xa: \ !J/I' \to A^*$$

as follows: for $K = 0$ mod r E *iJ/I'*, choo:;,c an *x* EL* such that $= 8$ and put

$$Xa(\bar{O}) = � ^{a,\cdot} \ \text{modq.3.}$$

Thi� definition is independent of the choice of the representative *8* E *8* and of *x* E *L**. for if *x'* E *L** is an element such that *w(x')* $=$ w(x) mod *r,* then w(x') $=$ *w(xa), a* E *K*.* Then .t' $=$ *xau, u* E *0*,* and since *au/u* $=$ 1 mod 11] (bccau:;.c *u* E /,:p), one gets $ax^1/x^1 = ax/x$ mod l.p.

One sees immediately that mapping *a* i--+ *x,,* is a homomorphism $1_{11,} \to$ *x(LIK)* with kernel *Rw.*

(9.12) Proposition. *R,,, is the unique p-Sylow subgroup* of $/_{11,}$

Remark: If LI *K* is a linite cxtcm,ion, then it is clear what this means. In the infinite ca<,c it ha,; to be understood in the sense of **profinite groups,** i.e., all finite quotient groups of *R,,.,* resp. /,,,/ $R_{11.}$ by dosed nonnal -;ubgroup:-. have p-power order, resp. an order prime *top.* In order to under�tand this better, we refer the reader to chap. IV, § 2. exercise 3-5.

Proof of (9.12): By (9.6), we may a�sumc that *K* is hen�elian. We restrict to the case where Ll *K* j5 a finite extension. The infinite case of the proposition follows fonnally from this.

If *Ru,* were not a p-group. then we would find an element *a* E *R,,,* of prime order £ -=/=- *p.* Let *K'* he the fixed field of *a* and *κ'* its residue class field. We show that *κ'* =A.Since *Ru,* £;; *fu,,* we have that *T* i; *K'.* Thus A, i; κ^1, so that AIK' is purely inseparable and of p-power degree. On the other hand, the degree has to be a power of£, for if *ii* EA and if o' EL is a lifting of *ii*, and f"Cl) E K'[xl b the minimal polynomial of *a* over *K'*, then *_f(x)* = *}{(xr,* where }{(x) E κ'lx] is the minimal polynomial of *ii* over κ^1• which has degree either I or £, as this is so for *f(x)*. Thus we have indeed *κ'* =A.so that *LIK'* is tamely ramified, and by (7.7) is of the form *L* $=$ *K'(a)* with *a* = *!/a, a* E *K'.* It follows that *m.x* =(a.with a primitive *{-th* root of unity (E K^1• Since *a* E R_{11},. we have on the other hand *aa/a* = *l;* =a I mod l_p, a contradiction. Thi� proves that R_{11} is a p-group.

Since *p* = char(A), the elements in have order prime to *p,* provided they are of finite order. The group *x(LIK)* = Hom(Ll/I',A*) therefore has order prime top. Thi� abo applie� to the group *l,r/Ru,* i; *x(LIK),* sothat R_{11}• is indeed the unique p-Sylow subgroup. LJ

(9.13) Definition. *The fixed field of R,,,,*

$$Vu,= V,,.(LIK) = \{x \ EL \ | \ ax \ =x \quad \text{for } all \quad a \ E \ Ru,\},$$

is *ca/Jed the* **ramification field** *of w over K.*

(9.14) Proposition. *VwlZw* is *the maximal tamely* ramified *subextemion* ofLIZu,.

Proof: By (9.6) and the fact that the value group and residue class field do not change, we may a<,5ume that $K = Zu,$ is henselian. Let V,r be the fixed field of *R,l'-* Since *Rw* is the p-Sylow subgroup of/,,,, *Vu,* is the union of all finite Galois subextension5 of *LIT* of degree prime to *p.* Therefore *V.,,* contains the maximal tamely ramified extension V of T (and thm of Z,p). Since the degree of each finite subextension MI *V* of *V.,,*IV is not divi5iblc by *p,* the residue field extension of MI *V* is separable (see the argument in the proof of (9.12)). Therefore *Vwl V* is tamely ramified, and *V.,,* = *V.* n

(9.15) Corollary. *We have the exact sequence*

$$\text{I}\text{--+} R.,,\text{--+} fw\text{--+} x(LIK)\text{--+} \text{I}.$$

Proof: By (9.6) we may as5ume, as we have already done several times before, that K is hense\ian. We restrict to considering the case of a llnite extension LI *K.* In the infinite case the proof follow:- as in (9.9). We have already seen that *R,,* i� the kernel of the arrow on the right. It therefore suffices to show that

$$(I_w : R_w) = [V_w : T_w] = \#\chi(L|K).$$

As *TwlK* is the maximal unramificd �ubextension of *V₁₁,IK, V,,,l'l�,* has inertia degree I. Thus, by (7.7),

$$[V,,. \ c \ T.,,] \ �\#(w(V;)fw(T,;))$$

Furthermore, by (7.5), we have $w(T_w^*) = v(K^*) =: r,$ and putting L1 = *w(L *),* we �ec tha$w(V_w^*)/v(K^*)$ is the subgroup .::1u,i;r of *!J.Jr* consisting of all element:- of order prime *top,* where p = char(K). Thus

$$V_w : T_w] = \#(\Delta^{(p)}/\Gamma).$$

Since A* ha� no clements of order divisible by *p,* we have on the other hand that

$$\chi(L|K) = \operatorname{Hom}(\Delta/\Gamma, \lambda^*) = \operatorname{Hom}(\Delta^{(p)}/\Gamma, \lambda^*).$$

But (7.7) impliei,, that A* contains them-th roob of unity whenever ,1.(f'J / r contains an element of order m, because then there is a Galoi� extension generated by radicals T,,,(n:./a)ll'w of degree m. This showi,, that x(LIK) i� the Pontryagin dual of the group $6.^{1}$f!) / I' so that indeed

$$V_w : T_w] = \#(\Delta^{(p)}/\Gamma) = \#\chi(L|K)\,.$$ □

Exercise **1.** Let K be a hen�clian !ield, LIK a ramitied Galm.\ exten�1on, $C; =$ G{LIK), $f = l(LIK)$ and $r =$ G/1 $=$ I is ahehan and become� aI'-modu!ebylettmgi.r=aiEI'operatcon Tf---'+ara 1.

Show that there i� a canonical isomorphi�m I � x(LIK) ot I'-modulc�. Show furthermore that tamely ramified extension can he embedded into a tamely ramified extcmion �uch that G j\ the �cmi-direct product of $X(l$ IK) with G(AIK): G � >1 G(AIK).

Hint: Use (7.7).

Exercise 2. The maximal tamdy ramified ahclian exten�ion V of Q\, i� finite over the maximal unram1!ied abelian extemion T of Q_{1}..

Exercise 3. Show that the maximal unramified extension of the power �cries field $K =$ is given by $T =$ IF\((t)), where $\overline{\mathbb{F}}_p$ i� the lgebraic closure of 1?'1,. and the amely ramified extension by $T(\{\sqrt[m]{t}$ Im E $\mathbb{N}, (m,p)=1\})$.

Exercise **4.** Let v be a nonarch1rnedean valuallon of the field K and let i; he an cxtcn�ion to the separable clo�ure K of K. Then the dccornpo�it1on held Z_1 of r over K i� isomorphic to the hcn�eli7at1on of K with respect to L". m the �en�e of §6. p. 143.

§ 10. Higher Ramification Groups

The inertia group and the ramification group inside the Galois group of valued fields are only the first term� in a whole seric<, of �ubgroups that we arc now going to study. We assume that LIK b a finite Galob extension and that v_K is a discrete nonnalized valuation of K, with po�itivc residue field characteristic p, which admits a *unique* extension w to L. We denote by $v_r = cw$ the associated nonnalized valuation of L.

(10.1) Definition. *For every* re,J/ number s � - I *we define lhc* s-th **ramification group** of LI K *by*

$$G_s = G_s(L|K) = \{ \sigma \in G \mid v_L(\sigma a - a) \geq s + 1 \text{ for all } a \in \mathcal{O} \}$$

Clearly, $G_{-1} = G$, G_0 is the inertia group $I = I(L|K)$, and G_1 the ramification group $R = R(L|K)$ which have already been defined in (9.3). As

$$v_L(\tau^{-1}\sigma\tau a - a) = v_L(\tau^{-1}(\sigma\tau a - \tau a)) = v_L(\sigma(\tau a) - \tau a)$$

and $\tau\mathcal{O} = \mathcal{O}$, the ramification groups form a chain

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$$

of normal subgroups of G. The quotients of this chain satisfy the

(10.2) Proposition. *Let $\pi_L \in \mathcal{O}$ be a prime element of L. For every integer $s \geq 0$, the mapping*

$$G_s/G_{s+1} \longrightarrow U_L^{(s)}/U_L^{(s+1)}, \quad \sigma \longmapsto \frac{\sigma\pi_L}{\pi_L},$$

is an injective homomorphism which is independent of the prime element π_L. Here $U_L^{(s)}$ denotes the s-th group of principal units of L, i.e., $U_L^{(0)} = \mathcal{O}^*$ and $U_L^{(s)} = 1 + \mathfrak{P}^s$, for $s \geq 1$.

We leave the elementary proof to the reader. Observe that one has $U_L^{(0)}/U_L^{(1)} \cong \lambda^*$ and $U_L^{(s)}/U_L^{(s+1)} \cong \lambda$, for $s \geq 1$. The factors G_s/G_{s+1} are therefore abelian groups of exponent p, for $s \geq 1$, and of order prime to p, for $s = 0$. In particular, we find again that the ramification group $R = G_1$ is the unique p-Sylow subgroup in the inertia group $I = G_0$.

We now study the behaviour of the higher ramification groups under change of fields. If only the base field K is changed, then we get directly from the definition of the ramification groups the following generalization of (9.5).

(10.3) Proposition. *If K' is an intermediate field of $L|K$, then one has, for all $s \geq -1$, that*

$$G_s(L|K') = G_s(L|K) \cap G(L|K').$$

Matters become much more complicated when we pass from $L|K$ to a Galois subextension $L'|K$. It is true that the ramification groups of $L|K$ are mapped under $G(L|K) \to G(L'|K)$ onto the ramification groups of $L'|K$, but the indexing changes. For the precise description of the situation we need some preparation. We will assume for the sequel that the residue field extension $\lambda|\kappa$ of $L|K$ is **separable**.

(10.4) Lemma. *The ring extension $\mathcal{O}$ of o is monogenous, i.e., there exists an $x \in \mathcal{O}$ such that $\mathcal{O} = o[x]$.*

Proof: As the residue field extension $\lambda|\kappa$ is separable by assumption, it admits a primitive element $\bar{x}$. Let $f(X) \in o[X]$ be a lifting of the minimal polynomial $\bar{f}(X)$ of $\bar{x}$. Then there is a representative $x \in \mathcal{O}$ of $\bar{x}$ such that $\pi = f(x)$ is a prime element of $\mathcal{O}$. Indeed, if x is an arbitrary representative, then we certainly have $v_L(f(x)) \geq 1$ because $\bar{f}(\bar{x}) = 0$. If x itself is not as required, i.e., if $v_L(f(x)) \geq 2$, the representative $x + \pi_L$ will do. In fact, from Taylor's formula

$$f(x+\pi_L) = f(x) + f'(x)\pi_L + b\pi_L^2, \quad b \in \mathcal{O},$$

we obtain $v_L(f(x+\pi_L)) = 1$ since $f'(x) \in \mathcal{O}^*$, because $\bar{f}'(\bar{x}) \neq 0$. In the proof of (6.8), we saw that the

$$x^j \pi^i = x^j f(x)^i, \quad j = 0, \dots, f-1, \quad i = 0, \dots, e-1,$$

form an integral basis of $\mathcal{O}$ over o. Hence indeed $\mathcal{O} = o[x]$. $\square$

For every $\sigma \in G$ we now put

$$i_{L|K}(\sigma) = v_L(\sigma x - x),$$

where $\mathcal{O} = o[x]$. This definition does not depend on the choice of the generator x and we may write

$$G_i(L|K) = \{\sigma \in G \mid i_{L|K}(\sigma) \geq i+1\}.$$

Passing to a Galois subextension $L'|K$ of $L|K$, the numbers $i_{L|K}(\sigma)$ obey the following rule.

(10.5) Proposition. *If $e' = e_{L|L'}$ is the ramification index of $L|L'$, then*

$$i_{L'|K}(\sigma') = \frac{1}{e'} \sum_{\sigma \mapsto \sigma'} i_{L|K}(\sigma).$$

Proof: For $\sigma' = 1$ both sides are infinite. Let $\sigma' \neq 1$, and let $\mathcal{O} = o[x]$ and $\mathcal{O}' = o[y]$, with $\mathcal{O}'$ the valuation ring of L'. By definition, we have

$$e' i_{L'|K}(\sigma') = v_L(\sigma' y - y), \quad i_{L|K}(\sigma) = v_L(\sigma x - x).$$

We choose a fixed $\sigma \in G = G(L|K)$ such that $\sigma|_{L'} = \sigma'$. The other elements of G with image σ' in $G' = G(L'|K)$ are then given by $\sigma\tau$, $\tau \in H = G(L|L')$. It therefore suffices to show that the elements

$$a = \sigma y - y \quad \text{and} \quad b = \prod_{\tau \in H} (\sigma\tau x - x)$$

generate the same ideal in $\mathcal{O}$.

Let /(X) E *O'[X]* be the minimal polynomial of *x* over *L'* Then *f(X) = fln=ll(X - rx)*. Letting *a* act on the coefficients *off,* we get the polynomial (er *f)(X)* = flrE// *(X* - arx). The coefficient� of *rrf - f* are all divisihle by *a= ay - y*. Hence *a* divides *(a.f)(x) - f(x)* = ±*h*.

To show that conversely his a divi5or of *a,* we write ya:-, a polynomial in *x* with coefficients in CJ, *y* = g(t). A& *x* is a zero of the polynomial *g(X) - y* E (TfXl, we have

s(X) - *y* � f(X)h(X). h(X) E O'[XJ.

Letting *a* operate on the coefficients of both sides and then :-,ubstituting *X = x* yield:-, *y - ay = (af)(x)(ah)(x)* = ±*h(ah)(x),* i.e., *h* divide:-, *a.* □

We now want to :-,how that the ramification group *G,(LIK)* is mapped onto the ramification group $G_1(L'IK)$ by the projection

G(L[K) - G(L°IK).

where *r* is given by the function *111.iK* : (-1. :xi)----+ f-1, oo),

$$t = 'IL1K(s) = \int_0^{'} \frac{\_,\_h\_}{(Go: G1)}$$

Here (Go Gt) is meant to denote the inverse (G, $G_{0})^{-1}$ when -1 :==*x* :::0, i.e.,:-,imply I, if-I<.,::: 0.For0 < *m* :== *s* :== *m*+ *l.m* EN, we have explicitly

1JL1K(S) = _!_Ct:1 +K2 +···+*gm*+*(.\' -m)gnH* 1) - *g;* =#G,.
Ro

The function *1JLIK* can be expre%cd in terms of lhe numbers *ILiK(a)* as follows:

(10.6) Proposition. *'ILIK* (�) = :Ju LrrEG min\ *iL K* (a), *s* + t j - I.

Proof: Let (;l(s) be the function on the right-hand side. It i:-, continuous and piecewi:-,e linear. One ha& H(O) = *1JLiK* (0) = 0, and if *m* 2: -1 is an integer andm <*s* <*m*+],then

$$9'(s) = \frac{1}{g_0}\#\{\sigma \in G \mid i_{L|K}(\sigma) \geq m+2\} = \frac{1}{(G_0 : G_{m+1})} = \eta'_{L|K}(s).$$

Hence *O* = *1}t* IK· 'J

(10.7) Theorem (HERBRAND). *Let $L'|K$ be a Galois subextension of $L|K$ and $H = G(L|L')$. Then one has*

$$G_s(L|K)H/H = G_t(L'|K) \quad \text{where} \quad t = \eta_{L|L'}(s).$$

Proof: Let $G = G(L|K)$, $G' = G(L'|K)$. For every $\sigma' \in G'$, we choose a preimage $\sigma \in G$ of maximal value $i_{L|K}(\sigma)$ and show that

$$i_{L'|K}(\sigma') - 1 = \eta_{L|L'}\big(i_{L|K}(\sigma) - 1\big).$$

Let $m = i_{L|K}(\sigma)$. If $\tau \in H$ belongs to $H_{m-1} = G_{m-1}(L|L')$, then $i_{L|K}(\tau) \geq m$ and $i_{L|K}(\sigma\tau) \geq m$, so that $i_{L|K}(\sigma\tau) = m$. If $\tau \notin H_{m-1}$, then $i_{L|K}(\tau) < m$ and $i_{L|K}(\sigma\tau) = i_{L|K}(\tau)$. In both cases we therefore find that $i_{L|K}(\sigma\tau) = \min\{i_{L|K}(\tau), m\}$. Applying (10.5), this gives

$$i_{L'|K}(\sigma') = \frac{1}{e_{L|L'}} \sum_{\tau \in H} \min\{i_{L|K}(\tau), m\}.$$

Since $i_{L|K}(\tau) = i_{L|L'}(\tau)$ and $e' = e_{L|L'} = \#H_0$, (10.6) gives the formula (*), which in turn yields

$$\begin{aligned}
\sigma' \in G_sH/H &\iff i_{L|K}(\sigma) - 1 \geq s \iff \eta_{L|L'}(i_{L|K}(\sigma) - 1) \geq \eta_{L|L'}(s)\\
&\iff i_{L'|K}(\sigma') - 1 \geq \eta_{L|L'}(s)\\
&\iff \sigma' \in G_t(L'|K), \quad t = \eta_{L|L'}(s).
\end{aligned}$$

□

The function $\eta_{L|K}$ is by definition strictly increasing. Let the inverse function be $\psi_{L|K} : [-1, \infty) \to [-1, \infty)$. One defines the **upper numbering** of the ramification groups by

$$G^t(L|K) := G_s(L|K) \quad \text{where} \quad s = \psi_{L|K}(t).$$

The functions $\eta_{L|K}$ and $\psi_{L|K}$ satisfy the following transitivity condition:

(10.8) Proposition. *If $L'|K$ is a Galois subextension of $L|K$, then*

$$\eta_{L|K} = \eta_{L'|K} \circ \eta_{L|L'} \quad \text{and} \quad \psi_{L|K} = \psi_{L|L'} \circ \psi_{L'|K}.$$

Proof: For the ramification indices of the extensions $L|K$, $L'|K$, $L|L'$ we have $e_{L|K} = e_{L'|K}\, e_{L|L'}$. From (10.7), we obtain $G_sH/H = (G/H)_t$, $t = \eta_{L|L'}(s)$, thus

$$\frac{1}{e_{L|K}}\#G_s = \frac{1}{e_{L'|K}}\#(G/H)_t\,\frac{1}{e_{L|L'}}\#H_s.$$

This equation is equivalent to

$$\psi'_{L|K}(s) = \psi'_{L'|K}(t)\psi'_{L|L'}(s) = (\psi_{L'|K} \circ \psi_{L|L'})'(s).$$

As $\psi_{L|K}(0) = (\psi_{L'|K} \circ \psi_{L|L'})(0)$, it follows that $\psi_{L|K} = \psi_{L'|K} \circ \psi_{L|L'}$ and the formula for φ follows. $\square$

The advantage of the upper numbering of the ramification groups is that it is invariant when passing from $L|K$ to a Galois subextension.

(10.9) Proposition. *Let $L'|K$ be a Galois subextension of $L|K$ and $H = G(L|L')$. Then one has*

$$G^t(L|K)H/H = G^t(L'|K).$$

Proof: We put $s = \psi_{L|K}(t)$, $G' = G(L'|K)$, apply (10.7) and (10.8), and get

$$G^t H/H = G_{\psi_{L|K}(t)}H/H = G'_{\varphi_{L|L'}(\psi_{L|K}(t))} = G'_{\psi_{L'|K}(t)} = G'^t. \qquad \square$$

Exercise 1. Let K and $K_n = K(\zeta)$, where ζ a primitive p^n-th root of unity. Show that the groups of $K_n|K$ are given as follows:

$$G_s = G(K_n|K) \quad \text{for } s = 0,$$
$$G_s = G(K_n|K_1) \quad \text{for } 1 \le s \le p-1,$$
$$G_s = G(K_n|K_2) \quad \text{for } p \le s \le p^2-1,$$
$$G_s = 1 \quad \text{for } p^{n-1} \le s.$$

Exercise 2. Let K' be an intermediate field of $L|K$. Describe the relation between the ramification groups of $L|K$ and of $L|K'$ in the upper numbering.

Chapter III

Riemann-Roch Theory

§ 1. Primes

Having set up lhe general theory of valued fields, we now return to algebraic number fields. We want to develop their basic theory from the valuation-theoretic point of view. This approach ha� two prominent advantages compared to the ideal-theoretic treatment given in the first chapter. The first one results from the possibility of pa��ing to completions, thereby enacting the important "local-to-global principle". Thi� will he done in chapter VI. The other advantage lies in the fact that the archimedean valuations bring into the picture the points at infinity, which were hitherto lacking, as the "primes at inlinity" In this way a perfect analogy with the function fields is achieved. This is the task to which we now tum.

(I.I) Definition. *A* prime (or place) p of *an algebraic* number *field K is a* cfas.� of *equivalent valuation�* of *K. The nonarchimcdcan equivalence* c/a.�ses *arc rnlled* finite prime.� *and the an:himedean* ones infinite *prime�.*

The infinite primes pare obtained, according to chap. II, (8.1), from the embeddings $\tau : K \to$ C. There arc two sorts of these: the real primes, which arc given by embedding5 $\tau : K \to$ R., and tbe complex primes. which arc induced by the pairs of complex conjugate non-real embcdding1i $K \to$ C. p i1s real or complex depending whether the completion KP is isomorphic to IR or to C. The infinite primes will be referred to by the formal notation p I oc, the finite ones by p 1cc.

In the case of a finite prime, the letter p ha1i a multiple meaning: ii also stand<; for the prime ideal of the ring CJ of integers of *K.* or for the maximal ideal of the associated valuation ring, or even for the maximal ideal of the completion. However, thi5 will nowhere create any risk of confusion. We write PIP if pis the characteri�tic of the re1iidue field *K():l)* of the Jinile prime p. For an infinite prime we adopt the convention that the completion KP also serve� as its own '·residue field." i.e., we put

$$K(p) := K_p, \quad \text{when } p|\infty.$$

To each prime $\mathfrak{p}$ of K we now associate a canonical homomorphism

$$v_{\mathfrak{p}} : K^* \longrightarrow \mathbb{R}$$

from the multiplicative group K^* of K. If $\mathfrak{p}$ is finite, then $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic exponential valuation which is normalized by the condition $v_{\mathfrak{p}}(K^*) = \mathbb{Z}$. If $\mathfrak{p}$ is infinite, then $v_{\mathfrak{p}}$ is given by

$$v_{\mathfrak{p}}(a) = -\log|\tau a|, \quad \text{where}$$

$\tau : K \longrightarrow \mathbb{C}$ is an embedding which defines $\mathfrak{p}$.

For an arbitrary prime $\mathfrak{p} \mid p$ (p prime number or $p = \infty$) we put furthermore

$$f_{\mathfrak{p}} = [\kappa(\mathfrak{p}) : \kappa(p)],$$

so that $f_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{R}]$ if $\mathfrak{p} \mid \infty$, and

$$\mathfrak{N}(\mathfrak{p}) = \begin{cases} p^{f_{\mathfrak{p}}} & \text{if } \mathfrak{p} \nmid \infty, \\ e^{f_{\mathfrak{p}}} & \text{if } \mathfrak{p} \mid \infty. \end{cases}$$

This convention suggests that we consider e as being an infinite prime number, and the extension $\mathbb{C}|\mathbb{R}$ as being *unramified* with inertia degree 2. We define the absolute value $|\ |_{\mathfrak{p}} : K \to \mathbb{R}$ by

$$|a|_{\mathfrak{p}} = \mathfrak{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(a)}$$

for $a \neq 0$ and $|0|_{\mathfrak{p}} = 0$. If $\mathfrak{p}$ is the infinite prime associated to the embedding $\tau : K \to \mathbb{C}$, then one finds

$$|a|_{\mathfrak{p}} = |\tau a|, \quad \text{resp.} \quad |a|_{\mathfrak{p}} = |\tau a|^2,$$

if $\mathfrak{p}$ is real, resp. complex.

If $L|K$ is a finite extension of K, then we denote the primes of L by $\mathfrak{P}$ and write $\mathfrak{P} \mid \mathfrak{p}$ to signify that the valuations in the class $\mathfrak{P}$, when restricted to K, give those of $\mathfrak{p}$. In the case of an infinite prime $\mathfrak{P}$ we define the inertia degree, resp. the ramification index, by

$$f_{\mathfrak{P}|\mathfrak{p}} = [L_{\mathfrak{P}} : K_{\mathfrak{p}}], \quad \text{resp.} \quad e_{\mathfrak{P}|\mathfrak{p}} = 1.$$

For arbitrary primes $\mathfrak{P} \mid \mathfrak{p}$ we then have the

(1.2) Proposition. (i) $\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}} = \sum_{\mathfrak{P}|\mathfrak{p}} [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L : K]$,

(ii) $\mathfrak{N}(\mathfrak{P}) = \mathfrak{N}(\mathfrak{p})^{f_{\mathfrak{P}|\mathfrak{p}}}$,

(iii) $v_{\mathfrak{P}}(a) = e_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{p}}(a)$ for $a \in K^*$,

(iv) $v_{\mathfrak{p}}(N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(a)) = f_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(a)$ for $a \in L_{\mathfrak{P}}^*$,

(v) Ial'lJ = INL,ll'Kp(a)lp fora EL.

The normalized valuations $|\ |_{\mathfrak p}$ satisfy the following **product formula,** which demonstrates how important it is to include the infinite primes.

(1.3) Proposition. *Given any $a \in K^*$, one has $|a|_{\mathfrak p} = 1$ for almost all $\mathfrak p$, and*

$$\prod_{\mathfrak p} |a|_{\mathfrak p} = 1 .$$

Proof: We have $v_{\mathfrak p}(a) = 0$ and therefore $|a|_{\mathfrak p} = 1$ for all $\mathfrak p$ which do not occur in the prime decomposition of the principal ideal (a) (see chap. I, § 11, p. 69). This therefore holds for almost all $\mathfrak p$. From (1.2) and formula (8.4) of chap. II,

$$N_{K|\mathbb{Q}}(a) = \prod_{\mathfrak p | p} N_{K_{\mathfrak p}|\mathbb{Q}_p}(a)$$

(which includes the case $p = \infty$, $\mathbb{Q}_\infty = \mathbb{R}$), we obtain the product formula for K from the product formula for $\mathbb{Q}$, which was proved already in chap. II, (2.1):

$$\prod_{\mathfrak p} |a|_{\mathfrak p} = \prod_p \prod_{\mathfrak p | p} |a|_{\mathfrak p} = \prod_p \prod_{\mathfrak p | p} \left| N_{K_{\mathfrak p}|\mathbb{Q}_p}(a) \right|_p = \prod_p \left| N_{K|\mathbb{Q}}(a) \right|_p = 1 \qquad \square$$

We denote by $J(\mathfrak o)$ the group of fractional ideals of K, by $P(\mathfrak o)$ the subgroup of fractional principal ideals, and by

$$Pic(\mathfrak o) = J(\mathfrak o)/P(\mathfrak o)$$

the ideal class group Cl_K of K.

Let us now extend the notion of fractional ideal of K by taking into account also the infinite primes.

(1.4) Definition. *A* **replete ideal** *of K is an element of the group*

$$J(\bar{\mathfrak o}) := J(\mathfrak o) \times \prod_{\mathfrak p | \infty} \mathbb{R}_+^* ,$$

where $\mathbb{R}_+^*$ denotes the multiplicative group of positive real numbers.

In order to unify notation, we put, for any infinite prime $\mathfrak p$ and any real number $\nu \in \mathbb{R}$,

$$\mathfrak p^{\nu} := e^{\nu} \in \mathbb{R}_+^* .$$

Given a system of real numbers $\nu_{\mathfrak p}$, $\mathfrak p \mid \infty$, let $\prod_{\mathfrak p\mid\infty} \mathfrak p^{\nu_{\mathfrak p}}$ always denote the vector

$$\prod_{\mathfrak p\mid\infty} \mathfrak p^{\nu_{\mathfrak p}} = (\ldots, e^{\nu_{\mathfrak p}}, \ldots) \in \prod_{\mathfrak p\mid\infty} \mathbb{R}_+^*$$

and *not* the product of the quantities $e^{\nu_{\mathfrak p}}$ in $\mathbb{R}$. Then every replete ideal $\mathfrak a \in J(\bar{\mathfrak o})$ admits the unique product representation

$$\mathfrak a = \prod_{\mathfrak p\nmid\infty} \mathfrak p^{\nu_{\mathfrak p}} \times \prod_{\mathfrak p\mid\infty} \mathfrak p^{\nu_{\mathfrak p}} = \prod_{\mathfrak p} \mathfrak p^{\nu_{\mathfrak p}},$$

where $\nu_{\mathfrak p} \in \mathbb{Z}$ for $\mathfrak p \nmid \infty$, and $\nu_{\mathfrak p} \in \mathbb{R}$ for $\mathfrak p \mid \infty$. Put

$$\mathfrak a_f = \prod_{\mathfrak p\nmid\infty} \mathfrak p^{\nu_{\mathfrak p}} \quad\text{and}\quad \mathfrak a_\infty = \prod_{\mathfrak p\mid\infty} \mathfrak p^{\nu_{\mathfrak p}}$$

so that $\mathfrak a = \mathfrak a_f \times \mathfrak a_\infty$. $\mathfrak a_f$ is a fractional ideal of K, and $\mathfrak a_\infty$ is an element of $\prod_{\mathfrak p\mid\infty} \mathbb{R}_+^*$. At the same time, we view $\mathfrak a_f$, resp. $\mathfrak a_\infty$ as replete ideals

$$\mathfrak a_f \times \prod_{\mathfrak p\mid\infty} 1, \quad \text{resp.} \quad (1) \times \mathfrak a_\infty.$$

Thus for all elements of $J(\bar{\mathfrak o})$ the decomposition

applies. To $a \in K^*$ we associate the **replete principal ideal**

$$[a] = \prod_{\mathfrak p} \mathfrak p^{v_{\mathfrak p}(a)} = (a) \times \prod_{\mathfrak p\mid\infty} \mathfrak p^{v_{\mathfrak p}(a)}.$$

These replete ideals form a subgroup $P(\bar{\mathfrak o})$ of $J(\bar{\mathfrak o})$. The factor group

$$Pic(\bar{\mathfrak o}) = J(\bar{\mathfrak o})/P(\bar{\mathfrak o})$$

is called the **replete ideal class group, or replete Picard group.**

(1.5) Definition. *The* **absolute norm** *of a replete ideal* $\mathfrak a = \prod_{\mathfrak p} \mathfrak p^{\nu_{\mathfrak p}}$ *is defined to be the positive real number*

$$\mathfrak N(\mathfrak a) = \prod_{\mathfrak p} \mathfrak N(\mathfrak p)^{\nu_{\mathfrak p}}.$$

The absolute norm is multiplicative and induces a surjective homomorphism

$$\mathfrak N : J(\bar{\mathfrak o}) \to \mathbb{R}_+^*.$$

The absolute norm of a replete principal ideal $[a]$ is equal to 1 in view of the product formula (1.3),

$$\mathfrak N([a]) = \prod_{\mathfrak p} \mathfrak N(\mathfrak p)^{v_{\mathfrak p}(a)} = \prod_{\mathfrak p} |a|_{\mathfrak p}^{-1} = 1.$$

We therefore obtain a surjective homomorphism

$$\mathfrak N : Pic(\bar{\mathfrak o}) \to \mathbb{R}_+^*$$

on the replete Picard group.

The relations between the replete ideals of a number field K and tho�c of an extension field L are afforded by the two homomorphisms

$$I(EJK) \overset{ILIK}{\underset{NLIK}{\rightleftarrows}} J(Qt.),$$

which are defined by

;,w(TTP"") �n n 'll""""",

N, dTT'll"") �n n ph,,,,,,_

Herc the various product signs have to be read according to our convention. These homomorphisms satisfy the

(1.6) **Proposition.**

(i) for a *chain* of *fields* K S; L <; *M, one has* NMIK = N1.1K o NMIL and i1vt1K = iMIL o iLiK·

(ii) *Nr1K(iL Ka)=* a^I1·KI fora E *.!(6K)-*

(iii) l)1(N1.1K('2l)) = 1)1(21.) forQl E *J(OL).*

(iv) *If* LIK *is* Galois *with Galois group G. then* for *every* prime *ideal* V *ofoI, one ha� NL1K(V)o1.* = n.,,.c:G *av.*

(v) For *any replete principal ideal* fa] of *K,* resp. *L,* one ha�

iL1d[al) = fa], resp. *NL1K<la]) = INLw(a)].*

(vi) *NLw(211) = NL1K(21)r* i.� *the ide..il* of *K generated by the* nom1s *NL1K(a)* of all *a* E 211.

Proof: (i) is ha1>ed on lhc transitivity of inertia degree and ramification index. (ii) follow1> from (1.2) in view of the fundamental identity L,.pP f'-J.llp<"-J.llP = IL : Kl. (iii) holds for any replete "prime ideal" V of L, hy (1.2):

'll(NL1Kf'lJ)) � '11(p^1·"") � '11(p)^1'•'1" � 'll('l)).

and lhcrcfore for all replete ideals of L.

(iv) The prime ideal plying below V decomposes in the ring O of integers of Las p = (V1 • *VrY,* with prime ideals V, = *a,V, a,* E G/G,ii, which arc conjugates of V and thus have the <,amc inertia degree *f.* Therefore

N,,Kf'l))O�p^1 0� TT'll'.^1 � h n o,r'lJ� n o'l).

(v) For any element $a \in K^*$, (1.2) implies that $v_{\mathfrak P}(a) = e_{\mathfrak P} v_{\mathfrak p}(a)$. Hence

$$i_{L|K}([a]) = i_{L|K}\Big(\prod_{\mathfrak p} \mathfrak p^{v_{\mathfrak p}(a)}\Big) = \prod_{\mathfrak p}\prod_{\mathfrak P|\mathfrak p} \mathfrak P^{e_{\mathfrak P} v_{\mathfrak p}(a)} = \prod_{\mathfrak P} \mathfrak P^{v_{\mathfrak P}(a)} = [a].$$

If, on the other hand, $a \in L^*$, then (1.2) and chap. II, (8.4) imply that $v_{\mathfrak p}(N_{L|K}(a)) = \sum_{\mathfrak P|\mathfrak p} f_{\mathfrak P} v_{\mathfrak P}(a)$. Hence

$$N_{L|K}([a]) = N_{L|K}\Big(\prod_{\mathfrak P} \mathfrak P^{v_{\mathfrak P}(a)}\Big) = \prod_{\mathfrak p} \mathfrak p^{\sum_{\mathfrak P|\mathfrak p} f_{\mathfrak P} v_{\mathfrak P}(a)} = [N_{L|K}(a)].$$

(vi) Let $\mathfrak a_1$ be the ideal of K which is generated by all $N_{L|K}(a)$, with $a \in \mathfrak A$. If $\mathfrak A$ is a principal ideal (a), then $\mathfrak a_1 = (N_{L|K}(a)) = N_{L|K}(\mathfrak A)$, by (v). But the argument which yielded (v) applies equally well to the localizations $\mathcal O_{\mathfrak p}|\mathfrak o_{\mathfrak p}$ of the extension $\mathcal O|\mathfrak o$ of maximal orders of $L|K$. $\mathcal O_{\mathfrak p}$ has only a finite number of prime ideals, and is therefore a principal ideal domain (see chap. I, §3, exercise 4). We thus get

$$(\mathfrak a_1)_{\mathfrak p} = N_{L|K}((\mathfrak A)_{\mathfrak p}) = N_{L|K}(\mathfrak A)_{\mathfrak p}$$

for all prime ideals $\mathfrak p$ of $\mathfrak o$, and consequently $\mathfrak a_1 = N_{L|K}(\mathfrak A)$. □

Since the homomorphisms $i_{L|K}$ and $N_{L|K}$ map replete principal ideals to replete principal ideals, they induce homomorphisms of the replete Picard groups of K and L, and we obtain the

(1.7) Proposition. *For every finite extension $L|K$, the following two diagrams are commutative:*

$$\begin{array}{ccc} Pic(\bar{\mathcal O}_L) & \xrightarrow{\ \mathfrak N\ } & \mathbb R_+^* \\ {\scriptstyle i_{L|K}}\uparrow\ \downarrow{\scriptstyle N_{L|K}} & & {\scriptstyle [L:K]}\uparrow\ \downarrow{\scriptstyle id} \\ Pic(\bar{\mathcal O}_K) & \xrightarrow{\ \mathfrak N\ } & \mathbb R_+^* . \end{array}$$

Let us now translate the notions we have introduced into the function-theoretic language of divisors. In chap. I, § 12, we defined the divisor group $Div(\mathfrak o)$ to consist of all formal sums

$$D = \sum_{\mathfrak p} \nu_{\mathfrak p}\mathfrak p,$$

where $\nu_{\mathfrak p} \in \mathbb Z$, and $\nu_{\mathfrak p} = 0$ for almost all $\mathfrak p$. Contained in this group is the group $P(\mathfrak o)$ of principal divisors $\operatorname{div}(f) = \sum_{\mathfrak p} v_{\mathfrak p}(f)\mathfrak p$, which allowed us to define the divisor class group

$$CH^1(\mathfrak o) = Div(\mathfrak o)/P(\mathfrak o).$$

It follow5 from the main theorem of ideal theory, chap. I, (3.9), that this group is isomorphic to the ideal class group Cl_K, which i1- a finite group (see chap.I, (12.14)). We now extend the5c conceph as followi,.

(1.8) Definition. *A* **replete divisor** (or **Arakelov divisor**) of *K is :1 formal*

where $v_p \in \mathbb{Z}$ forp f oo, $v_p \in$ IR forploo, *and* $vp = 0$ fora/most a// p.

The replete diviwrs fonn a group, which is denoted by Dil·(O). It admits a decomposition

$$Div(8) � /Jiv(o) \times \bigoplus_{pix} \mathbb{R}.p.$$

On the right-hand �ide, the second factor is endowed with the canonical topology, the !1r1-t one with the di1-crete topology. On the product we have the product topology, which makes Dir(O) into a locally compact topological group.

We now study the canonical homomorphism

$$\text{div}: K^* \longrightarrow Div(O), \quad \text{div}(/) = \sum_p vp(f)p.$$

The clements of the fonn div(/) are called **replete principal divisors.**

Remark: The compo'>ite of the mapping div : $K^* \longrightarrow$ Dil'(O) with the mapping

$$Div(O) \longrightarrow \prod_{P|=} \mathbb{R}., \quad \sum_P vppi \longmapsto (vp/i,)pi,-x\_,,$$

is equal, up to 1-ign, to the logarithm map

$$i.,K' - [1IF<. \quad i.(/I�(\dots \text{loglflp--} \;). \atop pl�$$

of Minkowski theory (see chap. **I,** * 7, and chap. **Ill.** * 3, p. 211). chap. I. (7.3), it map" the unit group onto a complete lattice r = in trace-zero space $H = \{(.rp) \in nPi'.XJ\ \mathbb{R} \mid Lplcx, lp = 0\}$.

(1.9) Proposition. *The kernel* of div : $K^* \longrightarrow$ *!)iv(O)* i� *1he* group *μ,(K) o(mars* of *unity in K, and its* image P((J) *is* a *discrete suhgroup* of *!)iv(O).*

Proof: By the above remark, the composite of div with the map $\mathrm{Div}(\bar{\mathcal O}) \to \prod_{\mathfrak p|\infty}\mathbb R$, $\sum_{\mathfrak p}\nu_{\mathfrak p}\mathfrak p \mapsto (\nu_{\mathfrak p})_{\mathfrak p|\infty}$, yields, up to sign, the homomorphism $\lambda: K^* \to \prod_{\mathfrak p|\infty}\mathbb R$. By chap. I, (7.1), the latter fits into the exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal O^* \xrightarrow{\lambda} \Gamma \longrightarrow 0,$$

where Γ is a complete lattice in trace-zero space $H \subseteq \prod_{\mathfrak p|\infty}\mathbb R$. Therefore $\mu(K)$ is the kernel of div. Since Γ is a lattice, there exists a neighbourhood U of 0 in $\prod_{\mathfrak p|\infty}\mathbb R$ which contains no element of Γ except 0. Considering the isomorphism $\alpha : \prod_{\mathfrak p|\infty}\mathbb R \to \bigoplus_{\mathfrak p|\infty}\mathbb R\mathfrak p$, $(\nu_{\mathfrak p})_{\mathfrak p|\infty} \mapsto \sum_{\mathfrak p|\infty}\nu_{\mathfrak p}\mathfrak p$, the set $\{0\} \times \alpha U \subseteq J(\mathcal O) \times \bigoplus_{\mathfrak p|\infty}\mathbb R\mathfrak p = \mathrm{Div}(\bar{\mathcal O})$ is a neighbourhood of 0 in $\mathrm{Div}(\bar{\mathcal O})$ which contains no replete principal divisor except 0. This shows that $P(\bar{\mathcal O}) = \mathrm{div}(K^*)$ lies discretely in $\mathrm{Div}(\bar{\mathcal O})$. □

(1.10) Definition. The factor group

$$CH^1(\bar{\mathcal O}) = \mathrm{Div}(\bar{\mathcal O})/P(\bar{\mathcal O})$$

is called the replete divisor class group (or Arakelov class group) of K.

As $P(\bar{\mathcal O})$ is discrete in $\mathrm{Div}(\bar{\mathcal O})$, and is therefore in particular closed, $CH^1(\bar{\mathcal O})$ becomes a locally compact Hausdorff topological group with respect to the quotient topology. It is the correct analogue of the divisor class group of a function field (see chap. I, § 14). For the latter we introduced the degree map onto the group $\mathbb Z$; for $CH^1(\bar{\mathcal O})$ we obtain a degree map onto the group $\mathbb R$. It is induced by the continuous homomorphism

$$\deg : \mathrm{Div}(\bar{\mathcal O}) \longrightarrow \mathbb R$$

which sends a replete divisor $D = \sum_{\mathfrak p}\nu_{\mathfrak p}\mathfrak p$ to the real number

$$\deg(D) = \sum_{\mathfrak p}\nu_{\mathfrak p}\log\mathfrak N(\mathfrak p) = \log\Big(\prod_{\mathfrak p}\mathfrak N(\mathfrak p)^{\nu_{\mathfrak p}}\Big).$$

From the product formula (1.3), we find for any replete principal divisor $\mathrm{div}(f) \in P(\bar{\mathcal O})$ that

$$\deg(\mathrm{div}(f)) = \sum_{\mathfrak p}\log\mathfrak N(\mathfrak p)^{v_{\mathfrak p}(f)} = -\log\Big(\prod_{\mathfrak p}|f|_{\mathfrak p}\Big) = 0.$$

Thus we obtain a well-defined continuous homomorphism

$$\deg : CH^1(\bar{\mathcal O}) \longrightarrow \mathbb R.$$

The kernel $CH^1(\bar{\mathcal O})^0$ of this map is made up from the unit group and the ideal class group $Cl_K = CH^1(\mathcal O)$ of K as follows.

(1.11) Proposition. *Let $\Gamma =$ denote the complete lattice of units in trace-zero space $H = \{(x_{\mathfrak p}) \in \prod_{\mathfrak p \mid \infty} \mathbb{R} \mid \sum x_{\mathfrak p} = 0\}$. There is an exact sequence*

$$0 \longrightarrow H/\Gamma \longrightarrow CH^1(\bar{\mathcal{O}})^0 \longrightarrow CH^1(\mathcal{O}) \longrightarrow 0.$$

Proof: Let $Div(\bar{\mathcal{O}})^0$ be the kernel of deg: $Div(\bar{\mathcal{O}}) \to \mathbb{R}$. Consider the exact sequence

$$0 \longrightarrow \prod_{\mathfrak p \mid \infty} \mathbb{R} \xrightarrow{\alpha} Div(\bar{\mathcal{O}}) \longrightarrow Div(\mathcal{O}) \longrightarrow 0,$$

where $\alpha((v_{\mathfrak p})) = \sum_{\mathfrak p \mid \infty} v_{\mathfrak p}\,\mathfrak p$. Restricting to $Div(\bar{\mathcal{O}})^0$ yields the exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \lambda(\mathcal{O}^*) & \longrightarrow & P(\bar{\mathcal{O}}) & \longrightarrow & P(\mathcal{O}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & H & \longrightarrow & Div(\bar{\mathcal{O}})^0 & \longrightarrow & Div(\mathcal{O}) & \longrightarrow & 0.
\end{array}$$

Via the snake lemma (see [23], chap. III, §3, (3.3)), this gives rise to the exact sequence

$$0 \longrightarrow H/\lambda(\mathcal{O}^*) \longrightarrow CH^1(\bar{\mathcal{O}})^0 \longrightarrow CH^1(\mathcal{O}) \longrightarrow 0. \qquad \square$$

The two fundamental facts of algebraic number theory, the finiteness of the class number and Dirichlet's unit theorem, now merge into (and are in fact equivalent to) the simple statement that the kernel $CH^1(\bar{\mathcal{O}})^0$ of the degree map deg: $CH^1(\bar{\mathcal{O}}) \to \mathbb{R}$ is **compact.**

(1.12) Theorem. *The group $CH^1(\bar{\mathcal{O}})^0$ is compact.*

Proof: This follows immediately from the exact sequence

$$0 \longrightarrow H/\Gamma \longrightarrow CH^1(\bar{\mathcal{O}})^0 \longrightarrow CH^1(\mathcal{O}) \longrightarrow 0.$$

As Γ is a complete lattice in the $\mathbb{R}$-vector space H, the quotient H/Γ is a compact torus. In view of the finiteness of $CH^1(\mathcal{O})$, we obtain $CH^1(\bar{\mathcal{O}})^0$ as the union of the finitely many compact cosets of H/Γ in $CH^1(\bar{\mathcal{O}})^0$. Thus

$CH^1((""0)^0$ itself is compact. $\square$

The correspondence between replete ideals and replete divisors is given by the two mutually inverse mappings

$$\mathrm{div}: J(\bar{o}) \longrightarrow \mathrm{Div}(\bar{o}), \qquad \mathrm{div}\Big(\prod_{\mathfrak p} \mathfrak p^{\nu_{\mathfrak p}}\Big) = \sum_{\mathfrak p} -\nu_{\mathfrak p}\mathfrak p,$$
$$o: \mathrm{Div}(\bar{o}) \longrightarrow J(\bar{o}), \qquad \sum_{\mathfrak p} \nu_{\mathfrak p}\mathfrak p \longmapsto \prod_{\mathfrak p} \mathfrak p^{-\nu_{\mathfrak p}}.$$

These are *topological isomorphisms* once we equip

$$J(\bar{o}) = J(o) \times \prod_{\mathfrak p \mid \infty} \mathbb{R}_+^*$$

with the product topology of the discrete topology on $J(o)$ and the canonical topology on $\prod_{\mathfrak p\mid\infty} \mathbb{R}_+^*$. The image of a divisor $D = \sum_{\mathfrak p} \nu_{\mathfrak p}\mathfrak p$ is also written

$$o(D) = \prod_{\mathfrak p} \mathfrak p^{-\nu_{\mathfrak p}}.$$

The minus sign here is motivated by classical usage in function theory. Replete principal ideals correspond to replete principal divisors in such a way that $P(\bar{o})$ becomes a discrete subgroup of $J(\bar{o})$ by (1.9), and $Pic(\bar{o}) = J(\bar{o})/P(\bar{o})$ is a locally compact Hausdorff topological group. We obtain the following extension of chap. I, (12.14).

(1.13) Proposition. *The mapping* $\mathrm{div}: J(\bar{o}) \to \mathrm{Div}(\bar{o})$ *induces a topological isomorphism*

$$\mathrm{div}: Pic(\bar{o}) \xrightarrow{\sim} CH^1(\bar{o}).$$

On the group $J(\bar{o})$ we have the homomorphism $\mathfrak{N}: J(\bar{o}) \to \mathbb{R}_+^*$, and on the group $\mathrm{Div}(\bar{o})$ there is the degree map $\deg: \mathrm{Div}(\bar{o}) \to \mathbb{R}$. They are obviously related by the formula

$$\deg(\mathrm{div}(\mathfrak a)) = -\log \mathfrak{N}(\mathfrak a),$$

and we get a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Pic(\bar{o})^0 & \longrightarrow & Pic(\bar{o}) & \xrightarrow{\mathfrak N} & \mathbb{R}_+^* & \longrightarrow & 0 \\
 & & \downarrow\cong & & \mathrm{div}\downarrow\cong & & \log\downarrow\cong & & \\
0 & \longrightarrow & CH^1(\bar{o})^0 & \longrightarrow & CH^1(\bar{o}) & \xrightarrow{\deg} & \mathbb{R} & \longrightarrow & 0
\end{array}$$

with exact rows. (1.12) now yields the

(1.14) Corollary. *The group*
$$PHoJ° \{ |a| \in Pic(/0) \mid <Jl(a) \}$$
is compact.

The preceding isomorphism result (1.13) invites a philosophical reflection. Throughout the historical development of algebraic number theory, a controversy persisted between the followers of Dedekind's ideal-theoretic approach, and the divisor-theoretic method of building up the theory from the valuation-theoretic notion of prime. Both theories are equivalent in the sense of the above isomorphism result, but they are also fundamentally different in nature. The controversy has finally given way to the realization that neither approach is dominant, that each one instead emanates from its own proper world, and that the relation between these worlds is expressed by an important mathematical principle. However, all this becomes evident only in higher dimensional arithmetic algebraic geometry. There, on an algebraic Z-scheme X, one studies on the one hand the totality of all *vector bundles*, and on the other, that of all *irreducible subschemes*, of X. From the first, one constructs a series of groups $K_i(X)$ which constitute the subject of algebraic K-theory. From the second is constructed a series of groups $CH^i(X)$, the subject of Chow theory. Vector bundles are by definition locally free $\mathcal{O}_X$-modules. In the special case $X = \operatorname{Spec}(\mathcal{O})$ this includes the fractional ideals. The irreducible subschemes and their formal linear combinations, i.e., the cycles of X, are to be considered as generalizations of the primes and divisors. The isomorphism between divisor class group and ideal class group extends to the general setting as a homomorphic relation between the groups $CH^i(X)$ and $K_i(X)$. Thus the initial controversy has been resolved into a seminal mathematical theory (for further reading, see [13]).

Exercise 1 (Strong Approximation Theorem). Let S be a finite set of primes and let $\mathfrak{p}_0$ be another prime of K which does not belong to S. Let $\alpha_\mathfrak{p} \in K$ be given numbers, for $\mathfrak{p} \in S$. Then for every $\varepsilon > 0$, there exists an $x \in K$ such that
$$|x - \alpha_\mathfrak{p}|_\mathfrak{p} < \varepsilon \text{ for } \mathfrak{p} \in S, \text{ and } |x|_\mathfrak{p} \le 1 \text{ for } \mathfrak{p} \notin S \cup \{\mathfrak{p}_0\}.$$

Exercise 2. Let K be totally real, i.e., $K_\mathfrak{p} = \mathbb{R}$ for all $\mathfrak{p} | \infty$. Let T be a proper nonempty subset of $\operatorname{Hom}(K, \mathbb{R})$. Then there exists a unit ε of K satisfying $\tau\varepsilon > 1$ for $\tau \in T$ and $0 < \tau\varepsilon < 1$ for $\tau \notin T$.

Exercise 3. Show that the absolute norm $\mathfrak{N}: Pic(\bar{\mathbb{Z}}) \to \mathbb{R}_+^*$ is an isomorphism.

Exercise 4. Let K and L be number fields, and let $\sigma: K \to L$ be a homomorphism. Given any replete divisor $D = \prod_\mathfrak{P} \mathfrak{P}^{\nu_\mathfrak{P}}$ of L, define a replete divisor of K by the rule
$$\sigma_* D = \prod_\mathfrak{p} \mathfrak{p}^{\sum_{\mathfrak{P}|\mathfrak{p}} \nu_\mathfrak{P} f_\mathfrak{P}},$$

where i� the inertia degree of ,P over r K and 'PIP �igni!ie� rp = 'Pl,x. Show that r, a homomorphism

r,: CH¹((7₁) -------,. $CH^1(i"!;,.)$_.

Exercise 5. Given any replete div1�or D = LP $V\mu P$ of K. define a replete div1�or of L hy the rule

r�{DJ =LL Vµ<"-!Jip'P,
P 'VP

\\-here e,:p,p denote� the ram1ticat1on mdex of ,P over K. Show that r* induce� a homomorphi�m

r*: CH¹(i"lx:)------,.CH¹(tJL).

Exercise 6. Show that •r = IL : KI and that

deg(r,D) =deg(D). deg(r*D) = [L: Kldcg(D).

§ 2. **Different and Discriminant**

It is our intention to develop a framework for the theory of algebraic number fields which shows the complete analogy with the theory of function fields. This goal leads us naturally to the notions of different and discriminant, a� we shall explain in § 3 and § 7. They control the ramification behaviour of an extension of valued fields.

Let LI K be a finite separable field extension, CJ � K a Dedekind domain with field of fractions K, and let O � L be iti,, integral closure in L. Throughout this section we assume syi,,tematically that the residue field extensions AIK of Ola arc separable. The theory of the different originates from the fact that we arc given a canonical nondegenerate symmetric bilinear fonn on the K-vector space L, 1·iz., the trace form

$$T(.t,y) = Tr(.ty)$$

(see chap. I, § 2). It allows us to associate to every fractional ideal Ql of L the **dual** CJ-module

'2(� / x E L / $Tc(x$ 'll) <;; v).

It is again a fractional ideal. For if a₁. .a_{11} E CJ is a basis of LIK and d = det(Tr(a₁a₁)) it� discriminant, then ad*21. � CJ for every nonzero a E Qln o. Indeed, if x = x₁a₁+- - - +$x_{11}a$,, E *21., with \; E K, then the $a_{,1}$ satisfy the system of linear equations $L7=_1 aJ.$, $Tr(a,aJ) = Tr(,\cdot ua_1)$ E CJ. This implies dax; E o and thus dax E 0.

The notion of duality is justified by the isomorphism

�Q(--=:.... Hom₀(Qt, o), ti-------+ (y 1-+ Tr(xy)).

Indeed. �ince o-homomorphi,;m /" : Q(---+ o extends uniquely to a K -homomorphism : L ---+ K in view of $Q(K = L$, we may consider Hom,?(Qt, CJ) as a submodule of HomK (/., K), namely, the image of *Q(with re�pcct to L ---+ HomK (L, K), x 1-+ (y 1-+ Tr(xy)). The module dual to CJ,

$$^*\mathcal{O} \cong \mathrm{Hom}_{o}(\mathcal{O}, o)$$

will obviously occupy a distingui�hcd place in thi� theory.

(2.1) Definition. *The fractional ideal*

�010 � 'O � / x E L | Tc(xOJ c; o)

i.� *called* **Dedekind's complementary module,** or *the* inverse **different.** *Its* inverse,

$$\mathfrak{D}_{\mathcal{O}|o} = \mathfrak{C}_{\mathcal{O}|o}^{-1}$$

i� called /he **different** of Ola.

As ittllo 2 O. theideal :Tiq0 S; CJ is actually an integral ideal of L. We will frequently denote it by *l) 1* iK. provided the intended �ubring� a, CJ arc evident from the context. In the �ame way, we write *i[LiK* imtcad of ito10. The different behaves in the following manner under change of rings o and 0.

(2.2) **Proposition.**

(i) *For a* tower of *field.�* K S; L S; M, *one* ha� *'.DMIK = '.DM1L'.DL1K.*

(ii) *For any multiplicative* subset *S* of *o*, *one has* :TI5-101S-10 = S-1'.Do10-

(iii) Ifq]lp arc *prime ideals* of CJ. resp. *o.* and 0,:µlo� are *the* a.�sociated *completiom, 1hen*

$$\mathfrak{D}_{\mathcal{O}|o}\mathcal{O}_{\mathfrak{P}} = \mathfrak{D}_{\mathcal{O}_{\mathfrak{P}}|o_{\mathfrak{p}}}.$$

Proof: (i) Let $A = o$ S; K, and let B S; L, C S; M be the imcgral clo�urc of o in L, resp. M. It then suffices to show that

$$\mathfrak{C}_{C|A} = \mathfrak{C}_{C|B}\mathfrak{C}_{B|A}.$$

The inclmion 2 follows from

Trtw K(l£ciRitR1AC) = TrLIK TrM1d(fc:RitR1AC)

= TrL K(if RIA TrM1dltc1BC)) <;A.

In view of *BC = C,* the inclusion<; is derived as follows:

TrMIK (lfciAC) = *TrL1K* (*B TrM1dltc* AC)) <; *A,*

so that TrM1ditc14C) <; *([RIA,* and thus

TrM t (itf:1:Ae:CiAC) = *itB:A TrM11.(l!ci,1C)* £;; *B.*

This does indeed imply *Q.'fl¹A![CiA* £;; l!c1H, and so itc1A £;; *Q.'ciH<l'RIA·*

(ii) i� trivial.

(iii) By (ii) we assume that *o* b a discrete valuation ring. We show that l!o1,_�is dense in In order to do thi,;. we use the fonnula

$$TrLIK = L\ TrL,vlKp$$

'+llP

(5ee chap. II, (8.4)), Let *x* E it010 and *y* E CJ,,p. The approximation theorem allows u� to tin<l an *T/* in *L* which is dose to _v with respect to *v13,* and clo�e to O with respect to *V'-J.l',* for !,p'lp. !,p'-=/= !,p. The left-hand side of the equation

TrL1K(XT}) = Trl.'VlKp(XT}) +,+l;"'J,..1TrL,vlKp(xr1)

then belongs to $\mathcal{O}_\mathfrak{p}$ since *Tr1.₁K(n1)* E *o* <; Op, hut the same is true of the elements hecau�e they arc close to zero with re�pect to *Vp.* Therefore $Tr_{L_\mathfrak{P}|K_\mathfrak{p}}($ E Op. Thb show5 that ito10 £;; 1:!:o.i,,'")"•

If on the other hand *x* E ([O-+,io", and if� E *L* is sufticienlly close to *x* with respect to and sufficiently close to O with re-;pcct to 1!•:p'. for l,p'-=/= l,p, then� E In fact. if *y* E C'J, then *TrL,vlKp(�y)* E Op, since $Tr_{L_\mathfrak{P}|K_\mathfrak{p}}(xy) \in \mathcal{O}_\mathfrak{p}$. Likewise $Tr_{L_{\mathfrak{P}'}|K_\mathfrak{p}}(\xi y)$ E Op for !,p'l!,p, because these elements are close to 0. Therefore $Tr_{L|K}(\xi y) \in \mathcal{O}_\mathfrak{p}$ n *K = o.* i.e.. S E . This shows that $\mathfrak{C}_{\mathcal{O}|o}$ is dense in $\mathfrak{C}_{\mathcal{O}_\mathfrak{P}|o_\mathfrak{p}}$, in other word8. $= \mathfrak{C}_{\mathcal{O}_\mathfrak{P}|o_\mathfrak{p}}$, and so $\mathfrak{D}_{\mathcal{O}|o}\mathcal{O}_\mathfrak{P} = \mathfrak{D}_{\mathcal{O}_\mathfrak{P}|o_\mathfrak{p}}$. □

If we put :1J = and :1J,:µ = '.DL,plKp, and consider '.D<:p at the same time as an ideal of CJ as the ideal CJ n ::U,,p), then (2.2), (iii) gives us the

(2.3) Corollary. '.D = fl₁₃'.D;;p.

The name "'different" is explained by the following explicit description, which wa� Dedekind's original way to define it. Let a E O and let $f(X)$ E v[XJ be the minimal polynomial of a. We define the **different of the element** a by

$$Or.ida) = \begin{cases} J'(a) & \text{if } L \text{ � } K(a), \\ 0 & \text{if } L \; i\text{-} \; K(a). \end{cases}$$

In the �pecial case where $O =$ o[al we then obtain:

(2.4) Proposition. *IfO* $=$ ofal, *then the different is the* principal ideal

$$T!L\ K \text{ � } (8L1da))$$

Proof: Let $f(X) = ao + a_1 X + \cdots + a_{11}X''$ be the minimal polynomial of a **and**

$$\frac{f(X)}{X-\alpha} = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1}$$

The **dual** ba'>i� of I, *r.x, ... , a''* [1] with respect to *Tr(xy)* is then given by

$$\frac{ho}{f'(a)'}\cdot \qquad \frac{h11\text{--}1}{f'(a)}$$

For if $a_1, \ldots, a_{11}$ are the roots *off*, then one has

$$\sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\,\frac{\alpha_i^r}{f'(\alpha_i)} = X^r, \qquad 0 \le r \le n-1,$$

as the difference of the two sides is a polynomial of degree ::: n - I with roots a_1. . *an*, rn is identically zero. We may write this equation **in** the **fonn**

$$\text{'fr[l.<!l.-"'-]�x'} \quad \frac{}{X\text{-}a} \quad \frac{}{f'(a)}$$

Considering now the coefficient of each of the power5 of X. we obtain

$$T,\cdot(a^{l}\_/''(\cdot a^{!}\_)J\_)\text{�}8_{,,}$$

and the claim follows.

As $O = o + oa + \cdots + oa^{11}\text{-}1$, we get

$$\text{C!:010} = f'(a)^{-1}(oho+ \quad +nhn\text{-}d\text{-}$$

Fmm the recursive fonnulas

$$b_{n-1} = 1,$$
$$b_{n-2} - \alpha b_{n-1} = a_{n-1},$$

it follows that

$$b_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \cdots + a_{n-i+1},$$

so that $\mathcal{O}b_0 + \cdots + \mathcal{O}b_{n-1} = \mathcal{O}[\alpha] = \mathcal{O}$; then $\mathcal{O}' = f'(\alpha)^{-1}\mathcal{O}$, and thus $\mathfrak{D}_{L|K} = (f'(\alpha))$. □

The proof shows that the module $\mathcal{O}[\alpha]^* = \{x \in L \mid Tr_{L|K}(x\mathcal{O}[\alpha]) \subseteq \mathfrak{o}\}$, which is the dual of the $\mathfrak{o}$-module $\mathcal{O}[\alpha]$, always admits the $\mathfrak{o}$-basis $\alpha^i/f'(\alpha)$, $i = 0, \dots, n-1$. We exploit this for the following characterization of the different in the general case where $\mathcal{O}$ need not be monogenous.

(2.5) **Theorem.** *The different $\mathfrak{D}_{L|K}$ is the ideal generated by all differents of elements $\delta_{L|K}(\alpha)$ for $\alpha \in \mathcal{O}$.*

Proof: Let $\alpha \in \mathcal{O}$ such that $L = K(\alpha)$, and let $f(X)$ be the minimal polynomial of α. In order to show that $f'(\alpha) \in \mathfrak{D}_{L|K}$ we consider the "conductor" $\mathfrak{f} = \{x \in L \mid x\mathcal{O} \subseteq \mathcal{O}[\alpha]\}$ of $\mathcal{O}[\alpha]$ (see chap. I, § 12, p. 79). On putting $b = f'(\alpha)$, we have for $x \in L$:

$$\begin{aligned} x \in \mathfrak{f} &\iff x\mathcal{O} \subseteq \mathcal{O}[\alpha] \iff b^{-1}x\mathcal{O} \subseteq b^{-1}\mathcal{O}[\alpha] = \mathcal{O}[\alpha]^* \\ &\iff Tr(b^{-1}x\mathcal{O}) \subseteq \mathfrak{o} \iff b^{-1}x \in \mathfrak{D}_{L|K}^{-1} \iff x \in b\,\mathfrak{D}_{L|K}^{-1}. \end{aligned}$$

Therefore $(f'(\alpha)) = \mathfrak{f}\,\mathfrak{D}_{L|K}$, so in particular $f'(\alpha) \in \mathfrak{D}_{L|K}$.

$\mathfrak{D}_{L|K}$ thus divides all the differents of elements $\delta_{L|K}(\alpha)$. In order to prove that $\mathfrak{D}_{L|K}$ is in fact the greatest common divisor of all $\delta_{L|K}(\alpha)$, it suffices to show that, for every prime ideal $\mathfrak{P}$, there exists an $\alpha \in \mathcal{O}$ such that $L = K(\alpha)$ and $v_{\mathfrak{P}}(\mathfrak{D}_{L|K}) = v_{\mathfrak{P}}(f'(\alpha))$.

We think of L as embedded into the separable closure $\bar{K}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$ in such a way that the absolute value $|\ |$ of $\bar{K}_{\mathfrak{p}}$ defines the prime $\mathfrak{P}$.

By chap. II, (10.4), we find an element β in the valuation ring $\mathcal{O}_{\mathfrak{P}}$ of the completion $L_{\mathfrak{P}}$ satisfying $\mathcal{O}_{\mathfrak{P}} = \mathfrak{o}_{\mathfrak{p}}[\beta]$, and the proof *loc. cit.* shows that, for every element $\alpha \in \mathcal{O}_{\mathfrak{P}}$ which is sufficiently close to β, one also has $\mathcal{O}_{\mathfrak{P}} = \mathfrak{o}_{\mathfrak{p}}[\alpha]$. From (2.2), (iii) and (2.4), it follows that

$$v_{\mathfrak{P}}(\mathfrak{D}_{L|K}) = v_{\mathfrak{P}}(\mathfrak{D}_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}) = v_{\mathfrak{P}}(\delta_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(\alpha)).$$

It therefore suffices to show that we can find an element α in $\mathcal{O}$ such that $L = K(\alpha)$ and

$$v_{\mathfrak{P}}(\delta_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(\alpha)) = v_{\mathfrak{P}}(\delta_{L|K}(\alpha)).$$

For this, let $\tau_2, \dots, \tau_r : L \to \bar{K}_{\mathfrak{p}}$ be K-embeddings giving the primes $\mathfrak{P}_2, \dots, \mathfrak{P}_r$ different from $\mathfrak{P}$. Let $\alpha \in \mathcal{O}_{\mathfrak{P}}$ be an element such that

(*) $\qquad |\sigma\tau_i\alpha - \alpha| = 1 \quad \text{for all} \quad \sigma \in G_{\mathfrak{p}} = G(\bar{K}_{\mathfrak{p}}|K_{\mathfrak{p}}).$

(Choose $a = 1$, rc&p. $a = 0$, according a5 the residue classe5 rfJ mod 13 which arc conjugate over tJp/P arc zero or not.) Using the Chinese remainder theorem, we now pick an a E O rnch that la-,81 and la_1a-al, for $i = 2, \dots, r$, are very small. We may even assume that $L = K$(a) (if not, modify $bya+n''y$, n E p,forv big, y E 0, L = K(y); forsuitable tJ-=/=- JL, one then finds $K(a +nvy) = K(a +n^1 'y) = K(y))$. Since a is close to ,8, we have O'l-l = Op[a]. Now

$$SL,i,!Kr(a) = \mathrm{TT}_{,;t} (a - \mathrm{ra}),$$

where r rum through the Kp-embeddings $L'l$-l ----+ KP different from I. Furthcnnorc,

$$8Lw(a)= TT_{ac;icl}(a-aa)= \mathrm{nca\text{-}ra})_{r,tcl}\mathrm{Ilnca\text{-}r1JrT10'})_{1=1\ J},$$

where a runs over the K -embeddings different from l, and the r_{11} arc certain elements in Gp· But now

$$\mathrm{la} - \mathrm{r1_1rr,al} = \mathrm{lr,}\text{�}^1\mathrm{a} - \mathrm{a1al} = \mathrm{lr,}\text{�}^1\mathrm{a} - a + a - a,al = 1,$$

since la - a,al is very �mall, and r,�^{1}a i� very clo�c to $^1/J$ (see (*)). Therefore $v,ii(tiLIK$ (a))= v'lJ(TT,$_{11}$(a - ra)) = asrequired.

□

The different characterize� the ramification behaviour of the extension LjK as follows.

(2.6) Theorem. *A prime ideal* 13 of *L i.�* ramified *over K if* and *only if* 'lll'.lJ1.1K-

Let 13·' *be the maximal power* of 13 *dividing '.DLIK,* and *lei e* be *the mmification index* of13 *over K. Then one has*

$$s = e - 1, \qquad \text{if13 } \textit{is tamely} \text{ ramified},$$

$$e \ \_::: s \ \_::: e - 1 + v,:\mu(e), \qquad \text{if13 } \textit{is wildly ramified.}$$

Proof: By (2.2), (iii), we may assume that o is a complete discrete valuation ring with maximal ideal p. Then, by chap. II, (10.4). we have O = tJ[al for a suitable a E 0. Let $f(X)$ be the minimal polynomial of a. (2.4) say5 that $s = v,,\mu(l'(a))$. As�ume LIK i� unramilied. Then $fi = a$ mod 13 i5 a simple *tero* of $f(X) = f(X)$ mod p, 50 that $J'(a)$ E 0^* and thus $s = 0 = e$ - I.

By (2.2), (i) and chap. II, (7.5), we may now pass to the maximal unramified extension and assume that $L|K$ is totally ramified. Then α may be chosen to be a prime element of $\mathcal{O}$. In this case the minimal polynomial

$$f(X) = a_0X^e + a_1X^{e-1} + \cdots + a_e, \qquad a_0 = 1, \text{ is}$$

an Eisenstein polynomial. Let us look at the derivative

$$f'(\alpha) = e\alpha^{e-1} + (e-1)a_1\alpha^{e-2} + \cdots + a_{e-1}.$$

For $i = 0, \ldots, e-1$, we find

$$v_{\mathfrak{P}}((e-i)a_i\alpha^{e-i-1}) = ev_{\mathfrak{p}}(e-i) + ev_{\mathfrak{p}}(a_i) + e - i - 1 \equiv -i - 1 \bmod e,$$

so that the individual terms of $f'(\alpha)$ have distinct valuations. Therefore

$$s = v_{\mathfrak{P}}(f'(\alpha)) = \min_i \{v_{\mathfrak{P}}((e-i)a_i\alpha^{e-i-1})\}.$$

If now $L|K$ is tamely ramified, i.e., if $v_{\mathfrak{p}}(e) = 0$, then the minimum is obviously equal to $e-1$, and for $v_{\mathfrak{p}}(e) \geq 1$, we deduce that $e \leq s \leq v_{\mathfrak{P}}(e) + e - 1$. □

The geometric significance of the different, and thus also the way it fits into higher dimensional algebraic geometry, is brought out by the following characterization, which is due to *E. KÄHLER*. For an arbitrary extension $B|A$ of commutative rings, consider the homomorphism

$$\mu : B \otimes_A B \longrightarrow B, \qquad x \otimes y \longmapsto xy,$$

whose kernel we denote by I. Then

$$\Omega_{B|A} := I/I^2 = I \otimes_{B \otimes B} B$$

is a $B \otimes B$-module, and hence in particular also a B-module, via the embedding $B \to B \otimes B$, $b \mapsto b \otimes 1$. It is called the **module of differentials** of $B|A$, and its elements are called **Kähler differentials.** If we put

$$dx = x \otimes 1 - 1 \otimes x \mod I^2,$$

then we obtain a mapping

$$d : B \longrightarrow \Omega^1_{B|A}$$

satisfying

$$d(xy) = xdy + ydx,$$

$$da = 0 \quad \text{for} \quad a \in A.$$

Such a map is called a **derivation** of $B|A$. One can show that d is universal among all derivations of $B|A$ with values in B-modules. $\Omega_{B|A}$ consists of the linear combinations $\sum y_i dx_i$. The link with the different is now this.

(2.7) **Proposition.** *The different* :Dc,10 is *the* **annihilator** of *the 0-* module S22J10, i.e.,

$$:Do1o=\{xEO[\ r:dy=0\ \ forall\ \ yEO).$$

Proof: For grealer notational clarity, let m, put $O = B$ and $a = A$. If A' is any commutative A-algebra and $B' = B$ @.4. A'. then it is easy to 5Ce that £?k,1A.' = £?k1,1 ®,1 A'. Thu5 the module of differentials is preserved under localization and completion, and we may therefore assume that A is a complete discrete valuation ring. Then we find by chap. II, (10.4), that B = A[xJ. and if /(X) E A[Xl i& the minimal polynomial of x, then *QRIA* is generated by *dx* (exercise 3). The annihilator of *d.i* j5 f'(x). On the other hand, by (2.4) we have *:DBIA* = (f'(x)). Thi� provc5 the claim. D

A mosl intimate connection holds between the different and the discriminant of CJ lo. The latter is defined as follows.

(2.8) **Definition.** *The* **discriminant** r:i010 i.� *the* ideal of *o which* is *generated by the* discriminants d(a1, , a,,) of *all /he* bases a1, ...*a11 ofL* IK *which are contained in 0.*

We will frequently write *IILIK* instead of lla10. If 0'1, , *an* i� an integral basis of Olo, then r:i, IK is the principal ideal generated by d(a1, .. , *an)= dLIK.* because all olher bases contained in Oare tran&fonn� of the given one by matrices with entries in n. The discriminant **i�** obtained rrom the different by taking the noon N, iK (see S 1).

(2,9) **Theorem.** *The following* relation *exi�b* between the discriminanl *and the* different:

$$\mathfrak{d}_{L|K} = N_{L|K}(\mathfrak{D}_{L|K}).$$

Proof: If S is a multiplicative sub5et of o, then clearly r:i.� S-1r:io10 and :Ds-iois 10 = S-1:Dc,10. We may therefore as�ume o is a discrete valuation ring. Then. since o is a principal ideal domain, so is() (see chap. I, §3, exercise 4). and it admil� an integral basis a1. . , *a,,* (see chap. I, (2.10)). So we have *IIL1K* = (d(a1, ,a11)). Dedekind's complementary module ...., *a11* which i1> characterized by is a principal ideal (/3) and admits the ... , *f3an* of discriminant

$$d(f3a1,\ ..\ ,f3a11) = N1.1K(/3)^2 d(a1, ...\ ,a11).$$

But $(N, 1;dfi)) = $ N1.1d!!o10) $=$ $=$ NL1d'.DL1K>-^{1}, and $(d(a_1, \ldots\ldots\ldots\ldots an)) = DLIK\cdot$ One ha� $d(a_1..$ = dct((a₁aJ))2.
$d(a;.$ .a;,)= for a, E HomK(L.K), and $Tr(a,a;) = 0_{11}$.
Then $d(a_1. \ldots an)$ ... ,c<i) = I. Combining these yields

$$DL^1{}_K = (d(a1, \ldots\ an)\text{-}^1) = (d(a^1{}_1, \ldots .,a;,)) = (d(/fo:1, \quad .fia11))$$
$$= {}^2_{N}L1K<'.DL1K)\text{-}\ i)LIK$$

and hence $NLw('JJL1K) = i)LIK$• LJ

(2.10) Corollary. *For* a tower of fields K S; L � M, one *has*

$$DM1K = \text{D��}^1_{/}\ \text{NL1K(ll,H1d-}$$

Proof: Applying to *'.DMIK = '.DM1L'.DLIK* the norm *N11J1K = Nrw* c *N,1111,* (1.6) give�

$$DMIK = NL\ K\ (\text{llM1dNL1K('JJ�:�/}^1) = N1\ \text{w(iJM1tJD�}^1/^{\text{I}}. \qquad \square$$

Putting i) $= D_{t.,K}$ and D,p = and viewing O;p al5o a� the ideal ll<p n o of K, the product formula for the different, together with theorem (2.9), yields:

(2.11) Corollary. D = TI,:p i.'l'll.

The cxtcn5ion LI K is called **unramified** if all prime ideals p of K arc unramitied. This amounts to requiring that all primes of K be unramilled. In fact, the infinite primes are always to be regarded a� unramified because "'lJI p = I.

(2.12) Corollary. *A prime ideal* p of K *is* rnmitied *in L* if;.md *only* ifplD. *In particular,* the *extension* LI K i., *unramified* if *the di:.criminant* $D =$ (I).

Combining this result ½ith Minkowski theory lead� to two important theorems on unramitied extensions of number llcld, which belong to the classical body of algebraic number theory. The first of the:,e results is the following.

(2.13) **Theorem.** Let *K* be *an algebraic number field* and *Jct S be* a *linilc set* of primes of *K. Then there exist only finitely many* extensions LI *K* of *given degree n which* are *unramified* outside of *S.*

Proof: If /,IK is an cxtcn5ion of degree *n* which is unramificd outside of *S,* then, by (2.12) and (2.6). it5 di5criminant *i:ILIK* is one of the finite number of divisors of the ideal n = n p<ccS" pn{l+nl. It therefore suffices to show Pt=

that there arc only finitely many extension:,, LI *K* of degree *n* with discriminant. We may assume without loss of generality that *K* = For if LI *K* is an extension of degree *n* with discriminant i:!, then *L* IIQ is an extension of degree *m* = nfK: Ql] with discriminant (d) = i:!'.;;1QNKl\l'(i:l). Finally. the discriminant of *L(* J=T)IQ differs from the discriminant of LIQ only by a con5tant factor. So we are reduced to proving that there exist only finitely many fields *K* IQ of degree *n* containing *R* with a given discriminant *d.* Such a field *K* has only complex embeddings *T* : *K* ---- + Choose one of them: To. In the Minkowski space

$$K_{\mathbb{R}} = \left[\prod_{\tau} \mathbb{C}\right]^{+}$$

(5ee chap. I, §5) consider the convex, centrally symmetric subset

***X* �{(,,)EK:, | llm(,,,,JI < c/jdj.**

1Re(zr₀)1 < I, lzrl < 1 for *T-=/-* ToJo).

where *C* is an arbitrarily big constant which depends only on *11.* For a convenient choice of *C,* the volume will satisfy

vol(X) > *2¹¹*JTJT = *2n* vol(oK),

where vol(oK) is the volume of a fundamental mesh of the lattice in *Ket* - sec chap. I, (5.2). By Minkow:,,ki':,, lattice poinl theorem I. (4.4)), we thw, find *a* E *OK,* *a-=/-* 0, �uch that *ja* = (ra) E *X,* that is,

(*) I lm(roa)I < *C*$\sqrt{}$*IJT,* I Re(roall < I. lral < I for *r -1-* To, *To.*

This *a* i� a primitive element of *K,* i.e., one has *K* = Q(a). Indeed, INK1v,(a)I = nr 1ml?. I implies IToal > I; thus Im(Toa) *-=I-()* so that the conjugates *Toa* and *T0a* of *a* have to he distinct. Since *ITai* < I for *T -=I-* To. T0, one has *Toa -=I- Ta* for all *T -=I-* To. This implies *K* = Q(a), because if Ql(a) � *K* then the restriction Tok�wl would admit an extension *T* different from To, contradicting *Toa -=I- Ta.*

Since the conjugate:,, *Ta* of *a* are subject lo the condiliom (*), which only depend on *d* and *n.* the cocfficicnh of the minimal polynomial of *a* are bounded once d and n are fixed. Thus every field $K|\mathbb{Q}$ of degree n with discriminant d is generated by one of the finitely many lattice points a in the bounded region X. Therefore there are only finitely many fields with given degree and discriminant. $\square$

The second theorem alluded to above is in fact a strengthening of the first. It follows from the following *bound on the discriminant*.

(2.14) Proposition. *The discriminant of an algebraic number field K of degree n satisfies*

$$|d_K|^{1/2} \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

Proof: In Minkowski space $K_{\mathbb{R}} = [\prod_\tau \mathbb{C}]^+$, $\tau \in \mathrm{Hom}(K,\mathbb{C})$, consider the convex, centrally symmetric subset

$$X_t = \{(z_\tau) \in K_{\mathbb{R}} \mid \sum_\tau |z_\tau| < t\}.$$

Its volume is

$$\mathrm{vol}(X_t) = 2^r\pi^s\frac{t^n}{n!}.$$

Leaving aside the proof of this formula for the moment (which incidentally was exercise 2 of chap. I, §5), we deduce the proposition from Minkowski's lattice point theorem (chap. I, (4.4)) as follows. Consider in $K_{\mathbb{R}}$ the lattice $\Gamma = j\mathcal{O}$ defined by $\mathcal{O}$. By chap. I, (5.2), the volume of a fundamental mesh is $\mathrm{vol}(\Gamma) = \sqrt{|d_K|}$. The inequality

$$\mathrm{vol}(X_t) > 2^n\,\mathrm{vol}(\Gamma)$$

therefore holds if and only if $2^r\pi^s\frac{t^n}{n!} > 2^n\sqrt{|d_K|}$, or equivalently if

$$t^n = n!\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|} + \varepsilon,$$

for some $\varepsilon > 0$. If this is the case, there exists an $a \in \mathcal{O}$, $a \neq 0$, such that $ja \in X_t$. As this holds for all $\varepsilon > 0$, and since X_t contains only finitely many lattice points, it continues to hold for $\varepsilon = 0$. Applying now the inequality between arithmetic and geometric means,

$$\frac{1}{n}\sum_\tau |\tau a| \ge \Big(\prod_\tau |\tau a|\Big)^{1/n},$$

we obtain the desired result:

$$1 \le |N_{K|\mathbb{Q}}(a)| = \prod_\tau |\tau a| \le \frac{1}{n^n}\Big(\sum_\tau |\tau a|\Big)^n < \frac{t^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}$$

$$\le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{n/2}\sqrt{|d_K|}.$$

Given this, it remains to prove the following lemma. $\square$

(2.15) Lemma. *In Minkowski space $K_{\mathbb{R}} = \left[\prod_\tau \mathbb{C}\right]^+$, the domain*

$$X_t = \Big\{(z_\tau) \in K_{\mathbb{R}} \;\Big|\; \sum_\tau |z_\tau| < t\Big\}$$

has volume

$$\mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}.$$

Proof: $\mathrm{vol}(X_t)$ is 2^s times the Lebesgue volume $\mathrm{vol}(f(X_t))$ of the image $f(X_t)$ under the mapping chap. I, (5.1),

$$f : K_{\mathbb{R}} \to \mathbb{R}^n, \quad (z_\tau) \mapsto (x_\tau),$$

where $x_\rho = z_\rho$, $x_\sigma = \mathrm{Re}(z_\sigma)$, $x_{\bar\sigma} = \mathrm{Im}(z_\sigma)$. Substituting x_i, $i = 1, \dots, r$, instead of x_ρ, and y_j, z_j, $j = 1, \dots, s$, instead of $x_\sigma, x_{\bar\sigma}$, we see that $f(X_t)$ is described by the inequality

$$|x_1| + \cdots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \cdots + 2\sqrt{y_s^2 + z_s^2} < t.$$

The factor 2 occurs because $|z_\sigma| = |z_{\bar\sigma}| = \sqrt{x_\sigma^2 + x_{\bar\sigma}^2}$. Passing to polar coordinates $y_j = u_j \cos\theta_j$, $z_j = u_j \sin\theta_j$, where $0 \le \theta_j \le 2\pi$, $0 \le u_j$, one sees that $\mathrm{vol}(f(X_t))$ is computed by the integral

$$V(t) = \int u_1 \cdots u_s \, dx_1 \cdots dx_r \, du_1 \cdots du_s \, d\theta_1 \cdots d\theta_s,$$

extended over the domain

$$|x_1| + \cdots + |x_r| + 2u_1 + \cdots + 2u_s \le t.$$

Restricting this domain of integration to $x_i \ge 0$, the integral gets divided by 2^r. Substituting $2u_j = w_j$ gives

$$V(t) = 2^r 4^{-s} (2\pi)^s W_{r,s}(t),$$

where the integral

$$W_{r,s}(t) = \int w_1 \cdots w_s \, dx_1 \cdots dx_r \, dw_1 \cdots dw_s,$$

has to be taken over the domain $x_i \ge 0$, $w_j \ge 0$ and

$$x_1 + \cdots + x_r + w_1 + \cdots + w_s < t. \quad (*)$$

Clearly $W_{r,s}(t) = t^{r+2s} W_{r,s}(1) = t^n W_{r,s}(1)$. Writing $x_2 + \cdots + x_r + w_1 + \cdots + w_s \le 1 - x_1$ instead of $(*)$, Fubini's theorem yields

$$W_{r,s}(1) = \int_0^1 W_{r-1,s}(1 - x_1)\, dx_1 = \int_0^1 (1 - x_1)^{n-1} dx_1 \, W_{r-1,s}(1)$$
$$= \frac{1}{n} W_{r-1,s}(1).$$

By induction, this implies that

$$I_{r,s}(1) = \frac{1}{n(n-1)\cdots(n-r+1)} I_{0,s}(1).$$

In the same way, one gets

$$I_{0,s}(1) = \int_0^1 w_1(1-w_1)^{2s-2}\,dw_1\, I_{0,s-1}(1),$$

and, doing the integration, induction shows that

$$I_{0,s}(1) = \frac{1}{(2s)!}\,.$$

Together, this gives $I_{r,s}(1) = \frac{1}{n!}$ and therefore indeed

$$\operatorname{vol}(X_t) = 2^s \operatorname{Vol}\big(f(X_t)\big) = 2^s 2^r 4^{-s} (2\pi)^s t^n I_{r,s}(1) = \frac{2^r \pi^s}{n!} t^n. \qquad \square$$

If we combine Stirling's formula,

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, \quad 0 < \theta < 1,$$

with the inequality (2.14), we obtain the inequality

$$|d_K| > \left(\frac{\pi}{4}\right)^{2s} \frac{1}{2\pi n} e^{2n - \frac{1}{6n}}.$$

This shows that the absolute value of the discriminant of an algebraic number field tends to infinity with the degree. In the proof of (2.13) we saw that there are only finitely many number fields with bounded degree and discriminant. So now, since the degree is bounded if the discriminant is, we may strengthen (2.13), obtaining

(2.16) Hermite's Theorem. There exist *only finitely many* number *fields with* bounded *discriminant.*

The expression $a_n =$ satisfies

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2}\left(1 + \frac{1}{n}\right)^n > 1,$$

i.e., $a_{n+1} > a_n$. Since $a_2 = \frac{\pi}{2} > 1$, (2.14) yields

(2.17) Minkowski's Theorem. *The* discriminant of a number *field K different* from $\mathbb{Q}$ *is* $\neq \pm 1$.

Combining this result with corollary (2.12), we obtain the

(2.18) Theorem. *The field* $\mathbb{Q}$ *does not admit any* unramified extensions.

These last theorems are of fundamental importance for number theory. Their significance is seen especially clearly in the light of higher dimensional analogues. For instance, let us replace the finite field extensions $L|K$ of a number field K by all smooth complete (i.e., proper) algebraic curves defined over K of a fixed genus g. If $\mathfrak{p}$ is a prime ideal of K, then for any such curve X, one may define the "reduction mod $\mathfrak{p}$". This is a curve defined over the residue class field of $\mathfrak{p}$. One says that X has *good reduction* at the prime $\mathfrak{p}$ if its reduction mod $\mathfrak{p}$ is again a smooth curve. This corresponds to an extension $L|K$ being unramified. In analogy to Hermite's theorem, the Russian mathematician *I.S. Šafarevič* formulated the conjecture that there exist only finitely many smooth complete curves of genus g over K with good reduction outside a fixed finite set of primes S. This conjecture was proved in 1983 by the mathematician *Gerd Faltings* (see [35]). The impact of this result can be gauged by the non-expert from the fact that it was the basis for *Faltings's* proof of the famous **Mordell Conjecture:**

Every algebraic equation

of genus $g > 1$ with coefficients in K admits only **finitely many solutions** in K.

A 1-dimensional analogue of Minkowski's theorem (2.18) was proved in 1985 by the French mathematician *J.-M. Fontaine*: over the field $\mathbb{Q}$, there are no smooth proper curves with good reduction mod p for all prime numbers p (see [39]).

Exercise 1. Let $d(\alpha)$ ... α^{n-1}), for an element $\alpha \in \mathcal{O}$ such that $L = K(\alpha)$.

Show that $\mathfrak{d}_{L|K}$ is generated by all discriminants of elements $d(\alpha)$ if $\mathcal{O}$ is a complete discrete valuation ring and the residue field extension $\lambda|\kappa$ is separable. In other words, ... equals the gcd of all discriminants of individual elements. This fails to hold in general. Counterexample: $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha)$, $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$ (see [60], chap. III, § 25, p. 443. The untranslatable German catch phrase *Discriminanten...* phenomenon ... there are *enrci/e1"*

for lhi�

Exercise 2. Let $L|K$ be a Galois extension of henselian fields with separable residue field extension and let G_i, $i \geq 0$, be the i-th ramification group. Then, if $\mathfrak{D}_{L|K} = \mathfrak{P}^s$, one has

$$s = \sum_{i=0}^{\infty} (\#G_i - 1).$$

Hint: If $\mathcal{O} = \mathfrak{o}[x]$ (see chap. II, (10.4)), then $s = v_L(\delta_{L|K}) = \sum_{\sigma \neq 1} v_L(x - \sigma x)$.

Exercise 3. The module of differentials $\Omega^1_{\mathcal{O}|\mathfrak{o}}$ is generated by a single element dx, $x \in \mathcal{O}$, and there is an exact sequence of $\mathcal{O}$-modules

$$0 \longrightarrow \mathfrak{D}_{\mathcal{O}|\mathfrak{o}} \longrightarrow \mathcal{O} \longrightarrow \Omega^1_{\mathcal{O}|\mathfrak{o}} \longrightarrow 0.$$

Exercise 4. For a tower $M \supseteq L \supseteq K$ of algebraic number fields there is an exact sequence of $\mathcal{O}_M$-modules

$$0 \longrightarrow \Omega_{L|K} \otimes \mathcal{O}_M \longrightarrow \Omega_{M|K} \longrightarrow \Omega_{M|L} \longrightarrow 0.$$

Exercise 5. If ζ is a primitive p-th root of unity, then

[illegible]

§ 3. Riemann-Roch

The notion of replete divisor introduced into our development of number theory in §1 is a terminology reminiscent of the function-theoretic model. We now have to ask the question to what extent this point of view does justice to our goal to also couch the number-theoretic results in a geometric function-theoretic fashion, and conversely to give arithmetic significance to the classical theorems of function theory. Among the latter, the Riemann-Roch theorem stands out as the most important representative. If number theory is to proceed in a geometric manner, it must work towards finding an adequate way to incorporate this result as well. This is the task we are now going to tackle.

First recall the classical situation in function theory. There the basic data is a compact Riemann surface X with the sheaf $\mathcal{O}_X$ of holomorphic functions. To each divisor $D = \sum_{P \in X} \nu_P P$ on X corresponds a **line bundle** $\mathcal{O}(D)$, i.e., an $\mathcal{O}_X$-module which is locally free of rank 1. If U is an open subset of X and $\mathcal{K}(U)$ is the ring of meromorphic functions on U, then the vector space $\mathcal{O}(D)(U)$ of sections of the sheaf $\mathcal{O}(D)$ over U is given as

$$\mathcal{O}(D)(U) = \{ f \in \mathcal{K}(U) \mid \operatorname{ord}_P(f) \geq -\nu_P \text{ for all } P \in U \}.$$

The Riemann-Roch problem is to calculate the dimension

$$\pounds(D) = \dim H^0(X.o(D))$$

of the vector space of global sections

$$H^0(X,\mathcal{O}(D)) = \mathcal{O}(D)(X).$$

In its first version the Riemann-Roch theorem does not provide a formula for $H^0(X,\mathcal{O}(D))$ itself, but for the **Euler-Poincaré characteristic**

$$\chi(\mathcal{O}(D)) = \dim H^0(X,\mathcal{O}(D)) - \dim H^1(X,\mathcal{O}(D)).$$

The formula reads

$$\chi(\mathcal{O}(D)) = \deg(D) + 1 - g,$$

where g is the **genus** of X. For the divisor $D = 0$, one has $\mathcal{O}(D) = \mathcal{O}_X$ and $\deg(D) = 0$, so that $\chi(\mathcal{O}_X) = 1 - g$; then this equation may also be replaced by

$$\chi(\mathcal{O}(D)) = \deg(D) + \chi(\mathcal{O}_X).$$

The classical Riemann-Roch formula

$$\ell(D) - \ell(\mathcal{K} - D) = \deg(D) + 1 - g$$

is then obtained by using Serre duality, which states that $H^1(X,\mathcal{O}(D))$ is dual to $H^0(X,\omega\otimes\mathcal{O}(-D))$, where $\omega = \Omega^1_X$ is the so-called **canonical module** of X, and $\mathcal{K} = \operatorname{div}(\omega)$ is the associated divisor (see for instance [51], chap. III, 7.12.1 and chap. IV, 1.1.3).

In order to mimic this state of affairs in number theory, let us recall the explanations of chap. I, §14 and chap. III, §1. We endow the places $\mathfrak{p}$ of an algebraic number field K with the rôle of points of a space X which should be conceived of as the analogue of a compact Riemann surface. The elements $f \in K^*$ will be given the rôle of "meromorphic functions" on this space X. The order of the pole, resp. zero of f at the point $\mathfrak{p} \in X$, for $\mathfrak{p}\nmid\infty$, is defined to be the integer $v_{\mathfrak{p}}(f)$, and for $\mathfrak{p}\mid\infty$ it is the real number $v_{\mathfrak{p}}(f) = -\log|f|_{\mathfrak{p}}$. In this way we associate to each $f \in K^*$ the replete divisor

$$\operatorname{div}(f) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f)\,\mathfrak{p} \in \operatorname{Div}(\bar{\mathcal{O}}).$$

More precisely, for a given divisor $D = \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}\mathfrak{p}$, we are interested in the replete ideal

$$\mathcal{O}(D) = \prod_{\mathfrak{p}} \mathfrak{p}^{-\nu_{\mathfrak{p}}},$$

and the set

$$H^0(\mathcal{O}(D)) = \{f \in K^* \mid \operatorname{div}(f) \geq -D\}$$

�II Eo(Dl,IOsf 1/1,S'J'l(pJ" locploc/,

where the relation $D' \le D$ between divisors $D' = \prod \mathfrak{p}^{\nu'_\mathfrak{p}}$ and $D = \prod \mathfrak{p}^{\nu_\mathfrak{p}}$ is simply defined to mean $\nu'_\mathfrak{p} \le \nu_\mathfrak{p}$ for all $\mathfrak{p}$. Note that $H^0(\mathfrak{o}(D))$ is no longer a vector space. An analogue of $H^1(X,\mathcal{O}(D))$ is completely missing. Instead of attacking directly the problem of measuring the size of $H^0(\mathfrak{o}(D))$, we proceed as in the function-theoretic model by looking at the "Euler-Poincaré characteristic" of the replete ideal $\mathfrak{o}(D)$. Before defining this, we want to establish the relation between the Minkowski space $K_\mathbb{R} = [\prod_\tau \mathbb{C}]^+$, $\tau \in \operatorname{Hom}(K,\mathbb{C})$, and the product $\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}$. The reader will allow us to explain this simple situation in the following sketch.

We have the correspondences

$$\tau: K \to \mathbb{R} \qquad \text{real prime, } \mathfrak{p} = \mathfrak{p}_\tau;\ K_\mathfrak{p} \cong \mathbb{R},$$

$$\tau \ne \bar\tau: K \to \mathbb{C} \qquad \text{complex prime, } \mathfrak{p} = \mathfrak{p}_\tau = \mathfrak{p}_{\bar\tau};\ K_\mathfrak{p} \cong \mathbb{C}.$$

There are the following isomorphisms

$$K \otimes_\mathbb{Q} \mathbb{R} \xrightarrow{\sim} K_\mathbb{R}, \qquad a \otimes x \longmapsto \big((\tau a)x\big)_\tau,$$

$$K \otimes_\mathbb{Q} \mathbb{R} \xrightarrow{\sim} \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}, \qquad a \otimes x \longmapsto \big((\tau_\mathfrak{p} a)x\big)_{\mathfrak{p}|\infty},$$

$\tau_\mathfrak{p}$ being the canonical embedding $K \to K_\mathfrak{p}$ (see chap. II, (8.3)). They fit into the commutative diagram

$$\begin{array}{ccccc}
K \otimes \mathbb{R} & \longrightarrow & K_\mathbb{R} & \subseteq & \prod_{\mathfrak{p}\ \text{real}} \mathbb{R} \times \prod_{\mathfrak{p}\ \text{complex}} (\mathbb{C} \times \mathbb{C})^+ \\
\Big\| & & \Big\uparrow & & \Big\| \qquad \Big\uparrow \wr\, \prod (\sigma_\mathfrak{p} \times \bar\sigma_\mathfrak{p}) \\
K \otimes \mathbb{R} & \longrightarrow & \prod_{\mathfrak{p}|\infty} K_\mathfrak{p} & = & \prod_{\mathfrak{p}\ \text{real}} K_\mathfrak{p} \times \prod_{\mathfrak{p}\ \text{complex}} K_\mathfrak{p},
\end{array}$$

where the arrow on the right is given by $a_\mathfrak{p} \mapsto (a_\mathfrak{p}, \bar a_\mathfrak{p})$. Via this isomorphism, we identify $K_\mathbb{R}$ with $\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}$:

$$K_\mathbb{R} = \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}.$$

The scalar product $\langle x, y\rangle = \sum_\tau x_\tau \bar y_\tau$ on $K_\mathbb{R}$ is then transformed into

$$\langle x, y\rangle = \sum_{\mathfrak{p}\ \text{real}} x_\mathfrak{p} y_\mathfrak{p} + \sum_{\mathfrak{p}\ \text{complex}} (x_\mathfrak{p} \bar y_\mathfrak{p} + \bar x_\mathfrak{p} y_\mathfrak{p}).$$

The Haar measure μ, on $K11c$ which is determined hy {\, v) becomes the product measure where

$$\mu_{\mathfrak p} = \text{Lebesgue measure on } K_{\mathfrak p} = \mathbb{R}, \text{ if } \mathfrak p \text{ real},$$
$$\mu_{\mathfrak p} = 2\,\text{Lebesgue measure on } K_{\mathfrak p} = \mathbb{C}, \text{ if } \mathfrak p \text{ complex}.$$

Indeed, the system $1/\sqrt{2}$, $i/\sqrt{2}$ is an orthonormal basis with respect to the scalar product $x\bar y + \bar x y$ on $K_{\mathfrak p} = \mathbb{C}$. Hence the square $Q = \{z = x + iy \mid 0 \le x, y \le 1/\sqrt{2}\}$ has volume $\mu_{\mathfrak p}(Q) = 1$, but Lebesgue volume 1/2.

Finally, the logarithm map

$$\ell : \Big[\prod_\tau \mathbb{C}^*\Big]^+ \longrightarrow \Big[\prod_\tau \mathbb{R}\Big]^+, \quad x \longmapsto \big(\log|x_\tau|\big)_\tau$$

studied in Minkowski theory is transformed into the mapping

$$\ell : \prod_{\mathfrak p|\infty} K_{\mathfrak p}^* \longrightarrow \prod_{\mathfrak p|\infty} \mathbb{R}, \quad (x_{\mathfrak p}) \longmapsto \big(\log|x_{\mathfrak p}|_{\mathfrak p}\big),$$

for one has the commutative diagram

$$\begin{array}{ccc} K_{\mathbb{R}}^* & \xrightarrow{\ \ell\ } & \big[\prod_\tau \mathbb{R}\big]^+ \\ \big\downarrow & & \big\downarrow \\ \prod_{\mathfrak p|\infty} K_{\mathfrak p}^* & \xrightarrow{\ \ell\ } & \prod_{\mathfrak p|\infty} \mathbb{R}\,, \end{array}$$

where the arrow on the right,

$$\Big[\prod_\tau \mathbb{R}\Big]^+ = \prod_\rho \mathbb{R} \times \prod_\sigma \big[\mathbb{R}\times\mathbb{R}\big]^+ \longrightarrow \prod_{\mathfrak p|\infty} \mathbb{R},$$

is defined by $x \mapsto x$ for $\rho \mapsto \mathfrak p$, and by $(x,x) \mapsto 2x$ for $\sigma \mapsto \mathfrak p$. This isomorphism takes the trace map $x \mapsto \sum_\tau x_\tau$ on $[\prod_\tau \mathbb{R}]^+$ into the trace map $x \mapsto \sum_{\mathfrak p|\infty} x_{\mathfrak p}$ on $\prod_{\mathfrak p|\infty} \mathbb{R}$, and hence the trace-zero space $H = \{x \in [\prod_\tau \mathbb{R}]^+ \mid \sum_\tau x_\tau = 0\}$ into the trace-zero space

$$H = \Big\{x \in \prod_{\mathfrak p|\infty} \mathbb{R} \;\Big|\; \sum_{\mathfrak p|\infty} x_{\mathfrak p} = 0\Big\}.$$

In this way we have translated all necessary invariants of the Minkowski space $K_{\mathbb{R}}$ to the product $\prod_{\mathfrak p|\infty} K_{\mathfrak p}$.

To a given replete ideal

$$\mathfrak a = \mathfrak a_f \cdot \mathfrak a_\infty = \prod_{\mathfrak p\nmid\infty} \mathfrak p^{\nu_{\mathfrak p}} \times \prod_{\mathfrak p|\infty} \mathfrak p^{\nu_{\mathfrak p}}$$

we now associate the following complete lattice $j\mathfrak a$ in $K_{\mathbb{R}}$. The fractional ideal $\mathfrak a_f \subseteq K$ is mapped by the embedding $j : K \to K_{\mathbb{R}}$ onto a complete lattice $j\mathfrak{a}_f$ of $K_\mathbb{R} = \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}$. By componentwise multiplication, $\mathfrak{a}_\infty = \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{\nu_\mathfrak{p}} = (\dots, e^{\nu_\mathfrak{p}}, \dots)$ yields an isomorphism

$$\mathfrak{a}_\infty : K_\mathbb{R} \longrightarrow K_\mathbb{R}, \quad (x_\mathfrak{p})_{\mathfrak{p}|\infty} \longmapsto (e^{\nu_\mathfrak{p}} x_\mathfrak{p})_{\mathfrak{p}|\infty},$$

with determinant

$$(*) \qquad \det(\mathfrak{a}_\infty) = \prod_{\mathfrak{p}|\infty} e^{f_\mathfrak{p}\nu_\mathfrak{p}} = \prod_{\mathfrak{p}|\infty} \mathfrak{N}(\mathfrak{p})^{\nu_\mathfrak{p}} = \mathfrak{N}(\mathfrak{a}_\infty).$$

The image of the lattice $j\mathfrak{a}_f$ under this map is a complete lattice

$$j\mathfrak{a} := \mathfrak{a}_\infty j\mathfrak{a}_f.$$

Let $\mathrm{vol}(\mathfrak{a})$ denote the **volume of a fundamental mesh** of $j\mathfrak{a}$ with respect to the canonical measure. By $(*)$, we then have

$$\mathrm{vol}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a}_\infty)\,\mathrm{vol}(\mathfrak{a}_f).$$

(3.1) Definition. *If $\mathfrak{a}$ is a replete ideal of K, then the real number*

$$\chi(\mathfrak{a}) = -\log \mathrm{vol}(\mathfrak{a})$$

will be called the **Euler-Minkowski characteristic** *of $\mathfrak{a}$.*

The reason for this terminology will become clear in § 8.

(3.2) Proposition. *The Euler-Minkowski characteristic $\chi(\mathfrak{a})$ only depends on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\bar{\mathcal{O}}) = J(\bar{\mathcal{O}})/P(\bar{\mathcal{O}})$.*

Proof: Let $[a] = [a]_f \times [a]_\infty = (a) \times [a]_\infty$ be a replete principal ideal. Then one has

$$[a]\mathfrak{a} = a\mathfrak{a}_f \times [a]_\infty \mathfrak{a}_\infty .$$

The lattice $j(a\mathfrak{a}_f)$ is the image of the lattice $j\mathfrak{a}_f$ under the linear map $a : K_\mathbb{R} \to K_\mathbb{R}$, $(x_\mathfrak{p}) \mapsto (a x_\mathfrak{p})$. The absolute value of the determinant of this mapping is obviously given

$$|\det(a)| = \prod_{\mathfrak{p}|\infty} |a|_\mathfrak{p} = \prod_{\mathfrak{p}|\infty} \mathfrak{N}(\mathfrak{p})^{-v_\mathfrak{p}(a)} = \mathfrak{N}([a]_\infty)^{-1}.$$

For the canonical measure, we therefore have

$$\mathrm{vol}(a\mathfrak{a}_f) = \mathfrak{N}([a]_\infty)^{-1}\mathrm{vol}(\mathfrak{a}_f).$$

Taken together with $(*)$, this yields

$$\mathrm{vol}([a]\mathfrak{a}) = \mathfrak{N}([a]_\infty\mathfrak{a}_\infty)\,\mathrm{vol}(a\mathfrak{a}_f) = \mathfrak{N}(\mathfrak{a}_\infty)\,\mathrm{vol}(\mathfrak{a}_f) = \mathrm{vol}(\mathfrak{a}),$$

so that $\chi([a]\mathfrak{a}) = \chi(\mathfrak{a})$. $\square$

The explicit evaluation of the Euler-Minkowski characteristic results from a result of Minkowski theory, viz., proposition (5.2) of chap. I.

(3.3) Proposition. *For every replete ideal* $\mathfrak a$ *of* K *one has*

$$\operatorname{vol}(\mathfrak a) = \sqrt{|d_K|}\,\mathfrak N(\mathfrak a).$$

Proof: Multiplying by a replete principal ideal $[a]$ we may assume, as $\operatorname{vol}([a]\mathfrak a) = \operatorname{vol}(\mathfrak a)$ and $\mathfrak N([a]\mathfrak a) = \mathfrak N(\mathfrak a)$, that $\mathfrak a_f$ is an integral ideal of K. By chap. I, (5.2) the volume of a fundamental mesh of $\mathfrak a_f$ is given by

$$\operatorname{vol}(\mathfrak a_f) = \sqrt{|d_K|}\,(\mathfrak o : \mathfrak a_f).$$

Hence

$$\operatorname{vol}(\mathfrak a) = \mathfrak N(\mathfrak a_\infty)\operatorname{vol}(\mathfrak a_f) = \mathfrak N(\mathfrak a_\infty)\sqrt{|d_K|}\,\mathfrak N(\mathfrak a_f) = \sqrt{|d_K|}\,\mathfrak N(\mathfrak a). \qquad \square$$

In view of the commutative diagram in § 1, p. 192, we will now introduce the **degree** of the replete ideal $\mathfrak a$ to be the real number

$$\deg(\mathfrak a) = -\log \mathfrak N(\mathfrak a) = \deg(\operatorname{div}(\mathfrak a)).$$

Observing that

$$\chi(\mathfrak o) = -\log\sqrt{|d_K|},$$

we deduce from proposition (3.3) the first version of the Riemann-Roch theorem:

(3.4) Proposition. *For every replete ideal* $\mathfrak a$ *of* K *we have the formula*

$$\chi(\mathfrak a) = \deg(\mathfrak a) + \chi(\mathfrak o).$$

In function theory there is the following relationship between the Euler-Poincaré characteristic and the genus g of the Riemann surface X in question:

$$\chi(\mathcal O) = \dim H^0(X, \mathcal O_X) - \dim H^1(X, \mathcal O_X) = 1 - g.$$

There is no immediate analogue of $H^1(X, \mathcal O_X)$ in arithmetic. However, there is an analogue of $H^0(X, \mathcal O_X)$. For each replete ideal $\mathfrak a = \prod_{\mathfrak p}\mathfrak p^{\nu_{\mathfrak p}}$ of the number field K, we define

$$H^0(\mathfrak a) = \{ f \in K^* \mid v_{\mathfrak p}(f) \ge \nu_{\mathfrak p} \text{ for all } \mathfrak p\}.$$

This is a finite set because $H^0(\mathfrak a)$ lies in the [illegible] of the lattice $j\mathfrak a_f \subseteq K_{\mathbb R}$ which is bounded by the conditions $|f_{\mathfrak p}| \le e^{-\nu_{\mathfrak p}}$. As the analogue of the dimension, we put $\ell(\mathfrak a) = 0$ if $H^0(\mathfrak a) = 0$, and in all other cases,

$$\ell(\mathfrak a) := \log \frac{\#H^0(\mathfrak a)}{\operatorname{vol}(W)}.$$

where the normalizing factor vol(W) is the volume of the set

$$w� l<c,)EK,�[l;icr11,,1 :' 1).$$

This volume is given explicilly by

$$\mathrm{vol}(W) = zr(2rr)",$$

where *r,* resp. *s,* is the number of real. resp. complex, prime� of K (see the proof of chap. I, (5.3)). In particular, one has

$$H^{0}(o) = Jl(K). \quad \text{sothat} \quad f(o) = \log \frac{\#11,(K)}{zrczrrr'}$$

because lflp :S 1 for all p, and TIP I/Ip= I implies lflp = I for all p, so that $H^0(o)$ is a finite subgroup of K^* and thus must consist of all roots of unity. This normalization leads *w,* necessarily to the following definition of the geom, of a number field, which had already been proposed *ad hoc* by the French mathematician *ANDRE Wm.* in 1939 (sec [l.381).

(3.5) Definition. *The* genus of *a number field K is* defined *to be the real number*

$$g = i'(v) - X(o) = \log � - \quad \#1,(K)./Til,;T$$

Observe that the genus of the field of rational number<; Q is 0. Using thi:;. definition, the Riemann-Roch formula (3.4) takei,. the following shape:

(3.6) Proposition. For *every replete ideal a* of *K one ha:;.*

$$x(a) = \deg(a) + £(0) - g.$$

The analogue of the strong Riemann-Roch formula

$$£(D) � \deg(D) + I - g + £(K - /J).$$

hinges on the following deep theorem of Minkow<;ki theory. which i<; due to *SERGF LA/\'G* and which reflects an arithmetic analogue of Serre duality. A:;. usual, let *r.* resp. *s,* denote the number of real, re1-p. complex, primes, and11=IK:QJ.

(3.7) Theorem (S *LANG). For replete ideals a=* nl' p"'p E *J(0), one has*

$$\#H''(a^{-1}) � \frac{2^1(2rr)'}{/Til,;j} �(a)+ o(�(a)'^{I}')$$

if 91(a) ---+ oo. Here, a.� usual, O(t) denotes a *function* suc/J *that O(t)/t* remain1,, *bounded* as *t* ---+ *x.*

For the proof of the theorem we need the following

(3.8) **Lemma.** Lei a_1, , 011*be fractional ideals representing the cla.sses* of *the finite ideal class group Pie(* a). *Let (* be a *positive conMant and*

$$211 = \{ o = \prod_p P''' P \mid n1 = a,, 91(p)vP \ 2 \ c91(a)^{1''111} \text{ for } Ploo)$$

Then *the constam (c:m be chosen in such a way that*

$$1(6) \text{�} \bigcup_{\models}^{h} '21,P(i5).$$

Pr-oof: Let 23, = {a E ,l(O) | nr = 01). Multiplying by a suitable replete principal ideal [al, every *a* E J(o) may be transformed into a replete ideal *a'* = a[aj :-uch that o� = 0_1 for some i. Consequently, one has 1(8) = LJt=I 23_1?(8). It therefore suffices to show that 23_1 £:;" '2l,P(8) for i = I. . *h*, if the constant c is chosen conveniently. To do thb, let *a= a,arx,* E 23,, O:,o = np1,x,PVp E nploc,iF!/.�. Then we find for the replete ideal

$$a;.,,= a'X)91(o,.,J-\text{�} = \prod_{''\text{�}} p''\text{�},$$

where *v*� = l!p - ¼ Lqlrx, /qvq, that 91(o�) = I, and thus Lplx *{pv*� = 0. The vector

$$(. \quad ,fps;....) \text{ En } \underset{Pl''''}{\text{ffi<}}$$

therefore lies in the trace-zero H = {(xp) E nploo JR | = 0). Inside it we have - see chap. I, - the complete unit Thus there exists a lattice point A(u) = (. . - /pvp(u),)pio-., *u* E *o**, �uch that

$$|fi,v\text{�} - /pvp(u)j :S \{pco$$

with a constant *lo* depending only on the lattice A(o*). This implies

$$vp\text{-}vp(u) = v\text{�}+\text{�} \underset{n}{L} \underset{qlex,}{\{qvq\text{-}vp(u):::\text{�}} \underset{n}{\log 91(arx.,)}+c_0 = \text{�} \underset{n}{\log 91(a)}+c_1$$

with c_1 = (O - h log91(0_1). Putting now b = *a[u* ^{1}J = TTpPnP, we get b_1 = 0_1. This is because [ult= (u)= (I) and

$$\{pnp = JP(\text{ vp - l'p(u)) :'S } \text{�} \log 91(a) + nc_1,$$

so that $91(p)^{11}$P::: *em¹91(a)fv/n* for Ploo; then b E -it,. so that *a=* b[u] E m,P(8), where *c* = *emi_* [J

Proof of (3.7): A� O(t) = O(t) - 1, we may replace $H^0((c^1)$ by

$H^0(n^{1}) =$ lfr\o.-^{1}) u {O} = { f E o.j^1 11 /Ip :S \Jl(i.,)^1'P for plcc).

We have to show that there arc constants C, C' �uch that

$$\#\overline{H}^0(\mathfrak{a}^{-1}) - \frac{2^r(2\pi)^s}{\sqrt{|d_K|}}\mathfrak{N}(\mathfrak{a})\Big| \le C\mathfrak{N}(\mathfrak{a})^{1-\frac{1}{n}}$$

for all o. E I(o) satisfying \)1(0.) 2: C'. For EK*. the set $11^\circ(n^{-1})$ is mapped bijectively via f-+ onto the set H^0(laja-^{1}). The numbers #ll^0(a-^{1}) and \Jl(a) thu� depend only on the da�:c. mod *P(O).* As by the preceding lemma J(0) = U;^{1}=l m, *P(O),* it suffices to �how(*) for ranging over the set 2l$_1$.

For this, we shall use the identification of Minkowski �pace

$$K_{\mathbb{R}} = \coprod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}$$

with its canonical measure. Since Ot = a, for n = np p^1'p E Q(,, we have

$$\overline{H}^0(\mathfrak{a}^{-1}) = \left\{ f \in \mathfrak{a}_i^{-1} \;\middle|\; |f|_{\mathfrak{p}} \le \mathfrak{N}(\mathfrak{p})^{1/p} \text{ for } \mathfrak{p}|\infty \right\}.$$

We therefore have to count the lattice points in r = Ja-;^{1} s; *Kffi.* which fall into the domain

where *Dp* = {x E *Kp* | lxlp :S \Jl(p)^1'P}. Let *F* be a fundamental me�h of *r*. We consider the �els

x � I *y* Er I *(F* + *y)* n *P,* # 01.

r �*lyer* I F + C;;P,I.

x, *Y* � ! *y* Er | (F + *y)* n *JP,*# 01.

A5 *y* � *mPH* = H^0 (n^1) �*x* and a�*LJY''y(F+y)* � *P..*S; *UF''x(F+y).* one has

$$\#Y \le \#\overline{H}^0(\mathfrak{a}^{-1}) \le \#X$$

a5 well as

#*Y* vol(F) :S vol(P$_0$) :S #*X* vol(F).

This implies

#lln(a-1) - vol(P..) < #X · #*Y*= #*(X* "- Y).
| vol(F) -

For the set $P_\mathfrak{a} = \prod_{\mathfrak p|\infty} D_\mathfrak{p}$, we now have

$$\operatorname{vol}(P_\mathfrak{a}) = \prod_{\mathfrak p \text{ real}} 2\mathfrak{N}(\mathfrak p)^{\nu_\mathfrak p} \prod_{\mathfrak p \text{ complex}} 2\pi\mathfrak{N}(\mathfrak p)^{\nu_\mathfrak p} = 2^r(2\pi)^s\mathfrak{N}(\mathfrak a_\infty)$$

(observe here that, under the identification $K_\mathfrak{p} = \mathbb{C}$ one has the equation $|x|_\mathfrak{p} = |x|^2$). For the fundamental mesh F, (3.3) yields

$$\operatorname{vol}(F) = \sqrt{|d_K|}\,\mathfrak{N}(\mathfrak a_f^{-1}).$$

From this we get

$$\left|\#\overline{H}^0(\mathfrak a^{-1}) - \frac{2^r(2\pi)^s}{\sqrt{|d_K|}}\,\mathfrak{N}(\mathfrak a)\right| \le \#(X \setminus Y).$$

Having obtained this inequality, it suffices to show that there exist constants C, C' such that

$$\#(X \setminus Y) \le \#\{\gamma \in \Gamma \mid (F+\gamma) \cap \partial P_\mathfrak{a} \neq \emptyset\} \le C\,\mathfrak{N}(\mathfrak a)^{\frac{n-1}{n}}$$

for all $\mathfrak a \in \mathfrak{A}_1$ with $\mathfrak{N}(\mathfrak a) \ge C'$. We choose $C' = 1$ and find the constant C in the remainder of the proof. We parametrize the set $P_\mathfrak{a} = \prod_{\mathfrak p|\infty} D_\mathfrak{p}$ via the mapping

$$\varphi : I^n \to P_\mathfrak{a},$$

where $I = [0,1]$, which is given by

$$I \longrightarrow D_\mathfrak{p}, \quad t \longmapsto 2a_\mathfrak{p}(t - \tfrac{1}{2}), \qquad \text{if } \mathfrak p \text{ real},$$

$$I^2 \longrightarrow D_\mathfrak{p}, \quad (\rho,\theta) \longmapsto a_\mathfrak{p}(\rho\cos 2\pi\theta, \rho\sin 2\pi\theta), \qquad \text{if } \mathfrak p \text{ complex},$$

where $a_\mathfrak{p} =$ We bound the norm $\|d\varphi(x)\|$ of the derivative $d\varphi(x) : \mathbb{R}^n \to \mathbb{R}^n$ $(x \in I^n)$. If $d\varphi(x) = (a_{ij})$, then $\|d\varphi(x)\| \le n \max |a_{ij}|$. Every partial derivative of φ is now bounded by $2a_\mathfrak{p}$, resp. $2\pi a_\mathfrak{p}$. Since $\mathfrak a \in \mathfrak{A}_1$, we have that $a_\mathfrak{p} = \mathfrak{N}(\mathfrak p)^{\nu_\mathfrak p} \le \mathfrak{N}(\mathfrak a)^{1/n}$ for all $\mathfrak p|\infty$. It follows that

$$\|d\varphi(x)\| \le 2\pi n \max a_\mathfrak{p} \le c_1\mathfrak{N}(\mathfrak a)^{1/n}.$$

The mean value theorem implies that

$$\|\varphi(x) - \varphi(y)\| \le c_1\mathfrak{N}(\mathfrak a)^{1/n}\|x - y\|,$$

where $\|\ \|$ is the euclidean norm. The boundary of $P_\mathfrak{a}$,

$$\partial P_\mathfrak{a} = \bigcup_\mathfrak{p}\Big[\partial D_\mathfrak{p} \times \prod_{\mathfrak q \neq \mathfrak p} D_\mathfrak{q}\Big],$$

is parametrized by a finite number of boundary cubes I^{n-1} of I^n. We subdivide every edge of I^{n-1} into $m = [\mathfrak{N}(\mathfrak a)^{1/n}] \ge C' = 1$ segments of equal length and obtain for I^{n-1} a decomposition into m^{n-1} small cubes of diameter $\le (n-1)^{1/2}/m$. From (**), the image of such a small cube under φ has a diameter $\le \frac{(n-1)^{1/2}}{m}c_1\mathfrak N(\mathfrak a)^{1/n} \le (n-1)^{1/2}c_1\frac{\mathfrak N(\mathfrak a)^{1/n}}{\mathfrak N(\mathfrak a)^{1/n}} = (n-1)^{1/2}c_1 =: c_2$. The number of translates $F+\gamma$, $\gamma\in\Gamma$, meeting a domain of diameter $\le c_2$ is bounded by a constant c_3 which depends only on c_2 and the fundamental mesh F. The image of a small cube under φ thus meets at most c_3 translates $F+\gamma$. Since there are precisely $m^{n-1} = ([\mathfrak N(\mathfrak a)^{1/n}]+1)^{n-1}$ cubes in I^{n-1}, we see that $\varphi(I^{n-1})$ meets at most $c_3([\mathfrak N(\mathfrak a)^{1/n}]+1)^{n-1}$ translates, and since the boundary $\partial P_{\mathfrak a}$ is covered by at most $2n$ such parts $\varphi(I^{n-1})$, we do indeed find that

$$\#\{\gamma\in\Gamma \mid (F+\gamma)\cap\partial P_{\mathfrak a}\neq\emptyset\} \le C\,\mathfrak N(\mathfrak a)^{1-\frac1n},$$

for all $\mathfrak a\in\mathfrak A$, with $\mathfrak N(\mathfrak a)\ge 1$, where $C = 2nc_3$ is a constant which is independent of $\mathfrak a\in\mathfrak A$, as required. $\square$

From the theorem we have just proved, we now obtain the strong version of the Riemann-Roch theorem. We want to formulate it in the language of divisors. Let $D = \sum_{\mathfrak p}\nu_{\mathfrak p}\mathfrak p$ be a replete divisor of K,

$$H^0(D) := H^0(\mathfrak o(D)) = \{f\in K^* \mid v_{\mathfrak p}(f)\ge -\nu_{\mathfrak p}\},$$

$$\ell(D) = \ell(\mathfrak o(D)) = \log\frac{\#H^0(D)}{\operatorname{vol}(W)} \quad\text{and}\quad \chi(D) = \chi(\mathfrak o(D)).$$

We call the number

$$i(D) := \ell(D) - \chi(D)$$

the index of specialty of D and get the

(3.9) Theorem (Riemann-Roch). *For every replete divisor $D\in Div(\bar{\mathfrak o})$ we have the formula*

$$\ell(D) = \deg(D) + \ell(\mathfrak o) - g + i(D).$$

The index of specialty $i(D)$ satisfies

$$i(D) = O(e^{-\frac{1}{n}\deg(D)}),$$

in particular, $i(D)\to 0$ for $\deg(D)\to\infty$.

Proof: The formula for $\ell(D)$ follows from $\chi(D) = \deg(D) + \ell(\mathfrak o) - g$ and $\chi(D) = \ell(D) - i(D)$. Putting $\mathfrak a^{-1} = \mathfrak o(D)$, we find by (3.7) that

$$\frac{\#H^0(\mathfrak a^{-1})}{2^r(2\pi)^s} = \frac{\mathfrak N(\mathfrak a)}{\sqrt{|d_K|}}\left(1 + O(\mathfrak N(\mathfrak a)^{-\frac1n})\right).$$

for some function $\varphi(\mathfrak a)$ which remains bounded as $\mathfrak N(\mathfrak a) \to \infty$, so that $\deg(D) = -\log \mathfrak N(\mathfrak a^{-1}) = \log \mathfrak N(\mathfrak a) \to \infty$. Taking logarithms and observing that $\log(1+O(t)) = O(t)$ and $\mathfrak N(\mathfrak a)^{-1/2} = \exp(-\frac12 \deg D)$, we obtain

$$\ell(D) = \ell(\mathfrak a^{-1}) = -\log(\sqrt{|d_K|}\,\mathfrak N(\mathfrak a^{-1})) + O(\mathfrak N(\mathfrak a)^{-1/2})$$
$$= \chi(D) + O(e^{-\frac12 \deg D}).$$

Hence $i(D) = \ell(D) - \chi(D) = O(e^{-\frac12 \deg D})$. □

To conclude this section, let us study the variation of the Euler-Minkowski characteristic and of the genus when we change the field K. Let $L|K$ be a finite extension and $\mathfrak o$, resp. $\mathcal O$, the ring of integers of K, resp. L. In §2 we considered **Dedekind's complementary module**

$$\mathfrak C_{L|K} = \{x \in L \mid Tr(x\mathcal O) \subseteq \mathfrak o\} \cong \operatorname{Hom}_{\mathfrak o}(\mathcal O, \mathfrak o).$$

It is a fractional ideal in L whose inverse is the different $\mathfrak D_{L|K}$. From (2.6), it is divisible only by the prime ideals of L which are ramified over K.

(3.10) Definition. The *fractional ideal*

$$\omega_K = \mathfrak C_{K|\mathbb Q} \cong \operatorname{Hom}_{\mathbb Z}(\mathfrak o, \mathbb Z)$$

is called the **canonical module** *of the number field* K.

By (2.2) we have the

(3.11) Proposition. *The canonical modules of L and K satisfy the relation*

$$\omega_L = \mathfrak C_{L|K}\,\omega_K.$$

The canonical module ω_K is related to the Euler-Minkowski characteristic $\chi(\mathfrak o)$ and the genus g of K in the following way, by formula (3.3): $\operatorname{vol}(\mathfrak o) = \sqrt{|d_K|}$.

(3.12) Proposition. $\deg \omega_K = -2\chi(\mathfrak o) = 2g - 2\ell(\mathfrak o)$.

Proof: By (2.9) we know that $\mathfrak N_{K|\mathbb Q}(\mathfrak D_{K|\mathbb Q})$ is the discriminant ideal $\mathfrak d_{K|\mathbb Q} = (d_K)$, and therefore by (1.6),

$$\mathfrak N(\omega_K) = \mathfrak N(\mathfrak D_{K|\mathbb Q})^{-1} = \mathfrak N(\mathfrak d_{K|\mathbb Q})^{-1} = |d_K|^{-1},$$

so that, as $\operatorname{vol}(\mathfrak o) = \sqrt{|d_K|}$, we have indeed

$$\deg \omega_K = -\log \mathfrak N(\omega_K) = \log |d_K| = 2\log \operatorname{vol}(\mathfrak o) = -2\chi(\mathfrak o) = 2g - 2\ell(\mathfrak o).$$ □

As for the genus, we now obtain the following analogue of the **Riemann-Hurwitz formula** of function theory.

(3.13) **Proposition.** *Let $L|K$ be a finite extension and g_L, resp. g_K, the genus of L, resp. K. Then one has*

$$g_L - \ell(\mathcal{O}_L) = [L:K]\big(g_K - \ell(\mathcal{O}_K)\big) + \frac{1}{2}\deg \mathfrak{D}_{L|K}\,.$$

In particular, in the case of an unramified extension $L|K$:

$$\chi(\mathcal{O}_L) = [L:K]\,\chi(\mathcal{O}_K).$$

Proof: Since $\omega_L = \mathfrak{D}_{L|K}\,\omega_K$, one has

$$\mathfrak{N}(\omega_L) = \mathfrak{N}(i_{L|K}\,\omega_K)\,\mathfrak{N}(\mathfrak{D}_{L|K}) = \mathfrak{N}(\omega_K)^{[L:K]}\,\mathfrak{N}(\mathfrak{D}_{L|K}),$$

so that

$$\deg \omega_L = [L:K]\deg\omega_K + \deg \mathfrak{D}_{L|K}.$$

Thus the proposition follows from (3.12). □

The Riemann-Hurwitz formula tells us in particular that, in the decision we took in §1, we really had no choice but to consider the extension $\mathbb{C}|\mathbb{R}$ as *unramified*. In fact, in function theory the module corresponding by analogy to the ideal $\mathfrak{D}_{L|K}$ takes account of precisely the branch points of the covering of Riemann surfaces in question. In order to obtain the same phenomenon in number theory we are forced to declare all the infinite primes $\mathfrak{P}$ of L unramified, since they do not occur in the ideal $\mathfrak{D}_{L|K}$.

Thus the fact that $\mathbb{C}|\mathbb{R}$ is unramified appears to be forced by nature itself. Investigating the matter a little more closely, however, this turns out not to be the case. It is rather a consequence of a well-hidden initial choice that we made. In fact, in chap. I, §5, we equipped the Minkowski space

$$K_{\mathbb{R}} = \Big[\prod_\tau \mathbb{C}\Big]^+$$

with the "canonical metric"

$$\langle x, y\rangle = \sum_\tau x_\tau \bar{y}_\tau\,.$$

Replacing it, for instance, by the "Minkowski metric"

$$(x, y) = \sum \alpha_\tau x_\tau \bar{y}_\tau\,,$$

$\alpha_\tau = 1$ if $\tau = \bar\tau$, $\alpha_\tau = \frac12$ if $\tau \neq \bar\tau$, changes the whole picture. The Haar measures on $K_{\mathbb R}$ belonging to $\langle\,,\rangle$ and $(\,,)$ are related as follows:

$$\mathrm{vol}_{\mathrm{canonical}}(X) = 2^s\,\mathrm{vol}_{\mathrm{Minkowski}}(X).$$

Distinguishing the invariants of Riemann-Roch theory with respect to the Minkowski measure by a tilde, we get the relations

$$\tilde\chi(\mathfrak a) = \chi(\mathfrak a) + \log 2^s, \quad \tilde l(\mathfrak a) = l(\mathfrak a) + \log 2^s$$

(the latter in case that $H^0(\mathfrak a) \neq 0$), whereas the genus remains unchanged. Substituting this into the Riemann-Hurwitz formula (3.13) preserves its shape only if one enriches $\mathfrak d_{L|K}$ into a replete ideal in which all infinite primes $\mathfrak P$ such that $L_{\mathfrak P} \neq K_{\mathfrak p}$ occur. This forces us to consider the extension $\mathbb C|\mathbb R$ as *ramified*, to put $e_{\mathfrak P|\mathfrak p} = [L_{\mathfrak P} : K_{\mathfrak p}]$, $f_{\mathfrak P|\mathfrak p} = 1$, and in particular

$$e_{\mathfrak p} = [K_{\mathfrak p} : \mathbb R], \qquad f_{\mathfrak p} = 1.$$

The following modifications ensue from this. For an infinite prime $\mathfrak p$ one has to define

$$v_{\mathfrak p}(a) = -e_{\mathfrak p}\log|a|, \quad \mathfrak p^\nu = e^{-\nu/e_{\mathfrak p}}, \quad \mathfrak N(\mathfrak p) = e.$$

The absolute norm as well as the degree of a replete ideal $\mathfrak a$ remain unaltered:

$$\tilde{\mathfrak N}(\mathfrak a) = \mathfrak N(\mathfrak a), \quad \widetilde{\deg}(\mathfrak a) = -\log\tilde{\mathfrak N}(\mathfrak a) = \deg(\mathfrak a).$$

The canonical module ω_K however has to be changed:

$$\tilde\omega_K = \omega_K \prod_{\mathfrak p\ \mathrm{complex}} \mathfrak p^{2\log 2}.$$

in order for the equation

$$\deg\tilde\omega_K = -2\tilde\chi(\mathfrak o) = 2g - 2\tilde l(\mathfrak o)$$

to hold. By the same token, the ideal $\mathfrak d_{L|K}$ has to be replaced by the replete ideal

$$\tilde{\mathfrak d}_{L|K} = \mathfrak d_{L|K} \prod \mathfrak P^{2\log 2}$$

so that

$$\tilde\omega_L = \tilde{\mathfrak d}_{L|K}\,\tilde\omega_K.$$

In the same way as in (3.13), this yields the Riemann-Hurwitz formula

$$g_L - \tilde l(\mathfrak o_L) = [L:K](g_K - \tilde l(\mathfrak o_K)) + \frac12 \deg\tilde{\mathfrak d}_{L|K}.$$

In view of this sensitivity to the chosen metric on Minkowski space $K_{\mathbb R}$, the mathematician UWE JANNSEN proposes as analogues of the function fields not just number fields K by themselves but number fields equipped with a metric of the type

$$\langle x, y\rangle_K = \sum_\tau \alpha_\tau x_\tau \bar{y}_\tau ,$$

$\alpha_\tau > 0$, $\alpha_\tau = \alpha_{\bar\tau}$, on $K_{\mathbb{C}}$. Let these new objects be called **metrized number fields.** This idea does indeed do justice to the situation in question in a very precise manner, and it is of fundamental importance for algebraic number theory. We denote metrized number fields $(K, \langle\ ,\ \rangle_K)$ as $\bar{K}$ and attach to them the following invariants. Let

$$\langle x, y\rangle_K = \sum_\tau \alpha_\tau x_\tau \bar{y}_\tau .$$

Let $\mathfrak{p} = \mathfrak{p}_\tau$ be the infinite prime corresponding to $\tau : K \to \mathbb{C}$. We then put $\alpha_{\mathfrak{p}} = \alpha_\tau$. At the same time, we also use the letter $\mathfrak{p}$ for the positive real number

$$\mathfrak{p} = e^{\alpha_{\mathfrak{p}}} \in \mathbb{R}^*_+ ,$$

which we interpret as the replete ideal $(1) \times (1, \dots, 1, e^{\alpha_{\mathfrak{p}}}, 1, \dots, 1) \in J(\mathcal{O}) \times \prod_{\mathfrak{p}|\infty} \mathbb{R}^*_+$. We put

$$e_{\mathfrak{p}} = 1/\alpha_{\mathfrak{p}} \quad \text{and} \quad f_{\mathfrak{p}} = \alpha_{\mathfrak{p}}[K_{\mathfrak{p}} : \mathbb{R}],$$

and we define the valuation $v_{\mathfrak{p}}$ of K^* associated to $\mathfrak{p}$ by

$$v_{\mathfrak{p}}(a) = -e_{\mathfrak{p}} \log |\tau a| .$$

Further, we put

$$\mathfrak{N}(\mathfrak{p}) = e^{f_{\mathfrak{p}}} \quad \text{and} \quad |a|_{\mathfrak{p}} = \mathfrak{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(a)},$$

so that again $|a|_{\mathfrak{p}} = |\tau a|$ if $\mathfrak{p}$ is real, and $|a|_{\mathfrak{p}} = |\tau a|^2$ if $\mathfrak{p}$ is complex. For every replete ideal $\mathfrak{a}$ of $\bar{K}$, there is a unique representation $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$, which gives the absolute norm $\mathfrak{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{\nu_{\mathfrak{p}}}$, and the degree

$$\deg_{\bar{K}}(\mathfrak{a}) = -\log \mathfrak{N}(\mathfrak{a}).$$

The *canonical module* of $\bar{K}$ is defined to be the replete ideal

$$\omega_{\bar{K}} = \omega_K \cdot \omega_\infty \in J(\bar{\mathcal{O}}) = J(\mathcal{O}) \times \prod_{\mathfrak{p}|\infty} \mathbb{R}^*_+ ,$$

where ω_K is the inverse of the different $\mathfrak{D}_{K|\mathbb{Q}}$ of $K|\mathbb{Q}$, and

$$\omega_\infty = (\alpha_{\mathfrak{p}}^{-1})_{\mathfrak{p}|\infty} \in \prod_{\mathfrak{p}|\infty} \mathbb{R}^*_+ .$$

The Riemann-Roch theory may be transferred without any problem, using the definitions given above, to metrized number fieldi,, $K = (K, (,)K)$, Distinguishing their invariants by the suffix f yields the relations

$$\mathrm{volR}(X) = Q\ Ja;\ \ \mathrm{vol}(X),$$

because Ta: (K1r.:, (,)K)----+ (K3:, (,)), (x-r) r-+ CJU-;-x-r), is an isometry with determinant TI-r .jci;, and therefore

$$XR(oK) = -\ \log volR(oK) = x(oK) - \log I)\ ,ja;,$$

$$\log \frac{\#II^{o}(OK)}{\mathrm{volK}(W)} = \ell(\mathcal{O}_K) - \log|\,|\sqrt{\alpha_\tau}\,.$$

The genus

#1,(KJv'l"dK]

$$f.:R = fR\_(OK) - XK(oK) = \epsilon(OK) - x(CJK) = \log ◆$$

does not depend on the choice of metric.

Just as in function theory, there is then no longer one smallest is replaced by the continuous family of metrized fields (Q, *axy)*, *a* E all of which have genus ,r.: = 0. One even has the

(3.14) Proposition. *The metrized fields* (Q, *axy)* are *the only* metrized *number* fields of genus *0*.

Proof: We have

,- - lo• #i,(KJv'l"dK] -0 - #µ(K)/jd;;T � 2' (2rr)'
�K- g 2'"(2rr)S -

Since rr is transcendental, one has $s = 0$. i.e., K is totally real. Thus $\#p.(K) = 2$ so that $|dK| = 4^{11\ 1}$, where $n = r =$ LK: IQ]. In view of the bound (2.14) on the di�criminant

IdKl/2 � S(¾r/2_

this can only happen if *n* .:S 6, But for this case one has sharper bounds, due to *Om.Y?KO* (sec 11111, table 2):

IdKl/n	�	3.09	4.21	5.30	6.35

This is not compatible with kh $1^1/n = 4$�, so we may conclude that *n* _:s 2. But there is no real quadratic field with di1-criminant *ldK* I = 4 (see chap. I, *2, exercise 4). Hence *11* = I, so that $K = Q$. □

An *extension of metri:ed numher fields* is a pair i = (K. (,)K), L = (L, (,)!,).such that K �Land the metric5

$$x, y\rangle_L = \sum \beta_\sigma x_\sigma \overline{y}_\sigma$$

5atisfy the relation υ'r 2: /Ja whenever r = alK• lf,.PIP arc infinite primes of LI K, ,.P belonging to *a* and p to r = *a* I K, we define the *ramification index* and *inertia degree* by

e'-J.lip=ctr//Ja and fq31p=/Ja/a,[L,v:Kpl-

Thus the fundamental identity

I: e•oi, f'v1p � [L, KI
'PIP

is preserved. Also ,.P i5 unramilicd if and only if *ar* = �*a*. For "replete prime ideals" p = ear, ,.P = *efi"*, we put

i11dP)=TT'1J"'PIP, NL1d'1J)=phiv.
'PIP

Finally we define the *different* of LIK to be the replete ideal

'Dr,,R='.1.hlK '.Dc,oEl(BL)=l(oL)x TI lR.�.
'-"l31"'-

where '.D$_{L\ K}$ is the different of LIK and

'.lJ�� (f'P/ae)·a1� E TT
'Pl�

where /3rp = *f3a* and ap = *ar* (,.P belongs to *a* and p to r = *a* I K). With this convention. we obtain the general *Riemann-Hurwitz formula*

gr, - f1:(0L) = [L: *Kl(g-K - fK(oK))* - � deg'D[ik ·

If we comider only number fields endowed with the Minkowski metric, then *L'-J.l #- KP* is always ramified. In this way the convention found in many textbooks i� no longer incompatible with the custom� introduced in the present book.

§ 4. Metrized CJ-Modules

The Riemann-Roch theory which wa5 presented in the preceding section in the case of replete ideals is embedded in a much more far-reaching theory which treats finitely generated o-modules. It is only in this setting that the theory display" its true nature. and becomes susceptible to the most comprehensive generali7.ation. This theory i� subject to a formafo,m which has been constructed by ALL"XA•\·nt.H GHOTI!FNntECK for higher dimensional algebraic varieties, and which we will no\\- develop for number fields. In doing so, our principal attention will he focu<;ed a� before on the kind of compactificalion which i<; accompli�hed by taking into account the infinite places. The effect is that a leading r6le is claimed by linear algebra - frn which we refer to [15]. Our treatment is based on a cour�e on "'Arakclov Theory and Grothcndieck-Riemann-Roch" taught hy Gu,'VTEH Tu1rw1,. There, however, proofs were not given directly, a� we will do here. but usually deduced as �pecial case� from the general abstract theory.

Let K be an algebraic number field and G the ring of integers of K. For the pa%age from K to IE. and we start by considering the ring

(l) $$K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}.$$

It admit� the following two further interpretations, between which we will freely go back and forth in the sequel without further explanation. The set

$$X(C) = \mathrm{Hom}(K,C)$$

induces a canonical decomposition of rings

(2) $$K,c \;;::\; \underset{aEX(C)}{\mathrm{ffi}} C. \quad o @ z \mapsto$$

Alternatively, the right-hand side may be viewed as the "ct Hom(X (C), C) of all function� $x : X(C) \to$ i.e.,

(3) $$K_{\mathbb{C}} \cong \mathrm{Hom}\big(X(\mathbb{C}), \mathbb{C}\big)$$

The field K is embedded in K,c via

$$K \longrightarrow K \otimes_{'q} C, \quad o \mapsto a @ 1,$$

and we identify it with its image. In the interpretation (2), the image of a EK appear� as the tuple E&a aa of conjugate� of o, and in the interpretation (3) as the function $x(a) = aa$.

We denote the generator of the Galois group G(CIIR) by $Fe:.,$, or �imply by F. This underline,;, the fact that it has a po�ition analogoU', to the Froheniw, automorphism Fp E G(i!i\,IF,,), in accordance with our dcci�ion of§ I to view the extension C IIR a� unramified. F induces an involution F on Kc

which, in the representation $K_{\mathbb{C}} = \mathrm{Hom}(X(\mathbb{C}), \mathbb{C})$ for $x : X(\mathbb{C}) \to \mathbb{C}$, is given by

$$(Fx)(\tau) = x(\bar{\tau}).$$

F is an automorphism of the $\mathbb{R}$-algebra $K_{\mathbb{C}}$. It is called the **Frobenius correspondence.** Sometimes we also consider, besides F, the involution $z \mapsto \bar{z}$ on $K_{\mathbb{C}}$ which is given by

We call it the **conjugation.** Finally, we call an element $x \in K_{\mathbb{C}}$, that is, a function $x : X(\mathbb{C}) \to \mathbb{C}$, **positive** (written $x > 0$) if it takes real values, and if $x(\tau) > 0$ for all $\tau \in X(\mathbb{C})$.

By convention every $\mathcal{O}$-module considered in the sequel will be supposed to be *finitely generated.* For every such $\mathcal{O}$-module M, we put

$$M_{\mathbb{C}} = M \otimes_{\mathbb{Z}} \mathbb{C}.$$

This is a module over the ring $K_{\mathbb{C}} = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{C}$, and viewing $\mathcal{O}$ as a subring of $K_{\mathbb{C}}$ – as we agreed above – we may also write

$$M_{\mathbb{C}} = M \otimes_{\mathcal{O}} K_{\mathbb{C}}$$

as $M \otimes_{\mathbb{Z}} \mathbb{C} = M \otimes_{\mathcal{O}} (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{C})$. The involution $x \mapsto Fx$ on $K_{\mathbb{C}}$ induces the involution

$$F(a \otimes x) = a \otimes Fx$$

on $M_{\mathbb{C}}$. In the representation $M_{\mathbb{C}} = M \otimes_{\mathbb{Z}} \mathbb{C}$ one clearly has

$$F(a \otimes z) = a \otimes \bar{z}.$$

(4.1) Definition. *A* **hermitian metric** *on the $K_{\mathbb{C}}$-module $M_{\mathbb{C}}$ is a sesquilinear mapping*

$$\langle \, , \, \rangle_M : M_{\mathbb{C}} \times M_{\mathbb{C}} \longrightarrow K_{\mathbb{C}},$$

i.e., a $K_{\mathbb{C}}$-linear form $\langle x, y \rangle_M$ in the first variable satisfying

$$\langle x, y \rangle_M = \overline{\langle y, x \rangle}_M,$$

such that one has $\langle x, x \rangle_M > 0$ for $x \neq 0$.

The metric $\langle \, , \, \rangle_M$ is called **F-invariant** *if we have furthermore*

$$F\langle x, y \rangle_M = \langle Fx, Fy \rangle_M.$$

This notion may be immediately reduced to the usual notion of a hermitian metric if we view the $K_{\mathbb{C}}$-module $M_{\mathbb{C}}$, by means of the decomposition $K_{\mathbb{C}} = \prod_{\tau} \mathbb{C}$, as a direct sum

$$M_{\mathbb{C}} = M \otimes_{\mathcal{O}} K_{\mathbb{C}} = \bigoplus_{\sigma \in X(\mathbb{C})} M_{\sigma}$$

of $\mathbb{C}$-vector spaces

$$M_{\sigma} = M \otimes_{\mathcal{O},\sigma} \mathbb{C}.$$

The hermitian metric $\langle\ ,\ \rangle_M$ then splits into the direct sum

$$\langle x, y\rangle_M = \bigoplus_{\sigma \in X(\mathbb{C})} \langle x_\sigma, y_\sigma \rangle_{M_\sigma}$$

of hermitian scalar products $\langle\ ,\ \rangle_{M_\sigma}$ on the $\mathbb{C}$-vector spaces M_σ. In this interpretation, the F-invariance of $\langle x, y\rangle_M$ amounts to the commutativity of the diagrams

$$\begin{tikzcd} M_\sigma \times M_\sigma \arrow[r, "\langle\ ,\ \rangle_{M_\sigma}"] \arrow[d, "F \times F"'] & \mathbb{C} \arrow[d, "F"] \\ M_{\bar\sigma} \times M_{\bar\sigma} \arrow[r, "\langle\ ,\ \rangle_{M_{\bar\sigma}}"'] & \mathbb{C}. \end{tikzcd}$$

(4.2) Definition. *A* **metrized $\mathcal{O}$-module** *is a finitely generated $\mathcal{O}$-module M with an F-invariant hermitian metric on $M_{\mathbb{C}}$.*

Example 1: Every fractional ideal $\mathfrak{a} \subseteq K$ of $\mathcal{O}$, in particular $\mathcal{O}$ itself, may be equipped with the **trivial metric**

$$\langle x, y\rangle = x\bar{y} = \bigoplus_{\sigma \in X(\mathbb{C})} x_\sigma \bar{y}_\sigma$$

on $\mathfrak{a} \otimes_{\mathcal{O}} \mathbb{C} = K \otimes_{\mathbb{Q}} \mathbb{C} = K_{\mathbb{C}}$. All the F-invariant hermitian metrics on $\mathfrak{a}$ are obtained as

$$\langle x, y\rangle_\alpha = \alpha x \bar{y} = \bigoplus_{\sigma} \alpha(\sigma) x_\sigma \bar{y}_\sigma ,$$

where $\alpha \in K_{\mathbb{R}}$ varies over the functions $\alpha : X(\mathbb{C}) \to \mathbb{R}_+^*$ such that $\alpha(\sigma) = \alpha(\bar\sigma)$.

Example 2: Let $L|K$ be a finite extension and $\mathfrak{A}$ a fractional ideal of L, which we view as an $\mathcal{O}$-module M. If $Y(\mathbb{C}) = \operatorname{Hom}(L, \mathbb{C})$, we have the restriction map $Y(\mathbb{C}) \to X(\mathbb{C})$, $\tau \mapsto \tau|_K$, and we write $\tau|\sigma$ if $\sigma = \tau|_K$. For the complexification $M_{\mathbb{C}} = \mathfrak{A} \otimes_{\mathcal{O}} \mathbb{C} = L_{\mathbb{C}}$ we obtain the decomposition

$$M_{\mathbb{C}} = \bigoplus_{\tau \in Y(\mathbb{C})} \mathbb{C} = \bigoplus_{\sigma \in X(\mathbb{C})} M_\sigma ,$$

where $M_\tau = \bigoplus_{\tau} \mathbb{C}$. M is turned into a metrized $\mathfrak{o}$-module by fixing the standard metrics

$$(x,y)_{M_\tau} = x\bar{y}$$

on the $(L:K)$-dimensional $\mathbb{C}$-vector spaces M_τ.

If M and M' are metrized $\mathfrak{o}$-modules, then so is their direct sum $M \oplus M'$, the tensor product $M \otimes M'$, the dual $\check{M} = \mathrm{Hom}_{\mathfrak{o}}(M, \mathfrak{o})$ and the n-th exterior power $\bigwedge^n M$. In fact, we have that

$$(M \oplus M')_{\mathbb{C}} = M_{\mathbb{C}} \oplus M'_{\mathbb{C}}, \quad (M \otimes_{\mathfrak{o}} M')_{\mathbb{C}} = M_{\mathbb{C}} \otimes_{K_{\mathbb{C}}} M'_{\mathbb{C}},$$

$$\check{M}_{\mathbb{C}} = \mathrm{Hom}_{K_{\mathbb{C}}}(M_{\mathbb{C}}, K_{\mathbb{C}}), \quad (\textstyle\bigwedge^n M)_{\mathbb{C}} = \bigwedge^n_{K_{\mathbb{C}}} M_{\mathbb{C}},$$

and the metrics on these $K_{\mathbb{C}}$-modules are given by

$$(x \oplus x', y \oplus y')_{M \oplus M'} = (x,y)_M + (x',y')_{M'}, \quad \text{resp.}$$

$$(x \otimes x', y \otimes y')_{M \otimes M'} = (x,y)_M\,(x',y')_{M'}, \quad \text{resp.}$$

$$(\check{x}, \check{y})_{\check{M}} = (x,y)_M, \quad \text{resp.}$$

$$(x_1 \wedge \dots \wedge x_n, y_1 \wedge \dots \wedge y_n)_{\bigwedge^n M} = \det((x_i, y_j)_M).$$

Here $\check{x}$, in the case of the module $M_{\mathbb{C}}$, denotes the homomorphism $\check{x} = (\ ,x)_M : M_{\mathbb{C}} \to K_{\mathbb{C}}$.

Among all $\mathfrak{o}$-modules M the projective ones play a special rôle. They are defined by the condition that for every exact sequence of $\mathfrak{o}$-modules $F' \to F \to F''$ the sequence

$$\mathrm{Hom}_{\mathfrak{o}}(M, F') \longrightarrow \mathrm{Hom}_{\mathfrak{o}}(M, F) \longrightarrow \mathrm{Hom}_{\mathfrak{o}}(M, F'')$$

is also exact. This is equivalent to any of the following conditions (the last two, because $\mathfrak{o}$ is a Dedekind domain). For the proof, we refer the reader to standard textbooks of commutative algebra (see for instance [90], chap. IV, §3, or [16], chap. 7, §4).

(4.3) Proposition. *For any finitely generated $\mathfrak{o}$-module M the following conditions are equivalent:*

(i) *M is projective,*

(ii) *M is a direct summand of a finitely generated free $\mathfrak{o}$-module,*

(iii) *M is locally free, i.e., $M \otimes_{\mathfrak{o}} \mathfrak{o}_{\mathfrak{p}}$ is a free $\mathfrak{o}_{\mathfrak{p}}$-module for any prime ideal $\mathfrak{p}$,*

(iv) *M is torsion free, i.e., the map $M \to M$, $x \mapsto ax$, is injective for all nonzero $a \in \mathfrak{o}$,*

(v) *$M \cong \mathfrak{a} \oplus \mathfrak{o}^n$ for some ideal $\mathfrak{a}$ of $\mathfrak{o}$ and some integer $n \geq 0$.*

In order to distinguish them from projective o-modules, we will henceforth call arbitrary finitely generated o-modules *coherent*. The **rank** of a coherent o-module M is defined to be the dimension

$$\operatorname{rk}(M) = \dim_K(M \otimes_o K).$$

The projective o-modules L of rank 1 are called **invertible** o-modules, because for them $L \otimes_o \check{L} \to o$, $a \otimes l \mapsto l(a)$, is an isomorphism. The invertible o-modules are either fractional ideals of K, or isomorphic to a fractional ideal of o-modules. Indeed, if L is projective of rank 1 and $a \in L$, $a \neq 0$, then, by (4.3), (iv), mapping

$$L \longrightarrow L \otimes_o K = K(a \otimes 1), \qquad x \longmapsto f(x)(a \otimes 1),$$

gives an injective o-module homomorphism $L \to K$, $x \mapsto f(x)$, onto a fractional ideal $\mathfrak{a} \subseteq K$.

To see the connection with the Riemann-Roch theory of the last section, which we are about to generalize, we observe that every replete ideal

$$\mathfrak{a} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{\nu_\mathfrak{p}} \prod_{\mathfrak{p} \mid \infty} \mathfrak{p}^{\nu_\mathfrak{p}} = \mathfrak{a}_f \mathfrak{a}_\infty$$

of K defines an invertible, metrized o-module. In fact, the identity $\mathfrak{a}_\infty = \prod_{\mathfrak{p} \mid \infty} \mathfrak{p}^{\nu_\mathfrak{p}}$ yields the function

$$a: X(\mathbb{C}) \longrightarrow \mathbb{R}_+, \quad a(\tau) = e^{2\nu_{\mathfrak{p}_\tau}},$$

where $\mathfrak{p}_\tau$ denotes as before the infinite place defined by $\tau : K \to \mathbb{C}$. Since $\mathfrak{p}_{\bar\tau} = \mathfrak{p}_\tau$, one has $a(\bar\tau) = a(\tau)$, and we obtain on the complexification

$$\mathfrak{a}_{f\mathbb{C}} = \mathfrak{a}_f \otimes_o \mathbb{C} = K_\mathbb{C}$$

the F-invariant hermitian metric

$$\langle x, y\rangle_\mathfrak{a} = a x \bar{y} = \sum_{\tau \in X(\mathbb{C})} e^{2\nu_{\mathfrak{p}_\tau}} x_\tau \bar{y}_\tau$$

(see example 1, p. 227). We denote the metrized o-module thus obtained by $L(\mathfrak{a})$.

The ordinary fractional ideals, i.e., the replete ideals $\mathfrak{a}$ such that $\mathfrak{a}_\infty = 1$, and in particular o itself, are thus equipped with the *trivial* metric $\langle x, y\rangle_\mathfrak{a} = (x, y) = x\bar{y}$.

(4.4) Definition. *Two metrized o-modules M and M' are called* **isometric** *if there exists an isomorphism*

$$f: M \longrightarrow M'$$

of o-modules which induces an isometry $f_\mathbb{C}: M_\mathbb{C} \to M'_\mathbb{C}$,

(4.5) Proposition.

(i) *Two* replete *ideah a and* b define *isometric* metrized *a-module;; L(a) and* L(b) *if and only if they* differ *by* a *replete principal ideal* [al: $a =$ bla].

(ii) *Every inverlib/e* metrizcd *o-module* is *isometric to* an o-module L(a).

(iii) L(ab) ;:;::: *L(a) ®o* l.(b), L(a-¹) = l(a).

Proof: (i) Let $\mathfrak a = \prod_{\mathfrak p} \mathfrak p^{\nu_{\mathfrak p}}$, $\mathfrak b = \prod_{\mathfrak p} \mathfrak p^{\mu_{\mathfrak p}}$, $[a] = \prod_{\mathfrak p} \mathfrak p^{\nu_{\mathfrak p}(a)}$, and let

$$\alpha(\sigma) = e^{2\nu_{\mathfrak p_\sigma}}, \quad \beta(\sigma) = e^{2\mu_{\mathfrak p_\sigma}}, \quad \gamma(\sigma) = e^{2\nu_{\mathfrak p_\sigma}(a)}.$$

If $a=$ bla], then J/p = /lp + Vp(a); thus $a=$ {3y, and ut = br(a). The a-module isomorphism b₁----+ar. *x* f--+ *a.t,* takes the form (.)b to the form (,)a, Indeed. viewing *a* as embedded in *Kc,* we find *a*= EB" *era* and

$$aii = \bigoplus_\sigma e^{-2\nu_{\mathfrak p_\sigma}(a)} = \gamma^{-1},$$

because l'p,,(a) = - log *iaal,* :;,o that

(ax .ay)a = *a(ax, ay)* = ay-¹(x y)=fJ{x, y) = (,·, Y)o.

Therefore b₁----+ur, *x* r-'1- *ax,* gives an isometry L(a) ;:;::: *L(b).*

Convcrc;ely, let *f,;* : L(b) ---+ *L(a)* be an isometry. Then the a-module homomorphism

J.;: br----+ a1

b given as multiplication by some element *a* E bt ¹u₁ � Hom (b . u). The identity

$$\beta\langle x, y\rangle = \langle x, y\rangle_{\mathfrak b} = \langle g(x), g(y)\rangle_{\mathfrak a} = \alpha\langle ax, ay\rangle = \alpha\gamma^{-1}\langle x, y\rangle$$

then implie& that $a=$ *fly,* so that *Vp* = *f.-Lp* + i•p(a) for all ploo. In view of u₁ = br(a), this yields u = blaJ.

(ii) Let *L* be an invertible metrized o-module. A� mentioned before, we have an isomorphi5tn

g:L-;. u₁

for the underlying o-module onto a fractional ideal ur. The isomorphism *L1:,* ---+ u₁c = *Kr:* gives us the F-invariant hermitian metric = (g(:¹Ct),g,C¹(y))L on *K,c.11* i� of the form

h(x,y) = *crx.V*

for some function a: X(C)---+ JR� &uch that *a(O)* = a(a). Putting now a(a) = *e²vp..,,* with *vp,,* E IR, makes ur with the metric *h* into the metrized a-module *L(a)* ar,sociated to the replete ideal a= llt TTP$_{100^{pl'p,}}$ and Lis bometric to *L(a).*

(iii) Let a= nplJvP, b = TTpt:i$^{1"P,}$ *a(a)* = e^{2}"P'1", *f3(a)* = *e*$^{2'''''}$. The isomorphism

a1®$_0$b1----+a1b1, *a@hf*--------,,*ah,*

between the o-modules underlying *L(a) @$_o$ L(b)* and *L(ab)* then yields, as *(ah,a'h')ah = afjaha'h' = a{a,a^1)fl{h,h^1)* = {a,a')a(h,h')D, an isometry L(a) ®*o* L(b) "' L(ob).

The a-module Hom$_0$(a$_1$. o) underlying Lea) is isomorphic. via the isomorphir,m

g:a;^{1}----+Hom$_0$(a1,0), af----------,,(g(a):x1---c>-a.\).

to the fractional ideal af^1. For the induced Kr:-isomorphir,m

g,c: K,c----+ HomK$_1$,(Kc, Kd

we have

$$g_{\mathbb{C}}(x)(y) = xy = \alpha^{-1}\alpha xy = \alpha^{-1}\langle y, \bar{x}\rangle_{L(\mathfrak{a})},$$

so that ,:�*(x)* = a-^{1}.f.and thur,

(,:c(x), *g,c(y))* i.(al = a-2(.f. *y')*i.(al = 0'-2 (X,.Dual

= *a-^{1}xf* = (x *Y)L(a* 11.

Thus *g* gives an ir,ometry Lea) ;;::: L(a-^{1}). □

(4.6) Definition. ***A* short exact sequence**

0 ----+ *M'* � *M* � *M"*--- + 0

of metrized *o-modules* ir, *by dclinition a short* exact �equence of the *underlying v-modules which .<.plits isometrically,* i.e., *in* the *sequence*

0----+ *M*�� *M*�� *M*� ----+ 0,

M�. ir, mapped ir,omclrical/y *onto* *and* the *orthogonal* complement *(a,cM*�)^1 *is* mapped *isometrically onto*

The homomorphisms *a. fJ* in a short exact sequence of metriLed o-module5 are called an **admissible monomorphism,** resp. **epimorphism.**

To each projective metrized a-module *M* ir, associated its **determinant** det *M,* an invertible metriLed a-module. The detcm1inant is the highest exterior power of *M,* i.e.,

detM = */\/'M,* *n* = rk(M).

(4.7) Proposition. *If $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ is a short exact sequence of projective metrized $\mathfrak{o}$-modules, we have a canonical isometry*

$$\det M' \otimes_{\mathfrak{o}} \det M'' \cong \det M.$$

Proof: Let $n' = \mathrm{rk}(M')$ and $n'' = \mathrm{rk}(M'')$. We obtain an isomorphism

$$\kappa : \det M' \otimes_{\mathfrak{o}} \det M'' \longrightarrow \det M$$

of projective $\mathfrak{o}$-modules of rank 1 by mapping

$$(m'_1 \wedge \ldots \wedge m'_{n'}) \otimes (m''_1 \wedge \ldots \wedge m''_{n''}) \mapsto \alpha m'_1 \wedge \ldots \wedge \alpha m'_{n'} \wedge m_1 \wedge \ldots \wedge m_{n''},$$

where $m_1, \ldots, m_{n''}$ are preimages of $m''_1, \ldots, m''_{n''}$ under $\beta : M \to M''$. This mapping does not depend on the choice of preimages, for if, say, $m_1 + \alpha m'_{n'+1}$, where $m'_{n'+1} \in M'$, is another preimage of m''_1 then

$$\begin{aligned} \alpha m'_1 \wedge \ldots \wedge \alpha m'_{n'} \wedge (m_1 + \alpha m'_{n'+1}) \wedge m_2 \wedge \ldots \wedge m_{n''} \\ = \alpha m'_1 \wedge \ldots \wedge \alpha m'_{n'} \wedge m_1 \wedge \ldots \wedge m_{n''} \end{aligned}$$

since $\alpha m'_1 \wedge \ldots \wedge \alpha m'_{n'} \wedge \alpha m'_{n'+1} = 0$. We show that the $\mathfrak{o}$-module isomorphism κ is an isometry. According to the rules of multilinear algebra it induces an isomorphism

$$\kappa : \det M'_{\mathbb{C}} \otimes_{K_{\mathbb{C}}} \det M''_{\mathbb{C}} \xrightarrow{\sim} \det M_{\mathbb{C}}$$

of $K_{\mathbb{C}}$ modules. Let $x'_i, y'_i \in M'_{\mathbb{C}}$, $i = 1, \ldots, n'$, and $x_j, y_j \in \alpha M'^{\perp}_{\mathbb{C}}$, $j = 1, \ldots, n''$, and furthermore

$$x' = \wedge_i x'_i, \quad y' = \wedge_i y'_i, \quad x = \wedge_j x_j, \quad y = \wedge_j y_j.$$

Then we have

$$\begin{aligned} (\kappa(x' \otimes \beta x), \kappa(y' \otimes \beta y))_{\det M} &= (\alpha x' \wedge x, \alpha y' \wedge y)_{\det M} \\ &= \det \begin{pmatrix} (\alpha x'_i, \alpha y'_k)_M & 0 \\ 0 & (x_j, y_l)_M \end{pmatrix} \\ &= \det((x'_i, y'_k)_{M'}) \det((\beta x_j, \beta y_l)_{M''}) \\ &= (x', y')_{\det M'} (\beta x, \beta y)_{\det M''} \\ &= (x' \otimes \beta x, y' \otimes \beta y)_{\det M' \otimes \det M''}. \end{aligned}$$

Thus κ is an isometry. □

Exercise 1. If M, N, L are metrized $\mathfrak{o}$-modules, then one has canonical isometries

$$M \otimes_{\mathfrak{o}} N \cong N \otimes_{\mathfrak{o}} M, \quad (M \otimes_{\mathfrak{o}} N) \otimes_{\mathfrak{o}} L \cong M \otimes_{\mathfrak{o}} (N \otimes_{\mathfrak{o}} L),$$

$$M \otimes_{\mathfrak{o}} (N \oplus L) \cong (M \otimes_{\mathfrak{o}} N) \oplus (M \otimes_{\mathfrak{o}} L).$$

Exercise 2. For any two projective metrized $\mathfrak{o}$-modules M, N, one has

$$\bigwedge^{n}(M \oplus N) \cong$$

Exercise 3. For any two projective metrized $\mathfrak{o}$-modules M, N, one has

$$\det(M \otimes_{\mathfrak{o}} N) \cong (\det M)^{\otimes \operatorname{rk}(N)} \otimes_{\mathfrak{o}} (\det N)^{\otimes \operatorname{rk}(M)}.$$

Exercise 4. If M is a projective metrized $\mathfrak{o}$-module of rank n, and $p \geq 0$, then there is a canonical isometry

$$\det(\bigwedge^{p} M) \cong (\det M)^{\otimes \binom{n-1}{p-1}}$$

§5. Grothendieck Groups

We will now manufacture two abelian groups from the collection of all metrized $\mathfrak{o}$-modules, resp. the collection of all projective metrized $\mathfrak{o}$-modules. We denote by $\{M\}$ the isometry class of a metrized $\mathfrak{o}$-module M and form the free abelian group

$$F_0(\bar{\mathfrak{o}}) = \bigoplus_{\{M\}} \mathbb{Z}\{M\}, \quad \text{resp.} \quad F^0(\bar{\mathfrak{o}}) = \bigoplus_{\{M\}} \mathbb{Z}\{M\},$$

on the isometry classes of projective, resp. coherent, metrized $\mathfrak{o}$-modules. In this group, we consider the subgroup

$$R_0(\bar{\mathfrak{o}}) \subseteq F_0(\bar{\mathfrak{o}}), \quad \text{resp.} \quad R^0(\bar{\mathfrak{o}}) \subseteq F^0(\bar{\mathfrak{o}}),$$

generated by all elements $\{M'\} - \{M\} + \{M''\}$ which arise from a short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of projective, resp. coherent, metrized $\mathfrak{o}$-modules.

(5.1) Definition. *The quotient groups*

$$K_0(\bar{\mathfrak{o}}) = F_0(\bar{\mathfrak{o}})/R_0(\bar{\mathfrak{o}}), \quad \text{resp.} \quad K^0(\bar{\mathfrak{o}}) = F^0(\bar{\mathfrak{o}})/R^0(\bar{\mathfrak{o}})$$

are called the **replete** (*or* **compactified**) **Grothendieck groups** *of* $\mathfrak{o}$. *If M is a metrized $\mathfrak{o}$-module, then $[M]$ denotes the class it defines in $K_0(\bar{\mathfrak{o}})$, resp. $K^0(\bar{\mathfrak{o}})$.*

The construction of the Grolhcndieck groups is such that a short exact sequence

$$0\text{------+}\ M'\text{------+}\ M\text{------+}\ M''\text{------- +}0$$

of metrized o-module,; becomc5 an additive decomposition in the group:

$$[M] � [M'] + [M''].$$

In particular, one has

$$[M' \text{EB}\ M''] \ � \ [M'] + [M''J.$$

The tensor product even induces a ring structure on $K_0(8)$. and $K^0(E5)$ then becomes a $K_0(8)$-module: extending lhe product

$$[M)[M') :� \{M \, 0_o \, M')$$

by linearity. and observing that $N ® M$;:,: $M ® N$ and $(M ® N) ® L$ _ $M ®(N ®L)$, we find right away that $F^0(8)$ is a commulativc ring and is a subring. Furthennore the �ubgroups $R_0(Ci)$ c;;;: $Fo(8)$ and $R^0(0)$ c;;;: turn out to be $F_0(8)$-5ubmodule�. For if

$$0\text{ ------+ }M'\text{ ------+ }M\text{ ------+ }M''\text{ ------+ }0$$

is a short exact sequence of coherent mclrizcd CJ-modules, and N is a projective mctri1:cd o-module, then it is clear that

$$0\text{ ------+ }N ® M'\text{ ------+ }N ® M\text{ ------+ }N ® M''\text{ ------+ }0$$

is a short exact sequence of mctri1:cd o-modules as well, so that. along with a generator $\{M^1) - \{Ml+ \{M^{11}\}$, the element

$$\{NJ(\{M') - \{M) + \{M''J) � \{N0M') - \{N\,OM) + \{NOM'')$$

will also belong to $R_0(0)$, resp. $R^0(8)$. This i5 why $K_0(i5) = F_0(8)/R_0(8)$ is a ring and $K^0(0) = F^0(i{:}5)/R^0(0)$ is a $K_0(8)$-module.

Associating to the class [M] of a projective CJ-module Min $K_0(8)$ its cla1,,,; in $K^0(0)$ (which again is denoted by [MJ), dctinc5 a homomorphism

$$Ko(i.5)\text{ ----+ }K^0(i5).$$

It is called the **Poincare homomorphism.** We will show next that the Poincare homomorphi�m is an iwmorphism. The proof is based on the following two lemmas.

(5.2) **Lemma.** *All rnherent* metrized *o-modulcs M i.ldmit* a "merrized *projective rc,;o/ulion*", *i.e.*, ;1 shmt exact 8equence

$$0\text{------+}E\text{------+}F\text{------+}M\text{-------+}O$$

of *metrized* CJ-modules *in which f,'* and *F* arc *projective.*

Proof: If $a_1,\ \ ,a''$ is a system of generators of M, and F is the free o-module $F = o'^1$, then

$$F\text{-----+ } M, \quad (x_1, \dots x,,) \text{ i-------+ } Lx,a1,$$
$$1=1$$

is a surjective o-module homomorphism. Its kernel E is torsion free. and hence a projective o-module by (4.3). In the exact sequence

$$0 \text{ -----+ } Ee \text{ -----+ } F:: \quad Mc \text{ -----+ } 0.$$

we choose a section- : *M": --+ Fe* of J, so that *F": = E{: EBsM1_·*. We obtain a metric on *F,c* by transferring the metric of *Mc* to *sM,c*, and by choosing any metric on *Ee*. This makes O --+ R --+ F --+ M --+ 0 into a short exact sequence of metrized a-modules in which E and F are projective. LJ

In a diagram of metrized projective resolutions of M

$$O\text{-----+}E\text{--+}F\text{--+}M\text{---------+}O$$
$$1 \qquad 1$$
$$0 \text{ -----+ } f,\text{-}, \text{ --+ } \quad F' \text{ --+ } \quad M \text{------+ } 0$$

the reolution in the top line will be called *dominant* if the vertical arrow are admissible epimorphisms.

(5.3) **Lemma.** *Let*

$$0\text{-----+ } E' \text{ -----+ } F' \ L \ M \text{ -----+ } 0, \qquad 0\text{-----+ } E'' \text{ -----+ } F'' \ ..!:.+ \ M\text{------+ } 0$$

be rwo *metrized projective* reso/u1iom of *the metri7ed o-module M. Then, laking the o-module*

$$F \ F' \ {}_{XM} \ F'' \ \backslash (x',x'') \in F' \times F'' \mid [(x'J \ f''(x''i)$$

and *the mapping* f: *F--+ M, (x',x'')* r--+ *f'(x'*, = *j* '(x''), *one* oblains *a third melriLed projective re.rnlution*

$$0\text{-----+}E\text{-----+}F\text{-----+}M\text{------+}0$$

with kernel $E = £' \times £^{11}$ *which domimlle. both* given *one.*

Proof: Since $F' \oplus F''$ is projective, so is F, being the kernel of the homomorphism $F' \oplus F'' \to M$. Thus E is also projective, being the kernel of $F \to M$. We consider the commutative diagram

$$\begin{tikzcd}
 & & F'_{\mathbb C} \arrow[r, shift left, "f'"] & M_{\mathbb C} \arrow[l, dashed, shift left] \arrow[r] & 0 \\
0 \arrow[r] & E_{\mathbb C} \arrow[u] \arrow[d] \arrow[r] & F_{\mathbb C} \arrow[u] \arrow[d] \arrow[r, shift left] & M_{\mathbb C} \arrow[l, shift left] \arrow[r] & 0 \\
0 \arrow[r] & E''_{\mathbb C} & F''_{\mathbb C} \arrow[r, shift left] & M_{\mathbb C} \arrow[l, shift left] \arrow[r] & 0.
\end{tikzcd}$$

where the vertical arrows are induced by the surjective projections

$$F \to F', \quad F \to F''.$$

The canonical isometries

$$s' : M_{\mathbb C} \longrightarrow s'M_{\mathbb C}, \quad s'' : M_{\mathbb C} \longrightarrow s''M_{\mathbb C}$$

give a section

$$s : M_{\mathbb C} \longrightarrow F_{\mathbb C}, \quad sx = (s'x, s''x),$$

of F which transfers the metric on to a metric on $sM_{\mathbb C}$. $F_{\mathbb C} = \times$ carries the sum of the metric, of $F''_{\mathbb C}$, so that $F_{\mathbb C} = E_{\mathbb C} \oplus$ also receives a metric, and

$$0 \longrightarrow E \longrightarrow F \longrightarrow M \longrightarrow 0$$

becomes a metrized projective resolution of M. It is trivial that the projections $E \to E'$ and $E \to E''$ are admissible epimorphisms, and it remains to show this for the projections $\pi' : F \to F'$, $\pi'' : F \to F''$. But we clearly have the exact sequence of $\mathfrak o$-modules

$$0 \longrightarrow E'' \xrightarrow{\ i\ } F = F' \times_M F'' \xrightarrow{\ \pi'\ } F' \longrightarrow 0,$$

where $ix'' = (0, x'')$. As the restriction of the metric of F to $E = E' \times E''$ is the sum of the metrics on E' and E'', we see that $i : E''_{\mathbb C} \to iE''_{\mathbb C}$ is an isometry. The orthogonal complement of $iE''_{\mathbb C}$ in $F_{\mathbb C}$ is the space

$$F'_{\mathbb C} \times_{M_{\mathbb C}} s''M_{\mathbb C} = \{(x', s''a) \in F'_{\mathbb C} \times s''M_{\mathbb C} \mid f'(x') = a\}.$$

Indeed, on the one hand it is clearly mapped bijectively onto $F'_{\mathbb C}$, and on the other hand it is orthogonal to $iE''_{\mathbb C}$. For if we write $x' = s'a + e'$ with $e' \in E'_{\mathbb C}$, then

$$(.r^1, s^{11}a) = sa + (e^{\prime}, 0).$$

where $(e',0)\in E_{\mathbb{C}}$ and we find that, for all $e\in E'_{\mathbb{C}}$,

$$((e,0),(x',s''a))_F = ((0,x''),(e,0))_F + ((0,x''),(e,0))_E = 0.$$

Finally, the projection $F'_{\mathbb{C}}\times_{M_{\mathbb{C}}} s''M_{\mathbb{C}}\to F'_{\mathbb{C}}$ is an isometry, for if $(x',s''a)$, $(y',s''b)\in F'_{\mathbb{C}}\times_{M_{\mathbb{C}}} s''M_{\mathbb{C}}$ and $x'=s'a+e'$, $y'=s'b+d'$, with $e',d'\in E'_{\mathbb{C}}$, then we get

$$(x',s''a)=sa+(e',0),\qquad (y',s''b)=sb+(d',0)$$

and

$$\begin{aligned}((x',s''a),(y',s''b))_F &= (sa,sb)_F+(sa,(d',0))_F+((e',0),sb)_F\\ &\quad +((e',0),(d',0))_E\\ &= (a,b)_M+(e',d')_{E'}=(s'a,s'b)_{F'}+(e',d')_{E'}\\ &= (s'a+e',s'b+d')_{F'}=(x',y')_{F'}.\end{aligned}$$ $\square$

(5.4) Theorem. *The Poincaré homomorphism*

$$K_0(\overline{\mathcal{O}})\to K^0(\overline{\mathcal{O}})$$

is an isomorphism.

Proof: We define a mapping

$$\pi: K^0(\overline{\mathcal{O}})\to K_0(\overline{\mathcal{O}})$$

by choosing, for every coherent metrized $\mathcal{O}$-module $\overline{M}$, a metrized projective resolution

$$0\to\overline{E}\to\overline{F}\to\overline{M}\to 0$$

and associating to the class $[\overline{M}]$ in $K^0(\overline{\mathcal{O}})$ the difference $[\overline{F}]-[\overline{E}]$ of the classes $[\overline{F}]$ and $[\overline{E}]$ in $K_0(\overline{\mathcal{O}})$. To see that this mapping is well-defined let us first consider a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \overline{E} \arrow[r] \arrow[d, "\alpha"] & \overline{F} \arrow[r] \arrow[d, "\beta"] & \overline{M} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & \overline{E}' \arrow[r] & \overline{F}' \arrow[r] & \overline{M} \arrow[r] & 0 \end{tikzcd}$$

of two metrized projective resolutions of $\overline{M}$, with the top one dominating the bottom one. Then $E\to F$ induces an isometry $\ker(\alpha)\cong\ker(\beta)$, so that we get

$$[\overline{F}]-[\overline{E}]=[\overline{F}']+[\ker(\beta)]-[\overline{E}']-[\ker(\alpha)]=[\overline{F}']-[\overline{E}'].$$

have the following identity in $K_0(8)$:

If now $0 \to E' \to F' \to M \to 0$, and $0 \to E'' \to F'' \to M \to 0$ are two arbitrary metrized projective resolutions of M, then by (5.3) we find a third one, $0 \to E \to F \to M \to 0$, dominating both, such that

$$[F'] - [E'] = [F] - [E] = [F''] - [E''] .$$

This shows that the map $\pi : F^0(\bar{\mathcal{O}}) \to K_0(\bar{\mathcal{O}})$ is well-defined. We now show that it factorizes via $K^0(\bar{\mathcal{O}}) = F^0(\bar{\mathcal{O}})/R^0(\bar{\mathcal{O}})$. Let $0 \to M' \to M \xrightarrow{\alpha} M'' \to 0$ be a short exact sequence of metrized coherent $\bar{\mathcal{O}}$-modules. By (5.2), we can pick a metrized projective resolution $0 \to E \to F \xrightarrow{f} M \to 0$. Then clearly $0 \to E'' \to F \xrightarrow{f''} M'' \to 0$ is a short exact sequence of metrized $\bar{\mathcal{O}}$-modules as well, where we write $f'' = \alpha \circ f$ and $E'' = \ker(f'')$. We thus get the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E & \longrightarrow & F & \xrightarrow{f} & M & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & E'' & \longrightarrow & F & \xrightarrow{f''} & M'' & \longrightarrow & 0
\end{array}$$

and the snake lemma gives the exact sequence of $\bar{\mathcal{O}}$-modules

$$0 \longrightarrow E \longrightarrow E'' \xrightarrow{f} M' \longrightarrow 0 .$$

It is actually a short exact sequence of metrized $\bar{\mathcal{O}}$-modules, for $E_{\mathfrak{p}}$ is mapped isometrically by f onto $M_{\mathfrak{p}}$, so that $E''_{\mathfrak{p}}$ is mapped isometrically by f onto $M'_{\mathfrak{p}}$. We therefore obtain in $K_0(\bar{\mathcal{O}})$ the identity

$$\pi(M') - \pi(M) + \pi(M'') = [E''] - [E] - ([F] - [E]) + [F] - [E''] = 0 .$$

It shows that $\pi : F^0(\bar{\mathcal{O}}) \to K_0(\bar{\mathcal{O}})$ does indeed factorize via a homomorphism

$$K^0(\bar{\mathcal{O}}) \to K_0(\bar{\mathcal{O}}) .$$

It is the inverse of the Poincaré homomorphism because the composed maps

$$K_0(\bar{\mathcal{O}}) \to K^0(\bar{\mathcal{O}}) \to K_0(\bar{\mathcal{O}}) \quad \text{and} \quad K^0(\bar{\mathcal{O}}) \to K_0(\bar{\mathcal{O}}) \to K^0(\bar{\mathcal{O}})$$

are the identity homomorphisms. Indeed, if $0 \to E \to F \to M \to 0$ is a projective resolution of M, and M is projective, resp. coherent, then in $K_0(\bar{\mathcal{O}})$, resp. $K^0(\bar{\mathcal{O}})$, one has the identity $[M] = [F] - [E]$. □

The preceding theorem shows that the Grothendieck group $K_0(\bar{\mathcal{O}})$ does not just accommodate all projective metrized $\bar{\mathcal{O}}$-modules, but in fact all coherent metrized $\bar{\mathcal{O}}$-modules. This fact has fundamental significance. For when dealing with projeclive modules, one is led very quickly to non-projective modules, for instance, to the residue class rings o/a. The corresponding classes in $K^0(i5)$, however, can act out their important r6let> only inside the ring $K_0(8)$, because only this ring can be immediately subjected to a more advanced theory.

The following relationship holds bclween the Grothendieck ring $K_0(E5)$ and the replete Picard group *Pic(i5),* which was intrcx:luced in §1.

(5.5) Proposition. *Associating to* a *replete ideal* a of *K the metrizcd o-module L(a) yields a homomorphism*

$$Pic(8) \to K_0(8)^*, \quad [a] \mapsto [L(o)].$$

into the unit group of the ring $K_0(8)$.

Proof: The correspondence $[a] \mapsto [L(a)]$ is independent of the choice of a replete ideal a inside the class [al E *Pic(i5).* Indeed, if b is another representative, then we have a= b[a], for some replete principal ideal la), and the metrized tJ-modules L(a) and *L(b)* are isometric by (4.5), (i), sothat *fL(a)]* = [L(b)]. The correspondence is a multiplicative homomorphi�m as

$$[L(nb)I � [L(n)0_o \; L(b)I � JL(n)][L(b)J. \qquad \square$$

In the sequel. we simply denote the class of a metrized invertible tl-module *L(a)* in $K_0(8)$ by [aj. In particular, to the replete ideal tJ = TIP p^0 correspond� the class $1 = [o]$ of the a-module *o* equipped with the lrivial metric.

(5.6) Proposition. $K_0(i5)$ is generated m, m1 additive *group by the element.* � la].

Proof: Let *M* be a projective metrized tJ-module. By (4.3), the underlying a-module admits a� quotient a fractional ideal a_1, i.e., we have an exact �equence

$$0 \to N \to M \to a_1 \to 0$$

of o-module�. This hecomes an exact sequence of metrized o-modulc1, once we restrict the metric from *M* to *N* and choose on a_1 the metric which is tram,fcrred via the isomorphism *Ni:* ::::::: or::- Thus a_1 becomes the metri?ed o-modulc *L(a)* corre<,ponding to the replete ideal a of *K,* �o that we get the identity [Ml= IN]+ lo] in $K_0(8)$. Induction on the rank shows that for every projeclive mctrized o-module *M,* there b a deeompo�ition

$$[Ml= ra, l + \cdots + lo,J.$$ □

The elemenli,, lo] in *K0({))* satisfy the following remarkable relation.

(5.7) **Proposition.** *For* w1y *two replete ideals a and* b of *K* we *have in* K0(8) *the* equation

$$(lal - l)(lbl - I)� 0.$$

Proof *(T4MMI:*): For every function *a* : *X* (IC) ----+ let ui,, consider on the Kc-module *Kc=* ffioEX(t:J the form

$$axy = ffia(a)xo5'o.$$

For every matrix *A* = (� �) of :,,uch functions, we con:,,ider on the K:::-module *Kc_*· EB *Kr:* the form

$$(x \text{ EB } y,x' \text{ EB } y')A = a,X' + yx\_v' + OyX' + fiyy'$$

a, Y, rc5p. { ,) *A,* is an *F* -invariant metric on *Ke,,* resp. on *K*:· EB *Kc,* if and only if *a* is F-invariant (i.e., *a(a)* = a(a")) and *a(a)* E rc:,,p. if all the functions *a, /3, y, 8* arc F-invariant, *a(a),* /J(a) E JR: and = *y,* and if moreover <let *A* = *afi* - *yy* > 0. We now assume this in what follows.

Let *a* and b be fractional ideals of *K.* We have to prove the formula

$$lal + lbl � labl +I.$$

We may assume that a_1 and b_1 are *inteiral* ideab to one another, because if nccc%ary we may pass to replete *a' = a[al,* b' = b[hj with corresponding ideals O; = *a₁a,* b; = b₁h without changing the cla%es lo], [b], [abl in $K_0(0)$. We denote the CJ-module a_1· when mctrized by *ax_v,* by *(a1.a),* and the o-module 111 EB b_1· metri1:ed by (,)4, for A=(; �),by(orEBb1,A).GivenanytwomatricesA= (; ;) and A• = (a'Y ' /3'), we wn•te

$$A\sim A',$$

if [(o_1 EB bi), A]= [(a_1 EB bt), A'] in $K_0(8)$. We no\¼ consider the canonical exact sequence

$$0\text{------+ Ot--------'?- Ot EB b1 ------+ bf------+ 0.}$$

Once we equip $\mathfrak{a}_\mathfrak{f}\oplus\mathfrak{b}_\mathfrak{f}$ with the metric $(\ ,\ )_A$ which is given by $A = \begin{pmatrix}\alpha & \gamma\\ \bar\gamma & \beta\end{pmatrix}$, we obtain the following exact sequence of metrized $\mathfrak{o}$-modules:

$$(*)\qquad 0 \longrightarrow (\mathfrak{a}_\mathfrak{f},\alpha) \longrightarrow (\mathfrak{a}_\mathfrak{f}\oplus\mathfrak{b}_\mathfrak{f}, A) \longrightarrow \Big(\mathfrak{b}_\mathfrak{f}, \beta - \frac{\gamma\bar\gamma}{\alpha}\Big) \longrightarrow 0$$

Indeed, in the exact sequence

$$0 \longrightarrow K_\mathfrak{f} \longrightarrow K_\mathfrak{f}\oplus K_\mathfrak{f} \longrightarrow K_\mathfrak{f} \longrightarrow 0,$$

the restriction of $(\ ,\ )_A$ to $K_\mathfrak{f}\oplus\{0\}$ yields the metric $\alpha x\bar y$ on $K_\mathfrak{f}$, and the orthogonal complement V of $K_\mathfrak{f}\oplus\{0\}$ consists of all elements $a\oplus b\in K_\mathfrak{f}\oplus K_\mathfrak{f}$ such that

$$(x\oplus 0, a\oplus b)_A = \alpha x\bar a + \gamma x\bar b = 0,$$

for all $x\in K_\mathfrak{f}$, so that

$$V = \{(-\bar\gamma/\alpha)b\oplus b \mid b\in K_\mathfrak{f}\}.$$

The isomorphism $V \to K_\mathfrak{f}$, $(-\bar\gamma/\alpha)b\oplus b\mapsto b$, transfers the metric $(\ ,\ )_A$ on V into the metric $\delta x\bar y$, where δ is determined by the rule

$$\delta = (\pi^{-1}(1),\pi^{-1}(1))_A = ((-\bar\gamma/\alpha)1\oplus 1, (-\bar\gamma/\alpha)1\oplus 1)_A$$

$$= \alpha\frac{\bar\gamma\gamma}{\alpha\alpha} - \gamma\frac{\bar\gamma}{\alpha} - \bar\gamma\frac{\gamma}{\alpha} + \beta = \beta - \frac{\gamma\bar\gamma}{\alpha}.$$

This shows that (*) is a short exact sequence of metrized $\mathfrak{o}$-modules, i.e.,

$$\begin{pmatrix}\alpha & \gamma\\ \bar\gamma & \beta\end{pmatrix} \sim \begin{pmatrix}\alpha & 0\\ 0 & \beta - \frac{\gamma\bar\gamma}{\alpha}\end{pmatrix}.$$

Replacing β by $\beta + \frac{\gamma\bar\gamma}{\alpha}$, we get

$$\begin{pmatrix}\alpha & \gamma\\ \bar\gamma & \beta + \frac{\gamma\bar\gamma}{\alpha}\end{pmatrix} \sim \begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}.$$

Applying the same procedure to the exact sequence $0 \to \mathfrak{b}_\mathfrak{f} \to \mathfrak{a}_\mathfrak{f}\oplus\mathfrak{b}_\mathfrak{f} \to \mathfrak{a}_\mathfrak{f} \to 0$ and the metric $\begin{pmatrix}\alpha' & \gamma\\ \bar\gamma & \beta'\end{pmatrix}$ on $\mathfrak{a}_\mathfrak{f}\oplus\mathfrak{b}_\mathfrak{f}$, we obtain

$$\begin{pmatrix}\alpha' + \frac{\gamma\bar\gamma}{\beta'} & \gamma\\ \bar\gamma & \beta'\end{pmatrix} \sim \begin{pmatrix}\alpha' & 0\\ 0 & \beta'\end{pmatrix}.$$

Choosing

$$\beta' = \beta + \frac{\gamma\bar\gamma}{\alpha},\qquad \alpha' = \frac{\alpha\beta}{\beta'},$$

makes the matrices on the left equal, and yields

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \Bigg($$

or, ifwe put8 = /J + 1!,.

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\delta} & 0 \\ 0 & \delta \end{pmatrix},$$

which is valid for any F-invariant function 8 : X (C) → Ill f>Uch that 8 :::_ fi. This implie5 furthermore

$$\begin{pmatrix} \frac{\alpha\beta}{\delta} & 0 \\ 0 & \delta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\varepsilon} & 0 \\ 0 & \varepsilon \end{pmatrix}$$

for any two F-invariant functioni,, 8,£ : X (C) → For if κ: X(C) → E. is an F-invariant function such that κ 2: 8, κ 2: F, (**) gives

$$\begin{pmatrix} \frac{\alpha\beta}{\delta} & 0 \\ 0 & \delta \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\kappa} & 0 \\ 0 & \kappa \end{pmatrix} \sim \begin{pmatrix} \frac{\alpha\beta}{\varepsilon} & 0 \\ 0 & \varepsilon \end{pmatrix}$$

Now putting 8 = f3and F' = I in(***), we **Jind**

$$[(\mathfrak{a}_f, \alpha)] + [(\mathfrak{b}_f, \beta)] = [(\mathfrak{a}_f, \alpha\beta)] + [\mathfrak{b}_f].$$

For the replete ideals a= np p1'p' b = np pVp, this means

(1) $$[\mathfrak{a}] + [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}_\infty] + [\mathfrak{b}_f],$$

for if we put a(a) = e2vP<,, fi(a) = c2μP", then we have

(ar,a) = L(a), (b1,/3) = L(b). (or,a/J) = /,(ob:x,)-

On the other hand. we obtain the formula

(2) [al+ [b,l � [ab,I + I

in the following manner. We have two exact sequence'> of (ohcrcnt metrized o-modulc<,:

$$0 \longrightarrow (\mathfrak{a}_f\mathfrak{b}_f, \alpha) \longrightarrow (\mathfrak{a}_f, \alpha) \longrightarrow \mathfrak{a}_f/\mathfrak{a}_f\mathfrak{b}_f \longrightarrow 0,$$

$$0 \longrightarrow (\mathfrak{b}_f, 1) \longrightarrow (\mathcal{O}, 1) \longrightarrow \mathcal{O}/\mathfrak{b}_f \longrightarrow 0.$$

A5 ctr and b1 are relatively prime, i.e., 0t + b1 = ci. it follows that

$$\mathfrak{a}_{\mathfrak{f}}/\mathfrak{a}_{\mathfrak{f}}\mathfrak{b}_{\mathfrak{f}} \longrightarrow \mathcal{O}/\mathfrak{b} \qquad \blacksquare$$

is an isomorphism, so that in the group $K^0(\bar{\mathcal O})$ one has the identity $[\mathfrak a \oplus \mathfrak b] = [\mathfrak a\mathfrak b \oplus \mathcal O]$, and therefore

$$[(\mathfrak a_\infty, \mathfrak a)] - [(\mathfrak a\mathfrak b_\infty, \mathfrak a)] = [(\mathcal O, 1)] - [(\mathfrak b_\infty, 1)],$$

and so

$$[\mathfrak a] - [\mathfrak a\mathfrak b_\infty] = 1 - [\mathfrak b_\infty].$$

From (1) and (2) it now follows that

$$[\mathfrak a] + [\mathfrak b] = [\mathfrak a\mathfrak b_\infty] + [\mathfrak b_f] = [\mathfrak a\mathfrak b_\infty\mathfrak b_f] + 1 = [\mathfrak a\mathfrak b] + 1.$$

In view of the isomorphism $K_0(\bar{\mathcal O}) \cong K^0(\bar{\mathcal O})$, this is indeed an identity in $K_0(\bar{\mathcal O})$. □

§ 6. The Chern Character

The Grothendieck ring $K_0(\bar{\mathcal O})$ is equipped with a canonical surjective homomorphism

$$\mathrm{rk}: K_0(\bar{\mathcal O}) \longrightarrow \mathbb Z.$$

Indeed, the rule which associates to every isometry class $\{M\}$ of projective metrized $\mathcal O$-modules the rank

$$\mathrm{rk}\{M\} = \dim_K(M \otimes_{\mathcal O} K)$$

extends by linearity to a ring homomorphism $F_0(\bar{\mathcal O}) \to \mathbb Z$. For a short exact sequence $0 \to M' \to M \to M'' \to 0$ of metrized $\mathcal O$-modules one has $\mathrm{rk}(M) = \mathrm{rk}(M') + \mathrm{rk}(M'')$, and so $\mathrm{rk}(\{M\} - \{M'\} - \{M''\}) = 0$. Thus rk is zero on the ideal $R_0(\bar{\mathcal O})$ and induces therefore a homomorphism $K_0(\bar{\mathcal O}) \to \mathbb Z$. It is called the **augmentation** of $K_0(\bar{\mathcal O})$ and its kernel $I = \ker(\mathrm{rk})$ is called the **augmentation ideal.**

(6.1) Proposition. *The ideal I, resp. I^2, is generated as an additive group by the elements $[\mathfrak a] - 1$, resp. $([\mathfrak a] - 1)([\mathfrak b] - 1)$, where $\mathfrak a, \mathfrak b$ vary over the replete ideals of K.*

Proof: By (5.6), every element $\xi \in K_0(\bar{\mathcal O})$ is of the form

$$\xi = \sum_{i=1} n_i [\mathfrak a_i].$$

If $\xi \in I$, then $\mathrm{rk}(\xi) = \sum_i n_i = 0$, and thus

$$\xi = \sum_i n_i[\mathfrak{a}_i] - \sum_i n_i = \sum_i n_i([\mathfrak{a}_i] - 1).$$

The ideal I^2 is therefore generated by the elements $([\mathfrak{a}] - 1)([\mathfrak{b}] - 1)$. As

$$[\mathfrak{c}]([\mathfrak{a}] - 1)([\mathfrak{b}] - 1) = \big(([\mathfrak{c}\mathfrak{a}] - 1) - ([\mathfrak{c}] - 1)\big)([\mathfrak{b}] - 1),$$

these elements already form a system of generators of the abelian group I^2. □

By (5.7), this gives us the

(6.2) Corollary. $I^2 = 0$.

We now define

$$\mathrm{gr}\,K_0(\mathfrak{o}) = \mathbb{Z} \oplus I$$

and turn this additive group into a ring by putting $xy = 0$ for $x, y \in I$.

(6.3) Definition. *The* additive *homomorphism*

$$c_1 : K_0(\mathfrak{o}) \to I, \quad c_1(\xi) = \xi - \mathrm{rk}(\xi)$$

is called the **first Chern** class. *The mapping*

$$\mathrm{ch} : K_0(\mathfrak{o}) \to \mathrm{gr}\,K_0(\mathfrak{o}), \quad \mathrm{ch}(\xi) = \mathrm{rk}(\xi) + c_1(\xi),$$

is called the **Chern character** of $K_0(\mathfrak{o})$.

(6.4) Proposition. *The Chern character*

$$\mathrm{ch} : K_0(\mathfrak{o}) \to \mathrm{gr}\,K_0(\mathfrak{o})$$

is an isomorphism of rings.

Proof: The mappings rk and c_1 are homomorphisms of additive groups, and both are also multiplicative. For rk this is clear, and for c_1 it is enough to check it on the generators $x = [\mathfrak{a}], y = [\mathfrak{b}]$. This works because

$$c_1(xy) = xy - 1 = (x-1) + (y-1) + (x-1)(y-1) = c_1(x) + c_1(y),$$

because $(x-1)(y-1) = 0$ by (5.7). Therefore ch is a ring homomorphism. The mapping

$$\mathbb{Z} \oplus I \to K_0(\mathfrak{o}), \quad n \oplus \xi \mapsto \xi + n,$$

is obviously an inverse mapping, so that ch is even an isomorphism. □

We obtain a complete and explicit description of the Chern character by taking into account another homomorphi�m, as well a,; the homomorphi�m rk: $K_0(0)$ --+ Z, namely

$$\det: K_0(0) - Pic(O)$$

which is induced by taking determinants det M of projective o-modules M as follows (see §4). detM is an invertible metrized o-module, and therefore of the form L(n) for some replete ideal n, which is well determined up to isomorphi,;m. Denoting by [det Ml the class of a in $Pic(O)$, the linear extcm,ion of the map {M) 1---+ rdetM] give� a homomorphi<,m

$$\det: F_0(0) - Pic(O).$$

It maps the subgroup $R_0(8)$ to I, because it i,; generated by the clements $/M') - \{M) + /M''/$ which arise from �hurt exact sequence�

$$0 - M' - M - M^{11} - 0$$

of projective metri7ed o-modules and which, by (4.7), satisfy

$$\det\{M) = [\det M] = [dctM' \otimes \det M^{11}J$$
$$= [dct M'l[\det M''J = \det\{M')\det/M''\backslash.$$

Thu-; we get an induced homomorphi,;111 <let: Ko(8)--+ $Pic(O)$. It satistlc� the following proposition.

(6.5) **Proposition.** (i) *The c1111onica/* /Jomomorp/Ji.m1

$$Pic(8) - K_0(0)^*$$

is *injective.*

(ii) *The restriction* ofdet *to I,*

$$<let:/ - Pic(O),$$

i.� an isommphi�m.

Proof: (i) The composite of both mappings

$$Pic(O) - K_0(o)^* \to Pic(8)$$

is the identity, -;ince for an invertible metrized o-module M, one clearly has dct $M = M$. Thi5 give� (i).

(ii) Next. viewing the elements of Pi/'(8) a<, clement� of $K_0(0)$,

$$8:Pic(O)- t, \quad O(x)=x-1,$$

usan inver�e mapping to <let : / → $Pic(O)$. In fact, one has $=$ id since dct([o] - I) $=$ dctlol $=$ rn], and 8 u det $=$ id ..,ince 8(det(loj -])) $=$ O(det[nJ) $=$ O(fal) $=$ [oj - I and because of the fact that Ii� generated by clements of the fonn la] - 1 (see {6.1)). D

From the i�omorphism det / _::: .. *Pic(8)*, we now obtain an isomorphism

grK0(8) ;;;; _.. Z EBPic(8)

and the composite

Ko(8) � gr Ko(8) �ZEBPic(6)

will again be called the Chem character of $K_0(8)$. Observing thal $\det(c_1(l;))$ = dct(I; - rk(l;) I)= det(l;), this yields the explicit description of the Grothendieck group K0(8):

(6.6) Theorem. *The Chem character* gives *an* isomorphism

ch : $K_0(6)$ .....::::,,. ZEB *Pic(8)*, ch(,;)= rk(l;) EB det(I;).

The expert should note that this homomorphism is a realization map from *K*-theory into Chow-theory. Identifying Pic(8) with the divisor class group $CH^1(6)$, we have to view Z EBPic(O) a� the "replete" *Chow rin!!,CH(B).*

§7. Grothendieck-Riemann-Roch

We now comider a finite extension LI *K* of algebraic number field5 and study the relations between the Grothendieck groups of *L* and *K*. Let *o*, resp. *0*, be the ring of integers of *K*, resp. L and write X(C) = Hom(K,C), Y(C) = Hom(/,,C). The inclusion i: *o---+ ()* and the surjection Y(C)---+ X(C), *a* i----+ *alK*, give two canonical homomorphi�ms

i*: K0(8) - Ko(O) and i*: Ko(i5) ----cl- Ko(8).

defined as follows.

If *M* is a projective metrized o-modulc, then $M \otimes_o 0$ is a projective 0-module. As

$$(M \otimes_{\mathcal{O}} \mathcal{O})_{\mathbb{C}} = M \otimes_{\mathcal{O}} \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{C} = M_{\mathbb{C}} \otimes_{K_{\mathbb{C}}} L_{\mathbb{C}},$$

the hermitian metric on the K:c-module *M,c* extends canonically to an F-invariant metric of the Le-module $(M \otimes_0 0)$::. Therefore *M ®c,0* is automatically a metrized 0-module, which we denote by i**M.* If

$$0 - M' - M - M'' - 0$$

is a short exact sequence of projective metrized a-modules, then

0----;,- M' @ 0----;,-M ® 0----;,-M11 @ 0----;,-0

i5 a t>hort exact sequence of metrized CJ-module�. becau<;e O it> a projective o-module and the metrics in the sequence

0----;,- M� ----;,- Mr ----;,- M� ----;,- 0

simply extend Lir-sesquilinearly to metrics in the �equence of Lr:-modules

0----;,- M(c ®K. Le ----;,- Mc ®K,· Le ---+ M�®K,_· Lr:--+ 0.

This is why mapping, in the usual way (i.e.. via the representation Ko(O) = Fo(O)/Ro(O)),

M>-+li'Ml�IM0n01

gives a well-defined homomorphism

i* : Ko(O) ---+ Ko(O).

The reader may verify for himself that this is in fact a ring homomorphism.

On the other hand, if M is a projective metrizcd 0-module, then M is automatically also a projective a-module. For the complexification M�: = M ®;c :C we have the decomposition

M,c � EB M, � EB EB M, � EB Ma'
TEY(l.:) acX(C) rlrr rrEX(:C)

where MT= M ®o.TC and

Ma� M0o.,C � EBM,
""

The (:-vector space� MT carry hermitian metrics (,)Mr• and we dcline the metric {,)M" on the C-vector space Mrr to be the orthogonal sum

{x,y),.,-" = L (x,,y,)M, •
""

This gives a hennitian metric on the Kr:,-module M[·, whose F-invariance if> clearly guaranteed by the F-invariance of the original metric (,)M. We denote the mctrizcd a-module M thus constructed by i*M.

If O → M' → M → M11 → 0 is a short exact sequence of projective metrized 0-modulcs, then

0---+ i*M'---+ i*M ---+ i*M''---+ 0

is clearly an exact sequence of projective mctri1:cd a-modules. A� before, thb b why the correspondence

Mf----i-[i*M]

gives us a well-defined (additive) homomorphism

i*: K_0(0)---+ K_0(6).

(7.l) Proposition (Projection Formula). *The diagram*

$$\begin{array}{ccccc} Ko(O) & \mathrm{x} & \mathrm{Ko(B)} & & Ko(O) \\ {\scriptstyle i_*}\downarrow & & \uparrow{\scriptstyle i^*} & & \downarrow{\scriptstyle i_*} \\ K_0(8) & \mathrm{x} & \mathrm{Ko(8)} & & \mathrm{Ko(i5)} \end{array}$$

is *commutative.* where *the horizontal* arrows arc *multiplication.*

Proof: If *M,* resp. *N,* is a projective mctrized 0-module, resp. o-module. there is an isometry

$$i^*(M \text{®}v\ i^*N) \text{ � } i^*M \text{®}_o N$$

of projective mctrized o-modules. Indeed, we have an isomorphism of the underlying o-modules

$$M \text{®}o\ (N \text{®}_o \mathrm{CJ}) \text{ � } M \text{®o } N. \quad a\text{®}\ (h@c) \text{ 1---+ } ca\text{®}\ h.$$

Tensoring with it induces an isomorphism

$$M_{\mathbb{C}} \otimes_{L_{\mathbb{C}}} (N_{\mathbb{C}} \otimes_{K_{\mathbb{C}}} L_{\mathbb{C}}) \cong M_{\mathbb{C}} \otimes_{K_{\mathbb{C}}} N_{\mathbb{C}}.$$

That this is an i5ometry of metrized K,�:-modules rc�ulh from the distributivity

$$\underset{\mathrm{Tiff}}{\mathrm{I:!.}}\ \mathrm{)M,I,}\ )N,,\ \text{�}\underset{\mathrm{rlr,}}{(\mathrm{Li.}}\ \mathrm{).w,)I.}\ )N,,$$

by applying mathematical grammar. □

The Riemann-Roch prohlem **in** Grothendieck"s perspective i5 the task of computing the Chern character ch(i*M) for a projective metrized *0*-module Min terms of ch(M). By (6.6), thi� amounts to computing det(i.M) in terms of det *M.* **But** dct *M* is an invertible metrized 0-module and is therefore iwmetric by (4.5) to the metrized 0-module L(Ql) of a replete ideal Qt of *L. N1* IK (Qt) i� then a replete ideal of *K,* and we put

NL1KidctM) :� *L(* NL1Ki'll))

This is an invertible metrized a-module which is well determined by *M* up to isometry. With this notation we first establish the following theorem.

(7.2) Theorem. For *any projective* metri7ed *0-module M one has:*

,kU,M) � rkiM) rkiO),

$$\det(i^*M) \text{ � } \mathrm{Ntw(detM)}0_0\ \ \mathrm{(deti^*O)'k(Ml\_}$$

Herc we have rk(O) = (L: K].

Proof: One has $M_K := M \otimes_{\mathfrak o} K = M \otimes_{\mathcal O} (\mathcal O \otimes_{\mathfrak o} K) = M \otimes_{\mathcal O} L =: M_L$ and therefore

$$\operatorname{rk}(i_*M) = \dim_K(M_K) = \dim_K(M_L) = \dim_L(M_L)\,|L:K| = \operatorname{rk}(M)\operatorname{rk}(\mathcal O).$$

In order to prove the second equation, we first reduce to a special case. Let

$$\lambda(M) = \det(i_*M) \quad \text{and} \quad \rho(M) = N_{L|K}(\det M) \otimes_{\mathfrak o} (\det i_*\mathcal O)^{\operatorname{rk}(M)}.$$

If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of projective metrized $\mathcal O$-modules, one has

$$(*) \qquad \lambda(M) \cong \lambda(M') \otimes_{\mathfrak o} \lambda(M'') \quad \text{and} \quad \rho(M) \cong \rho(M') \otimes_{\mathfrak o} \rho(M'').$$

The isomorphism on the left follows from the exact sequence $0 \to i_*M' \to i_*M \to i_*M'' \to 0$ by (4.7), and the one on the right from (4.7) also, from the multiplicativity of the norm $N_{L|K}$ and the additivity of the rank rk. As in the proof of (5.6), we now make use of the fact that every projective metrized $\mathcal O$-module M projects via an admissible epimorphism onto a suitable $\mathcal O$-module of the form $L(\mathfrak A)$ for some replete ideal $\mathfrak A$. Thus (*) allows us to reduce by induction on rk(M) to the case $M = L(\mathfrak A)$. Here $\operatorname{rk}(M) = 1$, we have to establish the isomorphism

$$\det\bigl(i_*L(\mathfrak A)\bigr) = L\bigl(N_{L|K}(\mathfrak A)\bigr) \otimes_{\mathfrak o} \det{}_{\mathfrak o}\mathcal O.$$

For the underlying $\mathfrak o$-modules this amounts to the identity

$$(**) \qquad \det{}_{\mathfrak o}\mathfrak A_f = N_{L|K}(\mathfrak A_f)\det{}_{\mathfrak o}\mathcal O,$$

which has to be viewed as inside $\det_K L$ and which is proved as follows. If $\mathcal O$ and $\mathfrak o$ were principal ideal domains, it would be obvious. In fact, in that case we could choose a generator α of $\mathfrak A_f$ and an integral basis $\omega_1, \dots, \omega_n$ of $\mathcal O$ over $\mathfrak o$. Since $N_{L|K}(\alpha)$ is by definition the determinant $\det(T_\alpha)$ of the transformation $T_\alpha : L \to L$, $x \mapsto \alpha x$, we would get the equation

$$\alpha\omega_1 \wedge \ldots \wedge \alpha\omega_n = N_{L|K}(\alpha)(\omega_1 \wedge \ldots \wedge \omega_n),$$

the left-hand side, resp. right-hand side, of which would, by (1.6), generate the left-hand side, resp. right-hand side, of (**). But we may always produce a principal ideal domain as desired by passing from $\mathcal O|\mathfrak o$ to the localization $\mathcal O_{\mathfrak p}|\mathfrak o_{\mathfrak p}$ for every prime ideal $\mathfrak p$ of $\mathfrak o$ (see chap. I, § 11 and § 3, exercise 4). The preceding argument then shows that

$$(\det{}_{\mathfrak o}\mathfrak A_f)_{\mathfrak p} = \det{}_{\mathfrak o_{\mathfrak p}}\mathfrak A_{f\mathfrak p} = N_{L|K}(\mathfrak A_{f\mathfrak p})\det{}_{\mathfrak o_{\mathfrak p}}\mathcal O_{\mathfrak p} = (N_{L|K}(\mathfrak A_f)\det{}_{\mathfrak o}\mathcal O)_{\mathfrak p},$$

and since this identity is valid for all prime ideals $\mathfrak p$ of $\mathfrak o$, we deduce the equality (**).

In order to prove that the metric'> agree on both sides of (**), we put $M = L(2l)$, $N = L(O)$, $a=$ Nt.1K(2l) and we view M,N,a as metrized o-modules, One **ha�** $Mr: = N-: = Le$ and a,:: = Kc, and we consider the metric� on the componenb

$$\text{Mrr�}\bigoplus_{r1r1}\text{lC}, \quad \text{Nrr�}\bigoplus_{rlr1}\text{lC}, \quad \text{Urr�C},$$

where a E Hom(K,C) and r E Hom(L,C) is such that rla. We have to show that, for i;, $T/$ E det:c Mr1 and a, h E one has the identity

$$\{ai;,hrJ)cte1M_{\sigma} = (a,h)a.-,\{i;,17)\det\bullet V_{\sigma}$$

For thi5, let 21.,:x, = n'lll(X, >,J3V•+1, so that one gets

$$a^{\circ}{}''= NL1Kcm''''> = \prod_{\mu loc} PVp$$

with vp = L'lllP f'lJ1pV'lJ. Then

$$(x,y)N,,. = \text{Lxrfr},_{,1rr} \qquad \langle x, y\rangle_{M_\sigma} = \sum_{\tau\mid\sigma} e^{2\nu_{\mathfrak{P}_\tau}} x_\tau \overline{y}_\tau\,,$$

$$\langle a, b\rangle_{\mathfrak{a}_\sigma} = e^{2\nu_{\mathfrak{p}_\sigma}} a\overline{b}\,, \qquad \nu_{\mathfrak{p}_\sigma} = \sum_{\mathfrak{P}\mid\mathfrak{p}_\sigma} f_{\mathfrak{P}\mid\mathfrak{p}_\sigma}\nu_{\mathfrak{P}} = \sum_{\tau\mid\sigma}\nu_{\mathfrak{P}_\tau}$$

Let � = x1 /\ ... /\ .\n, IJ = y1 I\ ... I\ Yn• We number the embeddings r la, r1, ..., r11, put l'/i = v'lJr1. and fonn the matrices

$$A = (x_{i\tau_k})\,, \quad B = (\overline{y}_{i\tau_k})\,, \quad D = \begin{pmatrix} e^{\nu_1} & & 0 \\ & \ddots & \\ 0 & & e^{\nu_n}\end{pmatrix}$$

Then, observing that

$$\det(D) = \prod_{r} ev-.,, = \prod_{'131Pa} \text{ehllPo}\ \text{\'•ii}= evp,,.,$$

we do indeed get

$$\begin{aligned}(a\text{�},hry)uctM,, &=ah\{i;,17),1c1M,,.\\ &= abdet(\,(AD)(BD)^1) = ah\,(\det D)^2\det(AB^1)\\ &= e^2vp,,.ah\ \{i;,1/)\det N,, = (a,\ h),,_{\sigma}\,(i;,1J)de1N_{\sigma}\end{aligned}$$

This proves our theorem, □

Extending the formulas of (7,2) to the free abelian group

$$F_0(0) \text{�} \bigoplus_{[Ml} \mathbb{Z}\{M\}$$

by linearity, and pm,sing lO the quotient group $K_0(0) = F_0(0)/R_0(0)$ yield!', the following corollary.

(7.3) Corollary. *For every* class t E K_0(i.5), one *has the fomwlns*

ckU,s) � *[L , K* J ck(sJ,

det(i*O = [dcti*O]rk(/;JN, 1ddetn.

The square of the metrized o-module dcti*O appearing in the second formula can he computed to be the *discriminant ilLIK* of the extension *L* IK, which we view as a metrizcd o-module with the *trivial* metric.

(7.4) Proposition. *There* i.� *a* canonical *isomorphism*

$$(\det i_*\mathcal{O})^{\otimes 2} \cong \mathfrak{d}_{L|K}$$

of *mctrized o-modu/e8.*

Proof: Com,ider on *O* the bilinear trace map

$$T : \mathcal{O} \times \mathcal{O} \longrightarrow \mathcal{o}, \quad (x, y) \longmapsto Tr_{L|K}(xy).$$

It induces an *a-module* homomorphism

T :detC'.J®detO -------+o.

given by

$$T\big((\alpha_1 \wedge \ldots \wedge \alpha_n) \otimes (\beta_1 \wedge \ldots \wedge \beta_n)\big) = \det\big(Tr_{L|K}(\alpha_i\beta_j)\big)$$

The image of *T* is the di5criminant ideal *ilt.IK,* which, by definition, is generated by the discriminant5

d(cv1 ..... w,1) = *det(TrL,K(cv,cv1))*

of all ba�e� of *LIK* which are contained in *0.* This is clear ir *('.)* admits an integral basis over *o,* since the *a,* and */3,* can be written in terms of such a basi� with coefficients in *O.* If there i� no such integral basis, it will exist after localizing Op lop at every prime ideal p (see chap. I, (2.10)). The image of

$$T_{\mathfrak{p}} : (\det \mathcal{O}_{\mathfrak{p}}) \otimes (\det \mathcal{O}_{\mathfrak{p}}) \longrightarrow \mathcal{o}_{\mathfrak{p}}$$

is therefore the discriminant ideal of Oplop and at the same time the localization of the image of *T.* Since two ideals are equal when their localizations are, we find image(T) = *i)LIK·* Furthermore, *T* has to be injective since (det Ofg:[2] is an invertible o-modulc. Therefore *T* is an v-module i�omorphism.

We now check that

$$T_{\mathbb{C}} : \left(\det(\mathcal{O})^{\otimes 2}\right)_{\mathbb{C}} \longrightarrow (\mathfrak{d}_{L|K})_{\mathbb{C}}$$

is indeed an i�ometry. For Oc = 0 ®c:. IC, we obtain the K::_·-module decomposition

$$\mathcal{O}_{\mathbb{C}} = \bigoplus \mathcal{O}_{\sigma},$$

where a varies over the set Hom(K. C). and the direct sum

Oa � ffi(O®o,c I:)� ffii:
,10

is taken over all T E Hom(L, C) such that r l K = a. The mapping O::_· - K 1• induced by TrLIK : 0--,,. o is given, for x = ffi 0 Xrr, x,.,. E 0,.,., by

TrL K(X) =

where Tra (xrr) = the xrr r E C being the components of x_0• The metric on (i*Oh: = is the orthogonal sum of the standard metrics

(x,y)" = L t,Yr = Tr,,(x"y)
,10

on the :I::-vector spaces (i.0)1r = 0,,. = EBr,rr C. Now let x,, y, E 0..,., i = I, ... ,11, and writex = x1/\ ... /\ \-n, y = y1 I\ /\y11 E det(O,.,.). The map Tc splits into the direct sum T,c = EB,,. Tc, of the maps

J'a : det(Orr) ®c dct(Oa) --+ (iJL1da = C

which are given by

$$T_{\sigma}(x \otimes y) = \det\left(Tr_{\sigma}(x_i y_j)\right).$$

For any two n-tuples \;, y; E Orr we form the matrices

A� Cfre(x,y,)), A'� (T1e(,;v;)), 8 � (Tca(,,x;i). B' � (T,·o(y,v;)).

Then one has AA' = BB'. and we obtain

$$\left\langle T_{\sigma}(x \otimes y), T_{\sigma}(x' \otimes y')\right\rangle_{(\mathfrak{d}_{L|K})_{\sigma}} = T_{\sigma}(x \otimes y)\, \overline{T_{\sigma}(x' \otimes y')}$$

� dct(T!-0(,,y1)) det(T!-e(,;v;l) � det(AA') � det(BB')

� det(T,-0 (.;i))det(T,-0 (y, y;)) � det((x,.x;le) det({y,, y; le)

= (x.x')detOa (_y. Y')<1er()CT = (x ® Y, \' ® Y')(de10a)0�-

This �how� that T,c i� an i�ometry. □

We now set out to rewrite the results obtained in (7.2) and (7.4) in the language of GROTHENDIECK's general formalism. For the homomorphism i_* there is the commutative diagram

$$\begin{tikzcd} K_0(\bar{\mathcal O}) \arrow[r, "rk"] \arrow[d, "i_*"] & \mathbb{Z} \arrow[d, "{[L:K]}"] \\ K_0(\bar{\mathfrak o}) \arrow[r, "rk"] & \mathbb{Z}, \end{tikzcd}$$

because $[L:K]$ times the rank of an $\mathcal O$-module M is its rank as $\mathfrak o$-module. Therefore i_* induces a homomorphism

$$i_*: I(\bar{\mathcal O}) \longrightarrow I(\bar{\mathfrak o})$$

between the kernels of both rank homomorphisms, so that there is a homomorphism

$$i_*: \operatorname{gr} K_0(\bar{\mathcal O}) \longrightarrow \operatorname{gr} K_0(\bar{\mathfrak o}).$$

It is called the Gysin map. (7.3) immediately gives the following explicit description of it.

(7.5) **Corollary.** *The diagram*

$$\begin{tikzcd} \operatorname{gr} K_0(\bar{\mathcal O}) \arrow[r, "\cong"] \arrow[d, "i_*"] & \mathbb{Z} \oplus Pic(\bar{\mathcal O}) \arrow[d, "{[L:K] \oplus N_{L|K}}"] \\ \operatorname{gr} K_0(\bar{\mathfrak o}) \arrow[r, "\cong"] & \mathbb{Z} \oplus Pic(\bar{\mathfrak o}) \end{tikzcd}$$

is commutative.

We now consider the following diagram

$$\begin{tikzcd} K_0(\bar{\mathcal O}) \arrow[r, "ch"] \arrow[d, "i_*"] & \operatorname{gr} K_0(\bar{\mathcal O}) \arrow[d, "i_*"] \\ K_0(\bar{\mathfrak o}) \arrow[r, "ch"] & \operatorname{gr} K_0(\bar{\mathfrak o}) \end{tikzcd}$$

where the Gysin map i_* on the right is explicitly given by (7.5), whereas the determination of the composite $ch \circ i_*$ is precisely the Riemann-Roch problem. The difficulty that confronts us here lies in the fact that the diagram is *not commutative.* In order to make it commute, we need a correction, which will be provided via the module of differentials (with trivial metric), by the *Todd class*, which is defined as follows.

The module .0{0$_{10}$ of differentials is only a coherent, and not a projective 0-modulc. But it1> class fDl, $_{10}$1 is viewed as an clement of $K_o(O)$ via the PoincarC isomorphism

$$K_0(\bar{\mathcal{O}}) \xrightarrow{\sim} K^0(\bar{\mathcal{O}})$$

and since rko(Db$_{10}$) = 0, it lies in / (0).

(7.6) **Definition.** *The* **Todd** class of Olo is *defined to be the element*

$$\mathrm{Td}(\mathcal{O}|\mathcal{o}) = 1 - \frac{1}{2}c_1\big([\Omega^1_{\mathcal{O}|\mathcal{o}}]\big) = 1 - \frac{1}{2}[\Omega^1_{\mathcal{O}|\mathcal{o}}] \in \operatorname{gr} K_0(\bar{\mathcal{O}}) \otimes \mathbb{Z}[\tfrac{1}{2}]$$

Because of the factor ½, the Todd class docs not belong to the ring gr Ko(O) itself, but i:- only an element of gr K_0(0) ® Zl {]. The module of differential5 .ab$_{10}$ is connected with the **different** *'.DLIK* Or the extension Ll *K* by the exact ,;cquence

0---+ *'.Dr.1K* ---+ *0*---+ *Q*�*Jlo* ---+ 0

of 0-modules (with trivial metrics) ('-CC §2, exercise 3). This implies that l.1?2)$_{10]}$ = 1 - *['.l.hw* l- We may therefore describe the Todd class also by the different:

$$\mathrm{Td}(\mathcal{O}|\mathcal{o}) = 1 + \frac{1}{2}([\mathfrak{D}_{L|K}] - 1) = \frac{1}{2}\big(1 + [\mathfrak{D}_{L|K}]\big).$$

The main result now follows from (7.3) w,ing the Todd class.

(7.7) **Theorem (Grothendieck-Riemann-Roch).** *The diagram*

Ko(i5) � grKn(O)

Ko(O) � gr K_0(0)

is commulative.

Proof: For� E K_0(i5). we have to !',how the identity

chU,0 � ;,(Td(Olo)ch(sl).

Decomposing ch(i*O = rk(i*O EB c1 (i*O and ch(S) = rk(,;") EB *c,* (0 and ob&erving that

Td(Olv)ch(s) � (I+½ (['.DL,Ki - !)) (,k(s) + c,(rn

�,ken+ [,,m + ½ ,k(sJ<l'.DL1Kl - 1J].

it rnffices to check the equations

(a) ,ku.n �,k(s),kU.[01).

(b) ,,*u.,1*�;,c,·1(sJJ + ,kc,1,1 u,10D

and

(c) ,k(;,101) �;.(I).

(d) 2c1 (;,[OJ) � ;,(l'.D11K I - 1)

in gr $K_0(0)$. The equations (a) and (c) are clear because of rk(i*fO]) = rk(i*CJ) = [L: K]. To show (b) and (d), we apply <let to both sides and are reduced by the commutative diagram (7.5) to the equations

(c) det(LO = *NL1K(* (detO) [deti*CJ]'k(/;J,

(f) (deti*CJ)[02] = *NL1K(det'.DL1K>-*

But (e) is the second identity of (7.3), and (t1 follow5 from (7.4) and (2.9). □

With this final theorem, the theory of algebraic integeVi can be integrated completely into a general programme of algebraic geometry as a special case. What is needed is the use of the geometric language for the objects considered. Thus the ring o is interpreted as the �cheme X = Spec(o), the projective metri7ed o-module5 a,; metrized 1·et *tor bundles,* the invertible c,-modules as *line bundles,* the inclusion i : o---+ CJ a5 morphism f : Y = Spec(CJ) ---+ X of schemes, the class as the *cotanient element,* etc. In this way one realizes in the present the old idea of viewing number theory a5 part of geometry.

§ 8. The Euler-Minkowski Characteristic

Considering the theorem of Grothendieck-Ricmann-Roch in the special case of an extension $K|\mathbb{Q}$, amounts to revisiting the Riemann-Roch theory of S 3 from our new point of view. At the center of that theory was the Euler-Minkowski characteristic

$$x(a) = -\log\mathrm{vol}(a)$$

of replete ideals *a* of *K*. Here, vol(a) was the *canonical mearnre* of a fundamental me�h of the lattice in Minkowski space *K:..:* = a€h. IR defined by *a*. This definition is properly explained in the theory of mctriLed modules of higher rank. More precisely, instead of considering *a* as a metrized o-module of rank l, it should be viewed as a metrized Z-module of rank [K : QJ. This point of view lead� us necessarily to the following detlnition of the Euler-Minkowski characteri�tic.

(8.1) Prnposition. *The* degree *map*

$$\deg K : Pit\,(l'J) \text{ ---+ } IR, \quad \deg K\,(laj) = -\log \backslash Jl(a).$$

extends uniquely 10 ;1 *homomorphism*

$$XK: \mathrm{Ko}(O)\text{-----+ },�$$

on $K_0(0)$, *and thereby on* $K^0(0)$. *It* is *given by*

$$XK = \mathrm{degudet}$$

and called *the* Euler-Minkowski characteristic over *K*.

Proof: Since, by (5.6), $K_0(0)$ i� generated as an additive group by the elements [aJ E *Pic(O)*, the map degK on *Pic(O)* determine� a unique homomorphism $K_0(8) \to$ IR which extends dcgK. But such a homomorphism i� given by the composite of the homomorphi�m�

$$K_0(0)� \quad Pic(O)� \quad JR.$$

a<, the composite *Pit* (8) ·-,ı, $K_0(0)$ � *Pit* (l'J) i� the identity. LJ

Via the Poincare isomorphism $K_0(0)$ � *K'\a)*. we transfer the maps det and *XK* to the Grothendieck group $K^0(0)$ of coherent metrized ()-modules. Then proposition (8.1) is equally valid *for* $K^0(0)$ a� for $K_0(0)$. We define in what follows *XK(M)* = xd[Ml) for a metrized n-mudule *M*. If LI *K* is an extension of algebraic number fields and i : n → CJ the inclusion of the maximal orders of *K*, resp. *L*, then applying degK to the formula (7.2) and using

$$\mathrm{dcgdQI)} � -\log;Jl('ll) � -\log;JJ(\,NLIK\,('llJ) � \deg K\,(\,NLIK\,('llJ)$$

(sec (l.6), (iii)) gives the

(8.2) **Theorem.** *For eve1y coherent 0-modulc M, the Riemann-Roch* formu/:.J

$$\chi_K(i_*M) = \deg_L(\det M) + \mathrm{rk}(M)\,\chi_K(i_*\mathcal{O})$$

is valid, *and* in particular, for an *invertible metrized 0-module M.* we *have*

$$\chi_K(i_*M) = \deg_L(M) + \chi_K(i_*\mathcal{O}).$$

We now speciali7e to the case of the base field K = Q. lhat is. we consider metrized Z-modulc<;. Such a module is simply a finitely generated abclian group M together with a euclidean metric on the real vector space

$$M_{\mathbb{R}} = M \otimes_{\mathbb{Z}}$$

Indeed, since Q ha<; only a single embedding into i.e., Qr: = a metric on M is simply given by a hermitian scalar product on the [>vector space M,c = M 1 ® C. Restricting thi:- to M f give:- a euclidean metric the sc�quilinear exten�ion of which reproduces the original metric.

If M i� a *projective* metri7ed Z-module, then the underlying Z-modulc is a finitely generated free abelian group. The canonical map M --+ M ® IR, a 1--+ a® I, identities M with a complete lattice in *Mn;;.* If a1, , *a11*is a Z-ba�i� of *M,* then the set

$$\Phi = \{x_1\alpha_1 + \cdots + x_n\alpha_n \mid x_i \in \mathbb{R},\ 0 \le x_i < 1\}$$

is a *fundamental me�h* of the lauice *M.* The euclidean metric { ,)*M* defines a Haar measure on M11,. Once we choo:-e an orthonormal basis c1, , *e11*of M1k, this Haar measure can be expres�cd, via the i<;omorphism *MJ....:.,. Rn,* J.1c1 +-- ·+ \11C11 i-------+ Ct 1, ... , *Xn),* by the Lebesgue measure on R.". With respect to this measure, the volume of the fundamental mesh *(/)* is given by

vol(<P) = idet({a,.a,))I 112

It will be denoted hy vol(M) for short. It does not depend on the choice of Z-basis a1, , *a11*because a different choice is linked to the original one by a matrix with integer coefficients which also ha<; an inverse with integer cocflicients. hence has determinant of ab<,olute value I.

A more elegant definition of vol(M) can be given in terms of the invertible metrizcd Z-modulc det *M*. det *M"9:.* i� a one-dimensional IR-vector space with metric (.)ctcr *M,* and with the lattice Jet M isomorphic to?.;, If x E det M i� a generator (for instance, x = a_1 /\. /\ a11), then

$$\mathrm{vol}(M) = \|x\|_{\det M} = \sqrt{\langle x, x\rangle_{\det M}}.$$

In the present case, where the base field is $\mathbb{Q}$, the degree map

$$\deg : \widehat{\mathrm{Pic}}(\bar{\mathbb{Z}}) \longrightarrow \mathbb{R}$$

is an isomorphism (see § 1, exercise 3), and we call the unique homomorphism arising from this,

$$\chi = \deg\circ\det : K_0(\bar{\mathbb{Z}}) \longrightarrow \mathbb{R},$$

the Euler-Minkowski characteristic. It is computed explicitly as follows.

(8.3) **Proposition.** *For a coherent metrized $\mathbb{Z}$-module M, one has*

$$\chi(M) = \log \#M_{tor} - \log \mathrm{vol}(M/M_{tor}).$$

In this formula M_{tor} denotes the torsion subgroup of M and M/M_{tor} the projective metrized $\mathbb{Z}$-module which receives its metric from M via $M\otimes\mathbb{R} = M/M_{tor}\otimes\mathbb{R}$.

Proof of (8.3): If M is a finite $\mathbb{Z}$-module, then the determinant of the class $[M] \in K_0(\bar{\mathbb{Z}})$ is computed from a free resolution

$$0 \longrightarrow E \longrightarrow F \xrightarrow{\alpha} M \longrightarrow 0,$$

where $F = \mathbb{Z}^n$ and $E = \ker(\alpha) \cong \mathbb{Z}^n$. If we equip $F\otimes\mathbb{R} = E\otimes\mathbb{R} = \mathbb{R}^n$ with the standard metric, the sequence becomes a short exact sequence of metrized $\mathbb{Z}$-modules, because $M\otimes\mathbb{R} = 0$. We therefore have in $K_0(\bar{\mathbb{Z}})$:

$$[M] = [F] - [E].$$

Let A be the matrix corresponding to the change of basis from the standard basis $e_1, \dots, e_n$ of F to a $\mathbb{Z}$-basis $e_1', \dots, e_n'$ of E. Then $x = e_1\wedge\dots\wedge e_n$, resp. $x' = e_1'\wedge\dots\wedge e_n'$, is a generator of $\det F$, resp. $\det E$, and

$$x' = \det A\cdot x = (F:E)\cdot x = \#M\cdot x.$$

The metric $\|\ \|$ on $\det E$ is the same as that on $\det F$, so that

$$\chi(E) = \deg(\det E) = -\log\|x'\| = -\log(\#M\|x\|) = -\log\#M + \chi(F),$$

and then

$$\chi(M) = \chi([F]-[E]) = \chi(F) - \chi(E) = \log\#M.$$

For an arbitrary coherent metrized $\mathbb{Z}$-module M we have the direct sum decomposition

$$M = M_{tor}\oplus M/M_{tor},$$

into metri7ed Z-modules. If a$_1$, , r.xn is a basis of the lattice M/M10,, then r = a1 A . A an is a generator of detM/M1or; then x(M/Mw,) = deg(detM/M10,) = -logllxll = -logvol(M/M1or). We therefore conclude that

x(M) = x(M1or) + x(M/M101) = log#M1or - logvol(M/M1,"). [J

The Euler-Minkowski characteristic of a replete ideal a,

x(a) = -logvol(a).

which we defined *ad hoc* in §3 via the Minkowski measure vol(a) now appears a5 a �imple special case of the Euler-Minkowski characteristic for metrized Z-modules to which the detailed development of the theory has led us. Indeed. viewing the metri1:ed o-modulc L(a) of rank 1 associated to u as the mctrized Z-module i.•L(a) of rank [K: QI, we get the

(8.4) Proposition. x(a) = x(i�L(a)).

Proof: Let u = 0100.., = 01 nplcx: p\.'p. The metric (,)1,L(ol on the C-vector space K1, = TTrEX(i'l C is then given by

(x,y),,L(o) = Lc2vP,x,y,.

where p, is the infinite place of K corresponding to the embedding r : K → It results from the standard metric (,) via the F -invariant transformation

T: Kc---+ K,c, (x,),cX(iCJ f----;- (e"Prxr)ncX('.:'J·

Equivalently,

(x,J)i,L(o) = (Tx,Ty).

The volume vol(i*L(a)) of a fundamental mesh of the lattice or in Kut with respect to the Haar measure defined by the euclidean metric on K1n i� then the volume of a fundamental mesh of the lattice Tar with respect to the canonical measure defined by ,( ). Thus

so!(;,L(a)) � ,ol(Tor).

In the representation Kw.= TTPI= Kp, the canonical embedding

Ku,;= K R---+ K.�: = K ®li'

maps an clement to the element (x,)rcx (Cl with x r = r ..1 P,. Here we extend r to Kp,· restriction of the transformation T: (r,) H (evP,x,) to K"3. = TT111-x. Kp is therefore given by (xp) H (e'·rxp), The lattice Ta$_1$ is then the same lattice which was denoted $\mathfrak{a}$ in §3. So we obtain

$$\operatorname{vol}(i_*L(\mathfrak{a})) = \operatorname{vol}(\mathfrak{a}),$$

i.e., $\chi(i_*L(\mathfrak{a})) = \chi(\mathfrak{a})$. □

Given this identification, the Riemann-Roch theorem (3.4) proven in §3 for replete ideals $\mathfrak{a}$,

$$\chi(\mathfrak{a}) = \deg(\mathfrak{a}) + \chi(\mathfrak{o}),$$

now appears as a special case of theorem (8.2), which says that

$$\chi(i_*L(\mathfrak{a})) = \deg(i_*L(\mathfrak{a})) + \chi(i_*\mathfrak{o}).$$

Chapter IV

Abstract Class Field Theory

§1. Infinite Galois Theory

Every field k equipped with a distinguished Galois extension: the separable closure Its Galois group Gk = G(flk) is called the **absolute Galois group** of k. As a rule, this extension will have inllnite degree. It does, however, have the advantage of collecting ail finite Galois extension5 of k. This is why it is reasonable to try to give it a prominent place in Galois theory. But such an attempt faces the difficulty that the main theorem of Galois theory doc:, not remain true for infinite extensions. Let us explain this in the following

Example: The absolute Galob group $G,_{1'}$ = G(FpiFI') of the field Fl' with p elements contains the Frohenim automorphism rp which is given by

r'i' = r1' for all x E *FP.*

The subgroup (tp) = {tp" In E Z} has the �ame fixed field *IFp* as the whole of *G1r,P.* Bul contrary to what we are u<;ed to in finite Galois theory, we find (tp) *f- Gw,,.* In order to check this, let u,; con�truct an element VJ E *G_,1'* which doc� not belong to (rp). We choose a sequence */an* lntM of integers satisfying

$$a_n \equiv a_m \bmod m$$

whenever but wch that lhere is no integer a �atisfying $a_{11} = a$ mod n for all n E An example of such a sequence is given by $a''=$ $n^1x_{11,}$ where we write n = 11^1pl'1,(ii), *(n', p)*= 1.and I = $n'r_{11}$ + p1'!,(nly11. Now put

Vin =tpa"lwl"' E G(IF'p11l[l<'I').

If *IF'p"'* £; IF*p'.* then m In, so that *an* = *am* mod *m,* and therefore

VJ,, l1i· ,,,,, = tp""]!fl"" = *tp<1"'* Irr,·,,,,, =*Vim*•

Observe Lhat tpl *·"i,n,* has order m. Therefore the *ifr*$_{11}$ define an automorphism i/1 of F\, = u�=I F,,,,, Now if, cannot belong to (rp) because *i/1* = *tp*^{0}, for a E Z, would imply ifrl. ,11 = tp""IF,,,1 = qi"l1i· ,,1 and hence *a"*= a mod n for all n, which is what we ruled out by construction.

The example does not mean, however, that we have to chuck the main theorem of Galois theory altogether in the case of infinite extensions. We just have to amend it using the observation that the Galois group $G = G(\Omega|k)$ of any Galois extension $\Omega|k$ carries a canonical topology. This topology is called the **Krull topology** and is obtained as follows. For every $\sigma \in G$ we take the cosets

$$\sigma G(\Omega|K)$$

as a basis of neighbourhoods of σ, with $K|k$ ranging over *finite* Galois subextensions of $\Omega|k$. The multiplication and the inverse map

$$G\times G \longrightarrow G,\ (\sigma,\tau)\longmapsto \sigma\tau, \quad \text{and} \quad G\longrightarrow G,\ \sigma\longmapsto \sigma^{-1},$$

are continuous maps, since the preimage of a fundamental open neighbourhood $\sigma\tau G(\Omega|K)$, resp. $\sigma^{-1}G(\Omega|K)$, contains the open neighbourhood $\sigma G(\Omega|K)\times \tau G(\Omega|K)$, resp. $\sigma G(\Omega|K)$. Thus G is a topological group which satisfies the following

(1.1) Proposition. *For every (finite or infinite) Galois extension $\Omega|k$ the Galois group $G = G(\Omega|k)$ is compact Hausdorff with respect to the Krull topology.*

Proof: If $\sigma, \tau \in G$ and $\sigma \neq \tau$, then there exists a finite Galois subextension $K|k$ of $\Omega|k$ such that $\sigma|_K \neq \tau|_K$, so that $\sigma G(\Omega|K) \neq \tau G(\Omega|K)$ and thus $\sigma G(\Omega|K) \cap \tau G(\Omega|K) = \emptyset$. This shows that G is Hausdorff. In order to prove compactness, consider the mapping

$$h : G \longrightarrow \prod_K G(K|k), \quad \sigma \longmapsto \prod_K \sigma|_K ,$$

where $K|k$ varies over the finite Galois subextensions. We view the finite groups $G(K|k)$ as discrete compact topological groups. Their product is therefore a compact topological space, by Tykhonov's theorem (see [98]). The homomorphism h is injective, because $\sigma|_K = 1$ for all K is equivalent to $\sigma = 1$. The sets $U = \prod_{K\neq K_0} G(K|k) \times \{\sigma\}$ form a subbasis of open sets of the product $\prod_K G(K|k)$, where $K_0|k$ varies over the finite subextensions of $\Omega|k$ and $\sigma \in G(K_0|k)$. If $\tilde\sigma \in G$ is a preimage of σ, then $h^{-1}(U) = \tilde\sigma G(\Omega|K_0)$. Thus h is continuous. Moreover $h(\tilde\sigma G(\Omega|K_0)) = h(G) \cap U$, so $h : G \to h(G)$ is open, and thus a homeomorphism. It therefore suffices to show that $h(G)$ is closed in the compact set $\prod_K G(K|k)$. To see this we consider, for each pair $L' \supseteq L$ of finite Galois subextensions of $\Omega|k$, the set

$$M_{L'|L} = \Big\{ \prod_K \sigma_K \in \prod_K G(K|k) \ \Big|\ \sigma_{L'}|_L = \sigma_L \Big\}$$

One clearly has $h(C) = \bigcap_{L'|L} M_{L'|L}$. So it suffices to show that $M_{L'|L}$ is closed. But if $G(L|k) = \{\sigma_1, \dots, \sigma_n\}$, and $S_i \subseteq G(L'|k)$ is the set of extensions of σ_i to L', then

$$M_{L'|L} = \bigcup_{i=1}^{n} \Big(\prod_{K \neq L, L'} G(K|k) \times S_i \times \{\sigma_i\} \Big),$$

i.e., $M_{L'|L}$ is indeed closed. □

The main theorem of Galois theory for infinite extensions can now be formulated as follows.

(1.2) Theorem. *Let $\Omega|k$ be a (finite or infinite) Galois extension. Then the assignment*

$$K \longmapsto G(\Omega|K)$$

is a 1-1-correspondence between the subextensions $K|k$ of $\Omega|k$ and the closed subgroups of $G(\Omega|k)$. The open subgroups of $G(\Omega|k)$ correspond precisely to the finite subextensions of $\Omega|k$.

Proof: Every open subgroup of $G(\Omega|k)$ is also closed, because it is the complement of the union of its open cosets. If $K|k$ is a finite subextension, then $G(\Omega|K)$ is open, because each $\sigma \in G(\Omega|K)$ admits the open neighbourhood $\sigma G(\Omega|N) \subseteq G(\Omega|K)$, where $N|k$ is the normal closure of $K|k$. If $K|k$ is an arbitrary subextension, then

$$G(\Omega|K) = \bigcap G(\Omega|K_i),$$

where $K_i|k$ varies over the finite subextensions of $K|k$. Therefore $G(\Omega|K)$ is closed.

The assignment $K \mapsto G(\Omega|K)$ is injective, since K is the fixed field of $G(\Omega|K)$. To prove surjectivity, we have to show that, given an arbitrary closed subgroup H of $G(\Omega|k)$, we always have

$$H = G(\Omega|K),$$

where K is the fixed field of H. The inclusion $H \subseteq G(\Omega|K)$ is trivial. Conversely, let $\sigma \in G(\Omega|K)$. If $L|K$ is a finite Galois subextension of $\Omega|K$, then $\sigma G(\Omega|L)$ is a fundamental open neighbourhood of σ in $G(\Omega|K)$. The map $H \to G(L|K)$ is certainly surjective, because the image $\bar{H}$ has fixed field K and is therefore equal to $G(L|K)$, by the main theorem of Galois theory for finite extensions. Thus we may choose a $\tau \in H$ such that

TIL $= alt$, i.e., r E HnaG(DIL). Thb show� that a belongs to the closure of Hin G(S21K), and thus to H itself, w that $H = G(QIK)$.

If H ban open subgroup of G(.Qlk), then it is also dosed, and therefore of the fonn $II=$ G(DIK). Bul G(Dlk) is the disjoint union of the open cosets of H. Since $G(Q$ lk) is compact, a finite number of cosets suffices to cover the group. Thus there is only a finite number of them; $fl = G$ (QI K) has finite index in G(Dlk), and this implie� that Klk has finite degree. □

The topological Galois groups $G =$ G(Dlk) have the special property that there is a fundamental system of neighbourhoods of the neutral clement I E G which consists of nomrnl subgroups. Thi5 property leads us to the abstract, purely group-theoretical notion of a profinite group.

(1.3) Definition. *A* **profinite group** is a *topologic1:d group G which* is Hausdorff and *compact,* and *which* admits a *bm,is of* neighbourhoods *of* I E *G consisting of nonnal* subgroups.

It can be �hown that the last condition is tantamount to G being totally disconnected, i.e., lo the condition that each element of G i� equal to its own connected component. Every dosed 'iubgroup H of G is obviously again a prolinite group. The disjoint coset decompo�ition

$$G = LJa,H$$

shows immediately that H is open if and only if the index $(G$: H) is finite.

Profinite groups are fairly dose relatives of finite groups. They can be reconstituted rather easily from their finite quotients. For the preci'ie de�cription of thi� we need the notion of *prrjective limit,* which naturally occur� in various places in number theory and which we will introduce next.

Exercise **I.** Let LI/..: he a Galois extemion and *Klk* an arbitrary cxten\1on, both contained in a common exlen�ion .!?lk. If *l.* n $K = k$, then the mapping

$$G(LKIK) \to G(Llk), \quad a \mapsto rrj,.$$

is a topological isomorplmm, that i\, an i\omorphi�m ot group\ an<l a homcomorphi\m of topological �paces.

Exercise 2. Given a family of Galois cxtensions m .!?lk, let *Klk* be the of all $K_i|k$, and $K_i'|k$ the composite of cxten\mn� K, lk .\ur.:h that J 1. If K, nK; $= k$ for all i, the one ha� a topological homorphi�m

$$G(Klk) \quad "'TTG(K,lk).$$

1<:xercise 3. A compact Hausdorff group i� total!y disconnected 1f and only 1f its neutral clement admit� a ba�1� of neighbourhood� con�i�ting only of normal �ubgroup�.

Exercise 4. Every quotient *Ci/II* of a protinite group G by a closed normal subgroup *H* i� a profinile group.

Exercise 5. Let G' he the clo�ure of the commutator subgroup of a profimte group, and G"h = G/G'. Show that every homomorphi�m *G* ---+ *A* into an ahelian protimte group factorize� through

§ 2. Projective and Inductive Limits

The notions of projective, resp. inductive limit generalize the operations of inter5ection, resp. union. If {X, LEI is a family of subsets of a topological space *X* which for any two sets *X*, *X*, also contain� the set *X*, n *X*, (re�p. X, U X;), then the projective (resp. inductive) limit of this family is simply de ined by

� *X;* = ,C1 *X*, (resp. � X = ,ld, *X*,).

Writing i::;; if X,-:; *X*, (resp. *X1-:; X1)* makes the indexing 5et / into a *directed system*, i.e., an ordered set in which, for every pair i, *j*, there exi5t5 a /,,_ such that i .:S *k* and *.i* .:S *k*. In the case at hand, such a *k* is given hy *Xk* = *X*, n *X*, (resp. *Xk* = *X* U *X*). For i .:S *j* we denote the inclusion *XJ* c... *X*, (re:-p. *X*, c... *X;)* by */11* and obtain a system *{X,,J;i)* of �et� and maps. The operations of intersection and union are now generalized by replacing the inclusiom *f,1* with arbitrary map5.

(2.1) Definition. *Let I he a directed system. A* projective, *resp.* inductive system over *I* i� a *family* {X;, *f;1* I i, *j* E /, i ::; *j) oftopologirnl space� X, and continuous* maps

f, *X*--------*X*+,. resp. /1,: *X*,--------+ *X*

such *thal one* has *J;,* = *idx* and

fa= *J;J* o *f,1.*, *resp.* *J;1.* = *f1k* of,,

when i .:S *j* .:S *k*.

In order to define the projective. resp. inductive limit of a projective. resp. inductive system *{X1, f,1)*, we make use of the direct product n,,.1 *X*, resp. the disjoint union Li,'=, X.

(2.2) Definition. *The* projective limit

$$X = \varprojlim_{i \in I} X_i$$

of *the projective system* $\{X_i, f_{ij}\}$ *is defined to be the subset*

$$X = \Big\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i \;\Big|\; f_{ij}(x_i) = x_j \quad \text{for} \quad j \le i \Big\}$$

of *the product* $\prod_{i \in I} X_i$.

The product $\prod_{i \in I} X_i$ is equipped with the product topology. If the X_i are Hausdorff, then so is the product, and it contains in this case X as a closed subspace. Indeed, one has

where $X_{ij} = \{ (x_k) \in \prod_k X_k \mid f_{ij}(x_i) = x_j \}$ so that it suffices to show the closedness of the sets X_{ij}. Writing $p_i : \prod_{k \in I} X_k \to X_i$ for the i-th projection, the two maps $f = p_j$, $f = f_{ij} \circ p_i : \prod_{k \in I} X_k \to X_j$ are continuous, and we may write $= \{ x \in \prod_k X_k \mid f(x) = f(x) \}$. But in the Hausdorff case the equation $= f(x)$ defines a closed subset. This representation $X = \bigcap_{i \in I} X_{ij}$ also the following

(2.3) Proposition. *The projective limit* $X = \varprojlim X_i$ *of nonempty compact spaces* X_i *is itself nonempty* and compact.

Proof: If all the X_i are compact, then so is the product $\prod_{i \in I} X_i$, by Tykhonov's theorem, and thus also the closed subset X. Furthermore, $X = \bigcap_{i, j} X_{ij}$ cannot be the empty set if the X_i are nonempty. In fact, as the product $\prod_i X_i$ is compact, there would have to be an intersection of finitely many X_{ij} which is empty. But this is impossible: if all indices i, j entering into this finite intersection satisfy $i, j \le n$, and if $x_n \in X_n$, then the element $(x_i)_{i \in I}$ belongs to this intersection, where we choose $x_i = f_{ni}(x_n)$, for $i \le n$, and arbitrarily for all other i. $\square$

(2.4) Definition. *The* inductive limit

$$X = \varinjlim_{i \in I} X_i$$

of an inductive system $\{X_i, f_{ij}\}$ is *defined* to *be the* quotient

$$X = \Big(\dot{\bigcup_{i \in I}} X_i \Big) \Big/ \sim$$

of *the* disjoint union $\dot{\bigcup}_{i \in I} X_i$, where *we consider* two elements $x_i \in X_i$ and $x_j \in X_j$ equivalent if *there* exists $k \ge i, j$ *such* that

$$f_{ik}(x_i) = f_{jk}(x_j).$$

In the applications, the projective and inductive systems $\{X_i, f_{ij}\}$ that occur will not just be systems of topological spaces and continuous maps, but the X_i will usually be topological groups, rings or modules, etc., and the f_{ij} will be continuous homomorphisms. In what follows, we will deal explicitly only with projective and inductive systems $\{G_i, g_{ij}\}$ of topological groups. But since everything works exactly the same way for systems of rings or modules, these cases may be thought of tacitly as being treated as well.

Let $\{G_i, g_{ij}\}$ be a projective, resp. inductive system of topological groups. Then the projective, resp. inductive limit

$$G = \varprojlim_{i\in I} G_i \quad \text{resp.} \quad G = \varinjlim_{i\in I} G_i$$

is a topological group as well. The multiplication in the projective limit is induced by the componentwise multiplication in the product $\prod_{i\in I} G_i$. In the case of the inductive limit, given two equivalence classes $x, y \in G = \varinjlim_{i\in I} G_i$, one has to choose representatives x_i and y_i in the same G_i in order to define

$$xy = \text{equivalence class of } x_i y_i.$$

We leave it to the reader to check that this definition is independent of the choice of representatives, and that the operation thus defined makes G into a group.

The projections $p_i : \prod_{j\in I} G_j \to G_i$, resp. the inclusions $\iota_i : G_i \to \bigsqcup_{j\in I} G_j$, induce a family of continuous homomorphisms

$$g_i : G \to G_i, \quad \text{resp.} \quad g_i : G_i \to G$$

such that $g_i = g_{ij} \circ g_j$, resp. $g_i = g_j \circ g_{ij}$, for $i \le j$. This family has the following universal property.

(2.5) **Proposition.** *If H is a topological group and*

$$h_i : H \to G_i, \quad \text{resp.} \quad h_i : G_i \to H$$

is a family of continuous homomorphisms such that

$$h_i = g_{ij} \circ h_j, \quad \text{resp.} \quad h_i = h_j \circ g_{ij}$$

for $i \le j$, then there exists a unique continuous homomorphism

$$h : H \to G = \varprojlim_{i\in I} G_i, \quad \text{resp.} \quad h : G = \varinjlim_{i\in I} G_i \to H$$

satisfying $h_i = g_i \circ h$, resp. $h_i = h \circ g_i$, for all $i \in I$.

The easy proof is left to the reader. A **morphism** between two projective, resp. inductive systems $\{G_i, g_{ij}\}$ and $\{G'_i, g'_{ij}\}$ of topological groups is a family of continuous homomorphisms $f_i : G_i \to G'_i$, $i \in I$, such that the diagrams

$$\begin{array}{ccc} G_j & \xrightarrow{f_j} & G'_j \\ {\scriptstyle g_{ij}}\downarrow & & \downarrow{\scriptstyle g'_{ij}} \\ G_i & \xrightarrow{f_i} & G'_i \end{array} \qquad \text{resp.} \qquad \begin{array}{ccc} G_j & \xrightarrow{f_j} & G'_j \\ {\scriptstyle g_{ij}}\uparrow & & \uparrow{\scriptstyle g'_{ij}} \\ G_i & \xrightarrow{f_i} & G'_i \end{array}$$

commute for $i \le j$. Such a family $(f_i)_{i\in I}$ defines a mapping

$$f : \prod_{i\in I} G_i \to \prod_{i\in I} G'_i, \quad \text{resp.} \quad f : \coprod_{i\in I} G_i \to \coprod_{i\in I} G'_i$$

which induces a homomorphism

$$f : \varprojlim_{i\in I} G_i \longrightarrow \varprojlim_{i\in I} G'_i, \quad \text{resp.} \quad f : \varinjlim_{i\in I} G_i \longrightarrow \varinjlim_{i\in I} G'_i .$$

In this way $\varprojlim$, resp. $\varinjlim$, becomes a functor. A particularly important property of this functor is its so-called "exactness". For the inductive limit $\varinjlim$, exactness holds without restrictions. In other words, one has the

(2.6) Proposition. *Let $\alpha : \{G'_i, g'_{ij}\} \to \{G_i, g_{ij}\}$ and $\beta : \{G_i, g_{ij}\} \to \{G''_i, g''_{ij}\}$ be morphisms between inductive systems of topological groups such that the sequence*

$$G'_i \xrightarrow{\alpha_i} G_i \xrightarrow{\beta_i} G''_i$$

is exact for every $i \in I$. Then the induced sequence

$$\varinjlim_{i\in I} G'_i \xrightarrow{\alpha} \varinjlim_{i\in I} G_i \xrightarrow{\beta} \varinjlim_{i\in I} G''_i$$

is also exact.

Proof: Let $G' = \varinjlim G'_i$, $G = \varinjlim G_i$, $G'' = \varinjlim G''_i$. We consider the commutative diagram

$$\begin{array}{ccccc} G'_i & \xrightarrow{\alpha_i} & G_i & \xrightarrow{\beta_i} & G''_i \\ \downarrow{\scriptstyle g'_i} & & \downarrow{\scriptstyle g_i} & & \downarrow{\scriptstyle g''_i} \\ G' & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & G''. \end{array}$$

Let x E G be such lhat /J(x) =I.Then there exist� an i and an x, E G, !>uch that $g_1(x_1)$ =x. As

$$g_i''\beta_i(x_i) = \beta g_i(x_i) = \beta(x) = 1,$$

there exists j � i such that fi, (x_1) equal<; I in C;'. Changing notation, we may therefore as<;ume lhat = I, so that there exists y_1 E C; !>uch that a,(y_1) =x,. Pulling y = we have $u(y)$ =x. □

The projective limit is not exact in complete generality, hut only for compact groups, so that we have the

(2.7) Proposition. *Let a* 1C;.x;$_1$1→ *\G,.x,J) :md f, /G$_1$,g$_1$i)* → */G;^{1}.X;$_1$') be morphisms between projective systems* of compact *topological groups 1,uch that the* sequence

C;� *c,* -1l+ C;'

is exact for *every* i E /. *Then*

� *C;* � Q!!! *G1* -*1*+ fu!! c;'

i.� again an *exact sequence* of *compact topological groups.*

Proof: Let x = (t,),f't E ¥!!! *G,* and *f,(.x)* = I. �o that /J,(t,) = I for all IE/. The prcimagc!> *Y,* � a,-^{1}(.x,) S; *C;* then form a projective of nonempty closed, and hence compact subsets of the *Gf.* By thi-, means that the projective limit Y = fu!! *Y,* S; � *C;* is nonempty, and *a* maps every element y E Y to *.x.* lJ

Now that we have at our disposal the notion of projcclivc limit, we return to our slarting point, the profinite groups. Recall lhat these are the topological groups which are Hausdorff. compacl and totally disconnected, i.e., they admit a basis of neighbourhoods of the neutral element con�isting of normal subgroups. The next proposition show!-. that they are preci�ely the projective limits of finite groups (which we vie\\- as compact topological groups with respect to the di�crctc topology).

(2.8) Proposition. *If G is a profinite group, and if N varies over the open normal subgroups of G, then one has, algebraically as well as topologically, that*

$$G \cong \varprojlim_{N} G/N.$$

If conversely $\{G_i, g_{ij}\}$ is a projective system of finite (or even profinite) groups, then

$$G = \varprojlim_{i} G_i$$

is a profinite group.

Proof: Let G be a profinite group and let $\{N_i \mid i \in I\}$ be the family of its open normal subgroups. We make I into a directed system by defining $i \leq j$ if $N_i \supseteq N_j$. The groups $G_i = G/N_i$ are finite since the cosets of N_i in G form a disjoint open covering of G, which must be finite because G is compact. For $i \leq j$ we have the projections $g_{ij} : G_j \to G_i$ and obtain a projective system $\{G_i, g_{ij}\}$ of finite, and hence discrete, compact groups. We show that the homomorphism

$$f : G \to \varprojlim_{i \in I} G_i, \quad a \mapsto \prod_{i} a_i, \quad a_i = a \bmod N_i,$$

is an isomorphism and a homeomorphism. f is injective because its kernel is the intersection $\bigcap_{i \in I} N_i$, which equals $\{1\}$ because G is Hausdorff and the N_i form a basis of neighbourhoods of 1. The groups

$$U_S = \prod_{i \in S} \{1\} \times \prod_{i \notin S} G_i,$$

with S varying over the finite subsets of I, form a basis of neighbourhoods of the neutral element in $\prod_{i \in I} G_i$. As $f^{-1}(U_S \cap \varprojlim G_i) = \bigcap_{i \in S} N_i$, we see that f is continuous. Moreover, as G is compact, the image $f(G)$ is closed in $\varprojlim G_i$. On the other hand it is also dense. For if $x = (x_i)_{i \in I} \in \varprojlim G_i$, and $x(U_S \cap \varprojlim G_i)$ is a fundamental neighbourhood of x, then we may choose a $y \in G$ which is mapped to x_k under the projection $G \to G/N_k$, where we put $N_k = \bigcap_{i \in S} N_i$. Then $y \bmod N_i = x_i$ for all $i \in S$, so that $f(y)$ belongs to the neighbourhood $x(U_S \cap \varprojlim G_i)$. Therefore the closed set $f(G)$ is indeed dense in $\varprojlim G_i$, and so $f(G) = \varprojlim G_i$. Since G is compact, f maps closed sets into closed sets, and thus also open sets into open sets. This shows that $f : G \to \varprojlim G_i$ is an isomorphism and a homeomorphism.

Conversely, let $\{G_i, g_{ij}\}$ be a projective system of profinite groups. As the G_i are Hausdorff and compact, so is the projective limit $G = \varprojlim G_i$, by (2.3). If N_i varies over a basis of neighbourhoods of the neutral element in G_i which consists of normal subgroups, then the groups

$$U_S = \prod_{i \in S} N_i \times \prod_{i \notin S} G_i ,$$

with S varying over the finite subsets of I, make up a basis of neighbourhoods of the neutral element in $\prod_{i \in I} G_i$ consisting of normal subgroups. The normal subgroups $U_S \cap \varprojlim G_i$ therefore form a basis of neighbourhoods of the neutral element in $\varprojlim G_i$; thus $\varprojlim G_i$ is a profinite group. □

Let us now illustrate the notions of profinite group and projective limit by a few concrete examples.

Example 1: The Galois group $G = G(\Omega|k)$ of a Galois extension $\Omega|k$ is a profinite group with respect to the Krull topology. This was already stated in § 1. If $K|k$ varies over the finite Galois subextensions of $\Omega|k$, then, by definition of the Krull topology, $G(\Omega|K)$ varies over the open normal subgroups of G. In view of the identity $G(K|k) = G(\Omega|k)/G(\Omega|K)$ and of (2.8), we therefore obtain the Galois group $G(\Omega|k)$ as the projective limit

$$G(\Omega|k) \cong \varprojlim_K G(K|k)$$

of the finite Galois groups $G(K|k)$.

Example 2: If p is a prime number, then the rings $\mathbb{Z}/p^n\mathbb{Z}$, $n \in \mathbb{N}$, form a projective system with respect to the projections $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, for $n \geq m$. The projective limit

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

is the ring of p-adic integers (see chap. II, § 1).

Example 3: Let $\mathcal{O}$ be the valuation ring in a $\mathfrak{p}$-adic number field K and $\mathfrak{p}$ its maximal ideal. The ideals $\mathfrak{p}^n$, $n \in \mathbb{N}$, make up a basis of neighbourhoods of the zero element 0 in $\mathcal{O}$. $\mathcal{O}$ is Hausdorff and compact, and so is a profinite ring. The rings $\mathcal{O}/\mathfrak{p}^n$, $n \in \mathbb{N}$, are finite and we have a topological isomorphism

$$\mathcal{O} \xrightarrow{\sim} \varprojlim_n \mathcal{O}/\mathfrak{p}^n, \quad a \mapsto \prod_{n \in \mathbb{N}} (a \bmod \mathfrak{p}^n).$$

The group of units $U = \mathcal{O}^*$ is closed in $\mathcal{O}$, hence Hausdorff and compact, and the subgroups $U^{(n)} = 1 + \mathfrak{p}^n$ form a basis of neighbourhoods of $1 \in U$. Thus

$$U \cong \varprojlim_n U/U^{(n)}$$

i� also a prolinite group. In fact, we have seen all this already in chap. IL 94.

Example 4: The Z/11Z, *n* EN, form a projective <;ystem with respect to the projections ---+ *Z/mZ, nlm,* where the ordering on Ni� now given by divi�ihility, *nlm,* The projective limit

$$2 = � \quad Z/nZ$$

was originally called the **PrUfer ring,** whereas nowaday<; it has become customary to refer to it by the somewhat curt abbreviation "1.cd-haf' (or '·zee-hat"). This ring is to occupy quite an important position in what follow�. It contains subring. The group<; *nZ, n* EN, are preci<;cly the open subgroups and it i� easy to verify that

$$'i;nZ \; � \; Z/nZ.$$

Taking, for each natural number *n,* the prime factorization *n* = TT!' *p''p,* the Chinese remainder theorem implies the decomposition

$$'£./nZ \; � \; \prod_p Z/l^{11}'Z,$$

and passing to the projective limit,

$$Z \; � \; \prod_p nzfl.$$

This takes the natural embedding of Z into Z to the diagonal embedding ;.f,----+ nl' *'llp, a* I---+ *(a.a,a, ...).*

Example 5: for the field IF'*I* with *q* elements, we get bomorphism�

$$G(IFqnlIFq) \; � \; Z/n'll.$$

one for every II E N, by mapping the Frobenius automorphism ip_{11} to I mod *n'll.* Passing to the projective limit give'> an isomorphism

$$G(IFqifq) \; � \; 2$$

which sends the Frobenius automorphism 'PE G(l8',$_1$1fq) to IE Z. and the subfroup (tp) = {'P" | *n* E Z] onto the den�c (but not clo5ed) -,ubgroup J'. of Z. Given this, it i� now clear, in the example at the beginning of this chapter, how we were able to construct an clement ifr E G($W,_1$lf,$_1$) which did not belong to (ip). In fact, looking at it via the i1>omorphism G($W^\circ,_1$llF',$_1$) � Z. what we did amounted to writing down the clement

$$.. ,0,0. lp,0,0, ...) \; E \; \prod_I TZ1 = i.$$

which docs not belong to Z.

Example 6: Let be """-""""""""" obtained by adjoining all roots of unity. Its group is then canonically isomorphic (as a topological group) to the group of units Z* ;:::; nl' Z;, of Z,

G(QIQ) c:e i'.

This isomorphism is obtained by passing to the projective limit from the canonical isomorphisms

$$G(\mathbb{Q}(\mu_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

where μ_{11} denotes the group of fl-th roots of unity.

Example 7: The groups ZI' and Z are (additive) <,pecial ca&cs of the class of **procyclic** groups. These are prolinite groups G which are topologically generated by a single element *a;* i.e., *G* is the closure (a) of the subgroup (a) = {a^{11} I fl E Z). The open subgroups of a procyclic group $C = (a)$ arc all of the form G". Indeed, G^{11} is closed, being the image of the continuous map *G* ---+ *C.* *x* f-'>- x^{11}. and the quotient group *G* / *G"* is finite, because it contains the finite group \a" mod G" IO ::=: v < n) as a dense subgroup, and is therefore c4ual to it. Conver&cly, if *H* is a subgroup of *CJ* of index *n,* then G" �*II*�G and $n =$ (G: H)::: (G: G")::: *n,* so that $H = G^{11}$.

Every procyclic group G is a quotient of the group Z. In fact, if $G =$ (a), then we have for every *n* the surjective homomorphism

'Jl,/11Z---+G/G^{11}, lmodnZf-'>-amodG^{11},

and in of (2.7), pa�sing to the projective limit yields a continuous �urjection------- + *G.*

Example 8: Let *A* be an ahelian torsion group. Then the **Pontryagin dual**

x(A) ~ Hom(A.Q/Z)

is a profinite group. For one has

A~ LJ *A,,*

where *A,* varies over the finite subgroups of *A,* and thus

x(AI = � x(A,)

with finite groups *x(Ai).* If for in5tance,

A = Q/Z = LJ ¼z;:z,
tlE'�1

then $\chi(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$, so that

$$\chi(\mathbb{Q}/\mathbb{Z}) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}.$$

Example 9: If G is any group and N varies over all normal subgroups of finite index, then the profinite group

$$\widehat{G} = \varprojlim_N G/N$$

is called the *profinite completion* of G. The profinite completion of $\mathbb{Z}$, for example, is the group $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$.

Exercise 1. Show that, for a profinite group G, the power map $G \times \mathbb{Z} \to G$, $(\sigma, n) \mapsto \sigma^n$, extends to a continuous map

$$G \times \widehat{\mathbb{Z}} \to G, \quad (\sigma, a) \mapsto \sigma^a,$$

and that one has $(\sigma^a)^b = \sigma^{ab}$, and $\sigma^{a+b} = \sigma^a \sigma^b$, if G is abelian.

Exercise 2. If $\sigma \in G$ and $a = \lim_{i\to\infty} a_i \in \widehat{\mathbb{Z}}$ with $a_i \in \mathbb{Z}$, then $\sigma^a = \lim \sigma^{a_i}$ in G.

Exercise 3. A *pro-p-group* is a profinite group G whose quotients G/N, modulo all open normal subgroups N, are finite p-groups. Imitating exercise 1, make sense of the powers σ^a, for all $\sigma \in G$ and $a \in \mathbb{Z}_p$.

Exercise 4. A closed subgroup H of a profinite group G is called a p-Sylow subgroup of G if, for every open normal subgroup N of G, the group HN/N is a p-Sylow subgroup of G/N. Show:

(i) For every prime number p, there exist a p-Sylow subgroup of G.

(ii) Every pro-p-subgroup of G is contained in a p-Sylow subgroup.

(iii) Every two p-Sylow subgroups of G are conjugate.

Exercise 5. What is the p-Sylow subgroup of $\widehat{\mathbb{Z}}$ and of $\widehat{\mathbb{Z}}^*$?

Exercise 6. If $\{G_i\}$ is a projective system of profinite groups and $G = \varprojlim G_i$, then $G_p = \varprojlim G_{i,p}$ (see § 1, exercise 5).

§ 3. Abstract Galois Theory

Class field theory is the final outcome of a long development of algebraic number theory the beginning of which was Gauss's reciprocity law

(�)(�)� (-1)9'''.

The endeavours to generalize this law finally produced a theory of the abelian extensions of algebraic and p-adic number fields. These extensions LIK are classified by certain subgroups .ML= NL,'KAt. of a group AK attached to the base field. In the local case, AK is the multiplicative group K^* and in the global case it i� a modification of the ideal cla5S group. At the hean of this theory there is a mysterious canonical isomorphism

$$G(L|K) \cong A_K/N_{L|K}A_L,$$

which - if we view things in the right way - encapsulates the reciprocity law in its most general form. Now, this map can be abstracted completely from the field-theoretic situation and treated on a purely group theoretical basis. In this way, class field theory can be given an abstract, but elementary foundation, to which we will now tum.

We begin our considerations by giving ourselves a profinitc group G. The theory we are about to develop is purely group theoretical in nature. However, the only application� we have in mind :lfe field theoretical, and the language of fleld theory allow� immediate insights into the group theoretical relations. We will therefore formally interpret the profinite group G as a Galois group in the following way. (Let us remark in passing that every profinite group is indeed the Galois group $G =$ G(kjk) of a Galois field extension klk; this will allow the reader to rely on his �tandard knowledge of Galoi� theory whenever the formal development in terms of group theory alone would :-eem odd.)

We denote the closed subgroups of G by (h, and call these indices K '•field�"; K will be called the fixed field of GK. The field k such that G� = G is called the base field, and k denotes the field sati:-fying G; = /1). The field belonging to the closure (a) of the cyclic group (o-) = {u' / k E �G/ generated by an element u E G is simply called the fixed field of u.

We write formally K <;: L or LI K if GL <;: GK, and we call the pair /,IK a field extension. LI K i� called a finite extension, if G L i,;, open, i.e.. of llnite index in GA. , and this index

$$[L : K] := (G_K : G_L)$$

will be called the degree of $L|K$. $L|K$ is �aid to be normal or Galois if Ch is a normal wbgroup of G_K. If this is the case, we define the Galois group ofLIKby

$$G(L|K) = G_K/G_L\,.$$

If $N \supseteq L \supseteq K$ arc Galois extensions of K, we define the restriction of an element $a \in G(N|K)$ to L by

$$a|_L = a \bmod G(N|L) \in G(L|K).$$

This gives a homomorphism

$$G(N|K) \longrightarrow G(L|K), \quad a \longmapsto a|_L,$$

\liith kernel $G(N|L)$. The extension $L|K$ is called cyclic, abclian, solvable, etc., if the Galois group $G(L|K)$ has these properties. We put

("intersection")

if G_K is topologically generated by the rnbgroups G_{K_i}, and

$K = \prod K_i$ ("compm.ite")

if $G_K = \bigcap_i G_{K_i}$. If $G_{K'} = a^{-1}G_K a$ for $a \in G$, we write $K' = K^a$.

Now let A be a (*ontinuous multiplicatin'* G-modulc. By this we mean a multiplicative abclian group A on which the elements $a \in G$ operate as automorphisms on the right, $a : A \longrightarrow A$, $a \mapsto a^{\sigma}$. This action must �atisfy

(i) $a^1 = a$,

(ii) $(ab)^{\sigma} = a^{\sigma} b^{\sigma}$,

(iii) $a^{\sigma\tau} = (a^{\sigma})^{\tau}$,

(iv) $A = \bigcup_{[K:k]<\infty} A_K$,

where A_K in the last condition denotes the fixed module A^{G_K} under G_K, so that

$$A_K = \{ a \in A \mid a^{\sigma} = a \text{ for all } \sigma \in G_K \},$$

and where K varie� over all extemions that are finite over k. The condition (iv) says that G operates continuously on A, i.e., the map

$$G \times A \longrightarrow A, \quad (\sigma, a) \longmapsto a^{\sigma},$$

is continuous, where A is equipped with the discrete topology. Indeed. thi.-; continuity b equivalent to the fact that, for every element $(\sigma, a) \in G \times A$, there exist,; an open subgroup $U = G_K$ of G such that the neighbourhood $\sigma U \times \{a\}$ of (σ, a) is mapped to the open -;ct $\{a^{\sigma}\}$, and thi� means simply that $a^{\sigma} \in A^U = A_K$.

Remark: In the exponential notation a^σ, the operation of G on A appears as an action on the right. This notation is adequate for many computations in the case of multiplicative G-modules A. For instance, the notation $a^{\sigma-1} := a^\sigma a^{-1}$ is to be preferred to writing $(\sigma-1)a = \sigma a \cdot a^{-1}$. On the other hand, classical usage often calls for an operation on the left. Thus in the case of a Galois extension $L|K$ of actual fields, the Galois group $G(L|K)$ acts as the automorphism group on L from the left, and therefore also in the same way on the multiplicative group L^*. This occasional switch from the left to the right should not confuse the reader.

For every extension $L|K$ we have $A_K \subseteq A_L$, and if $L|K$ is finite, then we have the norm map

$$N_{L|K}: A_L \to A_K, \quad N_{L|K}(a) = \prod_\sigma a^\sigma,$$

where σ varies over a system of representatives of $G_L \backslash G_K$. If $L|K$ is Galois, then A_L is a $G(L|K)$-module and one has

$$A_L^{G(L|K)} = A_K.$$

At the center of class field theory there is the **norm residue group**

$$H^0\big(G(L|K), A_L\big) = A_K / N_{L|K} A_L.$$

We also consider the group

$$H^{-1}\big(G(L|K), A_L\big) = {}_{N_{L|K}}A_L / I_{G(L|K)} A_L,$$

where

$${}_{N_{L|K}}A_L = \{a \in A_L \mid N_{L|K}(a) = 1\}$$

is the "norm-one group" and $I_{G(L|K)}A_L$ is the subgroup of ${}_{N_{L|K}}A_L$ which is generated by all elements

$$a^{\sigma-1} := a^\sigma a^{-1}$$

with $a \in A_L$, and $\sigma \in G(L|K)$. If $G(L|K)$ is cyclic and σ is a generator, then $I_{G(L|K)}A_L$ is simply the group

$$A_L^{\sigma-1} = \{a^{\sigma-1} \mid a \in A_L\}.$$

In fact, the formal identity $\sigma^k - 1 = (1+\sigma+\cdots+\sigma^{k-1})(\sigma-1)$ implies $a^{\sigma^k-1} = b^{\sigma-1}$ with $b = \prod_{i=0}^{k-1} a^{\sigma^i}$.

Let us now apply the notions introduced so far to the example of **Kummer theory.** For this, we impose on the G-module A the following axiomatic condition.

(3.1) Axiom. One has $H^{-1}(G(L|K),A_L) = 1$ for all *finite cyclic extensions* $L|K$.

The theory we are about to develop makes reference to a surjective G-homomorphism

$$\wp: A \longrightarrow A, \quad a \longmapsto a^{\wp},$$

with finite *cyclic* kernel $\mu_{\wp}$. The order $n = \#\mu_{\wp}$ is called the *exponent* of the operator $\wp$. The case of prime interest to us is when $\wp$ is the n-th power map $a \mapsto a^n$ and $\mu_{\wp} = \mu_n = \{\zeta \in A \mid \zeta^n = 1\}$ is the group of "n-th roots of unity" in A.

We now fix a field K such that $\mu_{\wp} \subseteq A_K$. For every subset $B \subseteq A$, let $K(B)$ denote the fixed field of the closed subgroup

$$H = \{\sigma \in G_K \mid \beta^{\sigma} = \beta \text{ for all } \beta \in B\}$$

of G_K. If B is G_K-invariant, then $K(B)|K$ is obviously Galois. A **Kummer extension** (with respect to $\wp$) is by definition an extension of the form

$$K\big(\wp^{-1}(\Delta)\big) \mid K,$$

where $\Delta \subseteq A_K$. A Kummer extension $K(\wp^{-1}(\Delta))|K$ is always Galois, and its Galois group is abelian of exponent n. Indeed, for an extension $K(\wp^{-1}(a))|K$, we have the injective homomorphism

$$G(K(\wp^{-1}(a))|K) \longrightarrow \mu_{\wp}, \quad \sigma \longmapsto \alpha^{\sigma-1},$$

where $\alpha \in \wp^{-1}(a)$. Since $\mu_{\wp} \subseteq A_K$, this definition does not depend on the choice of α. Thus, for a Kummer extension $L = K(\wp^{-1}(\Delta)) = \prod_{a\in\Delta} K(\wp^{-1}(a))$, the composite map

$$G(L|K) \longrightarrow \prod_{a\in\Delta} G(K(\wp^{-1}(a))|K) \longrightarrow \prod_{a\in\Delta} \mu_{\wp}$$

is an injective homomorphism.

The following proposition says that conversely, any abelian extension $L|K$ of exponent n is a Kummer extension.

(3.2) Proposition. *If $L|K$ is an abelian extension of exponent n, then*

$$L = K\big(\wp^{-1}(\Delta)\big) \quad \textit{with} \quad \Delta = A_L^{\wp} \cap A_K\,.$$

In particular, if $L|K$ is cyclic, then we find $L = K(\alpha)$ with $\alpha^{\wp} = a \in A_K$.

Proof: We havep-^{1}(,1) <;;;; *AL,* for if *x* EA and = *ai;.'* = *a* E *AK,* *a* E *AL,* then *x* = *i;a* E *AL* for some *i;* E µ�) <;;;; *AK.* Therefore K(p-^{1}(L1)) <;;;; *L.* On the other hand, the extension *LIK* is the composite of it5 cyclic subcxtensions. For it is the composite of its *finite* subextensions, and the Galoi5 group of a finite subextension is the product of cyclic groups, which may be interpreted as Galois group5 of cyclic �ubextemions. Let now MI *K* be a cyclic 5Ubextension of LI *K.* It suffices to show that *M* <;;;; K(tJ-^{1}(,1)). Let *a* be a generator of C(MIK) and (a generator Let *d* = [M: *KJ,* = *n/d* and *i;* = *(d'_* Since *NM1K(i;)* = *i;d* = I, <,hows that *i;* = for some *a* E *AM.* Thus *K* £ *K(a)* <;;;; *M.* But *a""* = *i;ia.* Thus *a"'* = *a* is equivalent to i = 0 mod *d,* 50 that *K(a)* = *M.* But *(a�))a-l* = (a"-^{1})t' = *i;l?* = I, �o that *a= a�* E *AK;* then *a* E tJ-^{1}(L1), and therefore *M* £ K(fl-^{1}(L1)). 0

As the main result of general Kummer theory, we now obtain the following

(3.3) **Theorem.** *The* correspondence

$$LI,\_.L�K(i? \quad '(Ll))$$

is a I-I-correspondence *between the* groups Ll *1,uch that Ar* £ L1 <;;;; *AK and the abelian* extensions LI *K* of exponent *n.*

If L1 *and L correspond to* each *other, then* Arn *AK* = Ll*, and* we *have* <i *canonical isomorphism*

$$Ll/Af \;;,: Hom(G(LIK),Jls,)), \quad a \text{ mod } Ai \text{ i----+ } Xa,$$

where the chan1.cter x,, : *G(LIK)-+ /L!f' is given by x"(a)* = *a"-^{1}*, for *U* E fl ^{1}(a).

Proof': Let *LIK* be an abelian extension of exponent *n.* By (3.2), we then find *L* = K(p-^{1}(L1)) with L1 =Arn *AKW.* e consider the homomorphism

$$\text{Ll----+ Hom(C(LIK),}\mu_{61}). \quad a \text{ i----+ } Xa,$$

where *Xa(a)* = a"-^{1}, *a* Ep-^{1}(a). Since

$$Xa = I \;\{=\}\; a'''' \;^1 = I \text{ for all } a \text{ E G(LIK)}$$
$$\{=\} \; a \text{ E } AK \;\{=\}\; a = alf' EA�,$$

it has the kernel *A�.* To prove the surjectivity, we let *X* E Hom(G(LIK), */lp),* *X* defines a cyclic extension MI *K* and is the composite of homomorphisms G(LIK)-+ *G(MIK)* *L* */Li;i-* Let *a* be a generator of *G(MIK).* Since

$N_{M|K}(f(\sigma)) = f(\sigma)^{[M:K]} = 1$, we deduce from (3.1) that $\chi(\sigma) = \alpha^{\sigma-1}$ for some $\alpha \in A_M$. Now, $(\alpha^{\wp})^{\sigma-1} = (\alpha^{\sigma-1})^{\wp} = \chi(\sigma)^{\wp} = 1$, so that $a = \alpha^{\wp} \in A_M^{G(M|K)} = A_K$. For all $\tau \in G(L|K)$ one has $\chi_a(\tau) = \chi(\tau|_M) = \alpha^{\tau-1} = \chi(\tau)$, so that $\chi = \chi_a$. This proves the surjectivity, and we obtain an isomorphism

$$\Delta/A_K^{\wp} \cong \operatorname{Hom}\big(G(L|K), \mu_{\wp}\big).$$

If Δ' is any group between $A_K^{\wp}$ and Δ and if $L' = K(\wp^{-1}(\Delta'))$, then $\Delta' = A_{L'}^{\wp} \cap A_K$. In fact, putting $\Delta'' = A_{L'}^{\wp} \cap A_K$, we have just seen that one has

$$\Delta''/A_K^{\wp} \cong \operatorname{Hom}(G(L'|K), \mu_{\wp}).$$

The subgroup $\Delta'/A_K^{\wp}$ corresponds under Pontryagin duality to the subgroup $\operatorname{Hom}(G(L'|K)/H, \mu_{\wp})$, where

$$H = \{\sigma \in G(L'|K) \mid \chi_a(\sigma) = 1 \text{ for all } a \in \Delta'\}.$$

As $\chi_a(\sigma) = \alpha^{\sigma-1}$ for $\alpha \in \wp^{-1}(a)$, H leaves fixed the elements of $\wp^{-1}(\Delta')$, and as $K(\wp^{-1}(\Delta')) = L'$, we find that $H = 1$, so that $\Delta'/A_K^{\wp} \cong \operatorname{Hom}(G(L'|K)/H, \mu_{\wp}) = \operatorname{Hom}(G(L'|K), \mu_{\wp})$. It follows that $\Delta'/A_K^{\wp} = \Delta''/A_K^{\wp}$, i.e., $\Delta' = \Delta''$.

It is therefore clear that the correspondence $\Delta \mapsto L = K(\wp^{-1}(\Delta))$ is a 1-1-correspondence, as claimed. This finishes the proof of the theorem. □

Remarks and Examples: 1) If $L|K$ is infinite, then $\operatorname{Hom}(G(L|K), \mu_{\wp})$ has to be interpreted as the group of all *continuous* homomorphisms $\chi : G(L|K) \to \mu_{\wp}$, i.e., as the character group of the *topological* group $G(L|K)$.

2) The composite of two abelian extensions of K of exponent n is again of the same type, and all of them lie in the *maximal* abelian extension of exponent n. It is given by $\tilde{K} = K(\wp^{-1}(A_K))$, and for the Pontryagin dual

$$G(\tilde{K}|K)^* = \operatorname{Hom}(G(\tilde{K}|K), \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(G(\tilde{K}|K), \mu_{\wp})$$

we have by (3.3) that

$$G(\tilde{K}|K)^* \cong A_K/A_K^{\wp}$$

3) If k is an actual field of positive characteristic p and $\bar{k}$ is the separable closure of k, then A may be chosen to be the additive group $\bar{k}$ and $\wp$ to be the operator

$$\wp : \bar{k} \to \bar{k}, \quad a \mapsto \wp a = a^p - a.$$

Then axiom (3.1) is indeed satisfied, for we have, in complete generality:

(3.4) Proposition. *For every cyclic finite field extension* L IK, *one has* *H-'(G(LIK), L)* � I.

Proof: The extemion L IK always admits a normal basis *{ac* I *a* E *G(L* IK)}, so that L = ffi,.,. *Koc*. This means that Lis a C(LIK)-induced module in the sen:-e of *7, and then H-^{1}*(G(L* IK), *L)* = 1, by (7.4). 0

The Kummer theory with respect to the operator *pa* = *afi* - *a* is usually called **Artin-Schreier theory.**

4) The chief application of the theory developed above is to the case where G i<; the absolute Galois group G(klk) of an actual field *k, A* is the multiplicative group k^* of the algebraic closure, and *5.J* is then-th power map *a* M *a*^{11}, for some natural number *n* which is relatively prime to the characteristic of A. (in particular, *n* is arbitrary if char(k) = 0). Axiom (3.1) is always satisfied in this ca:-c and is called **Hilbert 90** because thi:- statement occurs as *Sat::* number 90 among the 169 theorems in Hilbert's famow, "Zahlbcricht"' f72J. Thus we have the

(3.5) **Theorem (Hilbert 90).** *For a cyclic licld* extension LI*K one always has*

W'(G(LIK),C) � I.

*In other word*1,:

An element a E *L** of *n01m N1.iK (a)* = **1** is of *the [01m a* = /3"-1. *where f3 EL*� *and a* i.� *a genera/or* ofG(LIK).

Proof: Let 11 = !L: *K].* Ry virtue of the linear independence of the automorphisms I, *a,* ....*an*^{1} (sec [151, chap. *5,* §7, no. 5), there exists an element *y* E *L* * such that

f3=y+ay"+a1.,.."y""+ +a1+,,+·+"/)2y"" i-=/=O.

As *N1.w(a)* = I, one gets *a/3"* = */3*, and thw, *a*= /3^1-". [J

If now the field *K* contains the group *fln* of *n-th* roots of unity, the operator *f)(a)* = *an* has exponent *n,* and we obtain the following corollary, which i� the most important special case of theorem (3.3).

(3.6) Corollary. *Let n be a natural number which is relatively prime to the characteristic of the field K, and assume that $\mu_n \subseteq K$.*

Then the abelian extensions $L|K$ of exponent n correspond 1-1 to the subgroups $\Delta \subseteq K^*$ which contain K^{*n}, via the rule

$$\Delta \mapsto L = K\left(\sqrt[n]{\Delta}\right),$$

and we have

$$G(L|K) \cong \operatorname{Hom}(\Delta/K^{*n}, \mu_n).$$

Hilbert's theorem 90, which is the main basis of this corollary, admits the following generalization to arbitrary Galois extensions $L|K$, which goes back to the mathematician EMMY NOETHER (1882-1935). Let G be a finite group and A a multiplicative G-module. A 1-cocycle, or crossed homomorphism, of G with values in A is a function $f: G \to A$ satisfying

$$f(\sigma\tau) = f(\sigma)^\tau f(\tau)$$

for all $\sigma, \tau \in G$. The 1-cocycles form an abelian group $Z^1(G, A)$. For every $a \in A$, the function

$$f_a(\sigma) = a^{\sigma - 1}$$

is a 1-cocycle, for one has

$$f_a(\sigma\tau) = a^{\sigma\tau - 1} = (a^{\sigma-1})^\tau a^{\tau - 1} = f_a(\sigma)^\tau f_a(\tau).$$

The functions f_a are called 1-coboundaries and form a subgroup $B^1(G, A)$ of $Z^1(G, A)$. We define

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)$$

and obtain as a first result about this group the

(3.7) Proposition. *If G is cyclic, then $H^1(G, A) \cong \hat{H}^{-1}(G, A)$.*

Proof: Let $G = (\sigma)$. If $f \in Z^1(G, A)$, then for $k \geq 1$

$$f(\sigma^k) = f(\sigma^{k-1})^\sigma f(\sigma) = f(\sigma^{k-2})^{\sigma^2} f(\sigma)^\sigma f(\sigma) = \dots = \prod_{i=0}^{k-1} f(\sigma)^{\sigma^i},$$

and $f(1) = 1$ because $f(1) = f(1)f(1)$. If $n = \#G$, then

$$N_G f(\sigma) = \prod_{i=0}^{n-1} f(\sigma)^{\sigma^i} = f(\sigma^n) = f(1) = 1,$$

so that $f(a)$ E $N(; A = \{a$ E $A \mid Nr;a =$ rr=ri $aa' = 1\}$. Conversely we obtain, for every a E A such that $N c;a =$ I, a 1-cocycle by putting $f(o) = a$ and

$$f(ok) = \overset{,\_,}{\textrm{n}}_{!=0} aa'$$

The reader is invited to check this. The map f r+ $f(u)$ therefore i5 an isomorphism between $Z^1(G, A)$ and $N(,A$. This isomorphism maps $B^1(G, A)$ onto *le A*, because f E $8^1(G.A)$<====> $f(al..) =$ a'''-¹ for some fixed a <====> $f(a) = aa\ ^1$ <====} $f''(a)$ E /01\. D

Noclher's generalization of Hilbert's theorem 90 now reads:

(3.8) **Proposition.** *For* a *finite G,itois* field *extension* LI*K, one* has *that*

H'(G(LIK),L') � I

Proof: Let f: G--,)- L^* be a 1-cocyde. For c EL*, we put

$$a� \underset{a<c.GU-IK)}{L} f(a)c''$$

Since the automorphisms a are linearly independent (see rt5], chap. 5, §7, no. 5), we can chom,e c E L^* such that a f. 0. For r E $G(L$ IK), we obtain

$$a'= \underset{''}{L},f(a)r:c''' = \underset{''}{L},f(r)^{-1}f(ur)c''r = f(r)^{-1}a..$$

i.e., $f(r) = W^{-1}$ with $/3 = a^{-1}$. [J

This proposition will only be applied once in thi5 book (see chap. VI. (2.5)).

Exercise **1.** Show that Hilbert 90 in Nocthcr's fonnulation al�o hokb for the additive group L of a Galo1� extension LI*K*.

Hint: U5e the normal basi� theorem.

Exercise 2. Let A. be a field of char<1ctcristic fl and I its separable dosure. For fixed n c". 1, com1der rn the ring of Witt vectors W(K°) (�ee chap. II, IH, exercise 2--6) the additive group $W,.(k)$ of truncated Wilt vector� = (ao.a1, ... ,an-1). Show th.it axiom CU) holds for the G(klk)-module $A=$

Exercise 3. Show that the operator

$$p: W,,(k) \rightarrow W,,(kl, \quad pa = Fa - a,$$

i.-, a homomorphism with cyclil: kernel $p,$, of order p''. Di�cu�� the corre�ponding Kummer theory for the abelian extension� of exponent p''.

Exercise 4. Let G be a profinite group and A a continuous G-module. Put

$$H^1(G, A) = Z^1(G, A)/B^1(G, A),$$

where $Z^1(G, A)$ consists of all continuous : $G \to A$ with respect to the discrete topology on A) such that $(\sigma)^{\prime} f(\tau)$, and $B^1(G, A)$ consists of all functions of the form . Show that if g is a closed normal subgroup of G, then one an exact sequence

$$\to H^1(G/g, A^g) \to H^1(G, A) \to H^1(g, A).$$

Exercise 5. Show that $= \varinjlim H^1(G/N, A^N)$, where N varies over all the open normal subgroups

Exercise 6. If $1 \to A \to B \to C \to 1$ is an exact sequence of continuous G-modules, then one has an exact sequence

$$1 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B) \to H^1(G,C).$$

Remark: The $H^1(G, A)$ is only the first term of a whole series of groups $H^i(G, A)$, $i =$., which are the objects of group cohomology (see [45]). Class field theory can also be built upon this theory (see [10], [108]).

Exercise 7. Even for infinite Galois extensions $L|K$, one has Hilbert's theorem 90: $H^1(G(L|K), L^*) = 1$.

Exercise 8. If n is not divisible by the characteristic of the field K and if μ_n denotes the group of n-th roots of unity in the separable closure $\bar{K}$, then

$$H^1(G_K, \mu_n) \cong K^*/K^{*n}.$$

§ 4. Abstract Valuation Theory

The further development will now be based on a fixed choice of a surjective continuous homomorphism

$$d : G \to \hat{\mathbb{Z}}$$

from the profinite group G onto the procyclic group $\hat{\mathbb{Z}} = \prod_n \mathbb{Z}/n\mathbb{Z}$ (see §2, example 4). This homomorphism will produce a theory which is an abstract reflection of the ramification theory of p-adic number fields. Indeed, in the case where G is the absolute Galois group $G_k = G(\bar{k}|k)$ of a p-adic number field k, such a surjective homomorphism $d : G \to \hat{\mathbb{Z}}$ arises via the maximal unramified extension $\tilde{k}|k$: $\mathbb{F}$, the residue class field of k, then, by chap. II, §9, p. 173 and example 5 in we have canonical isomorphisms

$$G(\tilde{k}|k) \cong G(\bar{\mathbb{F}}|\mathbb{F}) \cong \hat{\mathbb{Z}}$$

which associate to the element I E i the Frobenius automorphi5m $\varphi \in G(\tilde{k}|k)$. It is defined by

$$a'P = a'1 \bmod \mathfrak{p} \quad \text{for} \quad a \text{ E l"ri,}$$

where(), re�p. p, denote the valuation ring of k, resp. its maximal ideal. The homomorphi&m d : G ---+ $S;$ in question i5 then given, in this concrete ca�e. as the compo5ite

$$G \longrightarrow G(\tilde{k}|k) \xrightarrow{\sim} \widehat{\mathbb{Z}}\,|$$

In the abstract situation, the initial choice of a surjective homomorphism d : G ---+ 2 mimics the p-adic case, but the applications of the theory are by no means confined to IJ-adic number field5. The kernel / has a certain fixed field *klk*, and *d* induces an i�omorphism *G(klk)* �

More generally, for any field K we denote by $/_K$ the kernel of the restriction d: *GK*---+ i, and call it the **inertia group** over *K*. Since

fK=GKnl=GKnGr=GK[,

the fixed field K of *IK* i� the composite

K �Kk.

We call *ilK* the **maximal unramified extension** of *K*. We put

(K �(Zcd(GKl). *'K �(I c/K)*

and obtain, when *fK* i5 finite, a surjective homomorphbm

$$dK = \frac{I}{!K} d:GK \text{-------} +Z$$

with kernel $/_K$, and an irnmorphism

$$dK: \text{G(iZIK) .....::::...+ } i.$$

(4.1) Definition. *The element ({!K* E G('f<IK) *such that dd({!K)* = I *is called the* **Frobenius** *over K.*

For a field extcn&ion LI K we define the **inertia degree** *.hw* and the **ramification index** n IK by

$$fi.1K = (d(GK): d(Gd) \quad \text{and} \quad l'LiK = UK: /i).$$

For a tower of field� K £;; L £;; M thi& definition obviou�ly implies that

$$f''1v1,K = .h1K \ fM1L \quad \text{and} \quad e,'vliK = Cf \text{ IK } eMIL.$$

(4.2) Proposition. *For every* extension *LIK* we *have the "fund,imcntal identity"*

[L: *K* J = */L1K CLIK* -

Proof: The exact commutative diagram

I-----+ IL ----+ Gt.-------)' d(GL) ------* I

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow d(G_K) \longrightarrow 1$$

immediately yield<;, if *LIK* is Galob, the exact sequence

I----; *h/IL----;* G(LIK)----; *d(GK)/d(G1)----;* I

If *LIK* is not Galois, we pass to a Galois extension *MIK* containing *L,* and get the result from the above transitivity rules *fore* and *f.* □

LIK b called **unramified** if *e,.,K* = I, i.e., if *L* <;; *i. LIK* is called **totally ramified** if *fLIK* = I, i.e., if *L* n *K* = *K.* In the unramified case, we have the :;.urjective homomorphism

G(KIK) - G(LIK)

and, if *fK* < oo, we call the image *<fJLIK of(f)K* the **Frobenius automorphism** of ***LIK.***

For an arbitrary extem,ion *LIK* one has

l �*LK.*

since *Li* = *LKk* = *Lk* = *L*, and *L* n flK is the maximal unrami!ICd subexlcnsion of LI *K.* It clearly has degree

hiK�*fLnK,Kl.*

Equally obvious is the

(4.3) Proposition. *If fK and fr are finite, then h1K = .fL/fK, and we have the commutative diagram*

GL __d,_, Z

1 lb

GK � *i*

In p:lflicular, one has (l)f. lR =

The Frobenius automorphism governs the entire class field theory like a king. It is therefore most remarkable that in the case of a finite Galois extension $L|K$, every $\sigma \in G(L|K)$ becomes a Frobenius automorphism once it is manœuvered into the right position. This is achieved in the following manner. For what follows, let us assume systematically that $[L:K] < \infty$. We pass from the Galois extension $L|K$ to the extension $\tilde L|K$ and consider in the Galois group $G(\tilde L|K)$ the semigroup

$$\operatorname{Frob}(\tilde L|K) = \{\tilde\sigma \in G(\tilde L|K) \mid d_K(\tilde\sigma) \in \mathbb{N}\}.$$

Observe here that $d_K : G_K \to \hat{\mathbb{Z}}$ factorizes through $G(\tilde L|K)$ because $\tilde K \subseteq \tilde L$; recall also that $0 \notin \mathbb{N}$. Firstly, we have the

(4.4) Proposition. *For a finite Galois extension $L|K$ the mapping*

$$\operatorname{Frob}(\tilde L|K) \longrightarrow G(L|K), \quad \tilde\sigma \longmapsto \tilde\sigma|_L,$$

is surjective.

Proof: Let $\sigma \in G(L|K)$ and let $\varphi \in G(\tilde L|K)$ be an element such that $d_K(\varphi) = 1$. Then $\varphi|_{\tilde K} = \varphi_K$ and $\varphi|_{L\cap\tilde K} = \varphi_{L\cap\tilde K|K}$. Restricting σ to the maximal unramified subextension $L \cap \tilde K|K$, it becomes a power of the Frobenius automorphism, $\sigma|_{L\cap\tilde K} = \varphi^n|_{L\cap\tilde K}$, so we may choose n in $\mathbb{N}$. As $\tilde L = L\tilde K$, we have

$$G(\tilde L|\tilde K) \cong G(L|L\cap\tilde K).$$

If now $\tau \in G(\tilde L|\tilde K)$ is mapped to $\sigma\varphi^{-n}|_L$ under this isomorphism, then $\tilde\sigma = \tau\varphi^n$ is an element satisfying $\tilde\sigma|_L = \tau\varphi^n|_L = \sigma\varphi^{-n}\varphi^n|_L = \sigma$ and $\tilde\sigma|_{\tilde K} = \varphi^n|_{\tilde K}$. Hence $d_K(\tilde\sigma) = n$, and so $\tilde\sigma \in \operatorname{Frob}(\tilde L|K)$. □

Thus every element $\sigma \in G(L|K)$ may be lifted to an element $\tilde\sigma \in \operatorname{Frob}(\tilde L|K)$. The following proposition shows that this lifting, considered over its fixed field, is actually the Frobenius automorphism.

(4.5) Proposition. *Let $\tilde\sigma \in \operatorname{Frob}(\tilde L|K)$, and let Σ be the fixed field of $\tilde\sigma$. Then we have:*

(i) $f_{\Sigma|K} = d_K(\tilde\sigma)$, (ii) $[\Sigma : K] < \infty$, (iii) $\tilde\Sigma = \tilde L$, (iv) $\tilde\sigma = \varphi_\Sigma$.

Proof: (i) $\Sigma \cap \tilde K$ is the fixed field of $\sigma|_{\tilde K} = \varphi_K^{d_K(\sigma)}$, so that

$$f_{\Sigma|K} = [\Sigma \cap \tilde K : K] = d_K(\sigma).$$

(ii) One has $\tilde K \subseteq \tilde\Sigma = \Sigma\tilde K \subseteq \tilde L$: thus

$$e_{\Sigma|K} = (\tilde\Sigma : \tilde K) = \#G(\tilde\Sigma|\tilde K) \le \#G(\tilde L|\tilde K)$$

is finite. Therefore $[\Sigma : K] = f_{\Sigma|K}e_{\Sigma|K}$ is finite as well.

(iii) The canonical surjection $\Gamma = G(\tilde L|\Sigma) \to G(\tilde\Sigma|\Sigma) \cong \hat{\mathbb Z}$ has to be bijective. For since $\Gamma = \overline{\langle\sigma\rangle}$ is procyclic, one finds $(\Gamma : \Gamma^n) \le n$ for every $n \in \mathbb N$ (see § 2). Thus the induced maps $\Gamma/\Gamma^n \to \hat{\mathbb Z}/n\hat{\mathbb Z}$ are bijective and so is $\Gamma \to \hat{\mathbb Z}$. But $G(\tilde L|\Sigma) = G(\tilde\Sigma|\Sigma)$ implies that $\tilde L = \tilde\Sigma$.

(iv) $f_{\Sigma|K}d_\Sigma(\sigma) = d_K(\sigma) = f_{\Sigma|K}$; thus $d_\Sigma(\sigma) = 1$, and so $\sigma = \varphi_\Sigma$. □

Let us illustrate the situation described in the last proposition by a diagram, which one should keep in mind for the sequel.

$$\begin{tikzcd}
 & L \arrow[rr, dash, "\varphi_L"] & & \tilde L = \tilde\Sigma \arrow[dd, dash] \\
 & & \Sigma \arrow[ur, dash, "\tilde\sigma = \varphi_\Sigma"'] & \\
K \arrow[ur, dash, "f_{L|K}"] \arrow[urr, dash, "f_{\Sigma|K}"'] \arrow[rrr, dash, "\varphi_K"'] & & & \tilde K
\end{tikzcd}$$

All the preceding discussions arose entirely from the initial datum of the homomorphism $d : G \to \hat{\mathbb Z}$. We now add to the data a multiplicative G-module A, which we equip with a homomorphism that is to play the role of a henselian valuation.

(4.6) Definition. *A* **henselian valuation** *of A_k with respect to $d: G \to \hat{\mathbb Z}$ is a homomorphism*

$$v : A_k \to \hat{\mathbb Z}$$

satisfying the following properties:

(i) $v(A_k) = Z \supseteq \mathbb Z$ *and* $Z/nZ \cong \mathbb Z/n\mathbb Z$ *for all* $n \in \mathbb N$,

(ii) $v(N_{K|k}A_K) = f_K Z$ *for all finite extensions* $K|k$.

Exactly like the original homomorphism $d : G_k \to \hat{\mathbb Z}$, the henselian valuation $v : A_k \to \hat{\mathbb Z}$ has the property of reproducing itself over every finite extension K of k.

(4.7) Proposition. For every field K which is finite over k, the formula

$$v_K = \frac{1}{f_K}\, v \circ N_{K|k} : A_K \longrightarrow \mathbb{Z}$$

defines a surjective homomorphism satisfying the following properties:

(i) $v_K = v_{K^\sigma} \circ \sigma$ for all $\sigma \in G$.

(ii) For every finite extension $L|K$, one has the commutative diagram

$$\begin{tikzcd} A_L \arrow[r, "v_L"] \arrow[d, "N_{L|K}"'] & \mathbb{Z} \arrow[d, "f_{L|K}"] \\ A_K \arrow[r, "v_K"] & \mathbb{Z} \end{tikzcd}$$

Proof: (i) If τ runs through a system of representatives of G_k/G_K, then $\sigma^{-1}\tau\sigma$ sweeps across a system of representatives of $\sigma^{-1}G_k\sigma/\sigma^{-1}G_K\sigma = G_k/G_{K^\sigma}$. Hence we have, for $a \in A_K$,

$$v_{K^\sigma}(a^\sigma) = \frac{1}{f_{K^\sigma}} v\Big(\prod_\tau a^{\sigma\sigma^{-1}\tau\sigma}\Big) = \frac{1}{f_K} v\Big(\big(\prod_\tau a^\tau\big)^\sigma\Big) = \frac{1}{f_K} v(N_{K|k}(a))$$
$$= v_K(a).$$

(ii) For $a \in A_L$ one has:

$$f_{L|K}\, v_L(a) = f_{L|K} \frac{1}{f_L} v(N_{L|k}(a)) = \frac{1}{f_K} v(N_{K|k}(N_{L|K}(a)))$$
$$= v_K(N_{L|K}(a)) \qquad \square$$

(4.8) Definition. *A* **prime element** of A_K is an element $\pi_K \in A_K$ such that $v_K(\pi_K) = 1$. We put

$$U_K = \{u \in A_K \mid v_K(u) = 0\}.$$

For an unramified extension $L|K$, that is, an extension such that $f_{L|K} = [L:K]$, we have from (4.7), (ii) that $v_L|_{A_K} = v_K$. In particular, a prime element of A_K is itself also a prime element of A_L. If on the other hand, $L|K$ is totally ramified, i.e., $f_{L|K} = 1$, and if π_L is a prime element of A_L, then $\pi_K = N_{L|K}(\pi_L)$ is a prime element of A_K.

Exercise I. Assume that every closed abelian suhgroup of G is procyclic Let K lk be a fimte extension. A **microprime** p of K is by definition a conJugacy da�� \u) � GK of some Frobenius element u E Frob(klK) which i� not a proper power um, $11 > 1$, of some other Froheniu� element a' E Frob([IK). Let �pc<.:(K) he the set of a!l microprimes of K. Show that 1f LIK is a finite extension, then there i� a canonical mapping

:r: spee(L) → �rec(K).

Ahove any m1cropnmc p there are only finitely many mieroprime\ � of L. i.e., the set JT^{-1}(p) is finite. We write �IP to mean� E Jr^{1}(p).

Exercise 2. For a finite exten�ion LIK and a mieropnmc �IP of L, let $h.11p$ = d(�)/d(p). Show that

Exercise 3. For an infinite exten�ion L IK, let

�ree(L) = 1i._t!! �pee(L..,),

$L''IK$ vane� over the finite subextensions of $L]K$. Whal are the m1eroprime�

Exercise **4.** Show that 1f LIK i� Galoi�. then the Galoi� group G([,IK) operate� tran�it1vely on spce(L). The "decomposition group"

G,:μ(LIK) = (a E G(LIK) IW = �I

and if z_{13}= L(.,,pi/lKI is the "dc<.:0mpo�1tion field"' of� E �pec(L), then is unramified.

§ 5. The Reciprocity Map

Continuing with the nolation of the previous section, we consider again a profinite group G, a continuous G-module A, and a pair of homomorphisms

d: G --+ **Z,** v: $A1$- --+ **Z.**

such that d is continuous and surjeclivc and v is a henselian valuation with respect to d. In the following we introduce the convention that the letter K, whenever it occurs without embellishment� or commentary to the contrary, will alway� denote a field *offinite* degree over k. We furthermore impose the following axiomatic condition, which will be systematically a%umed in lhc sequel.

(5.1) Axiom. *For* every *unrnmitied* finite *extension LIK one has*

H'(G(LIK),U,)�1 foe ;�o,-1,

For an infinite extension $L|K$ we set

$$N_{L|K}A_L = \bigcap_M N_{M|K}A_M,$$

with $M|K$ varying over the finite subextensions of $L|K$.

Our goal is to define a canonical homomorphism

$$r_{L|K} : G(L|K) \longrightarrow A_K/N_{L|K}A_L,$$

for every finite Galois extension $L|K$. To this end, we pass from $L|K$ to the extension $\tilde{L}|K$ and define first a mapping on the semigroup

$$\mathrm{Frob}(\tilde{L}|K) = \{\sigma \in G(\tilde{L}|K) \mid d_K(\sigma) \in \mathbb{N}\}.$$

(5.2) Definition. *The* **reciprocity map**

$$r_{\tilde{L}|K}: \mathrm{Frob}(\tilde{L}|K) \longrightarrow A_K/N_{\tilde{L}|K}A_{\tilde{L}}$$

is defined by

$$r_{\tilde{L}|K}(\sigma) = N_{\Sigma|K}(\pi_\Sigma) \bmod N_{\tilde{L}|K}A_{\tilde{L}},$$

where Σ is the fixed field of σ and $\pi_\Sigma \in A_\Sigma$ is a prime element.

Observe that Σ is of finite degree over K by (4.5), and σ becomes the Frobenius automorphism φ_Σ over Σ. The definition of $r_{\tilde{L}|K}(\sigma)$ does not depend on the choice of the element π_Σ. For another one differs from π_Σ only by an element $u \in U_\Sigma$, and for this we have $N_{\Sigma|K}(u) \in N_{\tilde{L}|K}A_{\tilde{L}}$, so that $N_{\Sigma|K}(u) \in N_{M|K}A_M$ for every finite Galois subextension $M|K$ of $\tilde{L}|K$. To see this, we may clearly assume that $\Sigma \subseteq M$. Applying (5.1) to the unramified extension $M|\Sigma$, one finds $u = N_{M|\Sigma}(\varepsilon)$, $\varepsilon \in U_M$, and thus

$$N_{\Sigma|K}(u) = N_{\Sigma|K}(N_{M|\Sigma}(\varepsilon)) = N_{M|K}(\varepsilon) \in N_{M|K}A_M.$$

Next we want to show that the reciprocity map $r_{\tilde{L}|K}$ is multiplicative. To do this, we consider for every $\sigma \in G(\tilde{L}|K)$ and every $n \in \mathbb{N}$ the endomorphisms

$$\sigma - 1: A_{\tilde{L}} \longrightarrow A_{\tilde{L}}, \qquad a \longmapsto a^{\sigma-1} = \sigma a/a,$$

$$\sigma_n: A_{\tilde{L}} \longrightarrow A_{\tilde{L}}, \qquad a \longmapsto a^{\sigma_n} = \prod_{i=0}^{n-1} a^{\sigma^i}.$$

In formal notation, this gives $\sigma_n = \frac{\sigma^n - 1}{\sigma - 1}$, and we find that

$$(\sigma - 1)\circ\sigma_n = \sigma_n \circ (\sigma - 1) = \sigma^n - 1.$$

Now we introduce the homomorphism

$$N = N_{\tilde{L}|K}: A_{\tilde{L}} \longrightarrow A_K$$

and prove two lemmas for it.

(5.3) **Lemma.** Let *'P, a* E Frob(LI K) *with dK* (({}) = I, *dK(a) = n. If E is the fixed field* of *a and a* E Ar, *then*

$$N_{\Sigma|K}(a) = (N \circ \varphi_n)(a) = (\varphi_n \circ N)(a).$$

Proof: The maximal unramified subextension E^0 = *EnK* IK is of degree 11, and its Galois group $G(E^01K)$ j5 generated by the Frobenius automorphi<;m if!ro$_1$K = if!Kl1::11 = 'PIKlrn ='Piro.Consequently, = lf)nlAro· On the other hand, one has *EK = I* and *E* n *K* = and therefore *N*EIE11 =*NIA,,-* For *a* E Ar we thus get

N:r:1da) = Nrn,K(Nr1E11(a)) = *N(a)<P" = N(a<P").*

The Ja,;t equation follows from *tpG('i* I*K) = GCL*IR *)ip.* □

The subgroup $I_{G(\tilde{L}|\tilde{K})}U_{\tilde{L}}$, which is generated by all elements of the fonnu'1,uE $J_{\tilde{L}}$, $\tau \in G(\tilde{L}|\tilde{K})$, is mapped to 1 by the homomorphism *N = NL1R: Ur* ---+$U_{\tilde{K}}$. We therefore obtain an induced homomorphism

N: *Ho(G(liK).Vr)* ------+ *UR*

on the quotient group Ho(G(lli<). *Ur) = ULf /G(liRiU[-* For this group, we have the following lemma.

(5.4) Lemma. *lfx* E H_0(G(lli<), *U[)* is *fixed by* an *element ,;p* E G(LIK) such *rhatdK(<{') =* I, *i.e.,.t'f" =x, then*

$$N(x) \in N_{\tilde{L}|K}U_{\tilde{L}}.$$

Proof: Let *x = u* mod */G(TiKiU[,* with ,li,o-l = I, sothat

(*) *u<P* ^{1} = *hu*�'-^{1}. *u$_1$ EU[,* r, EG(Lli).
I=I

Let MI *K* be a finite Galois subcxtension of LI*K.* In order to prove that *N(u)* E *NM'KUM,* we may assume that *u.u,* E *UM* and *L* � *M.* Let *n* = [M : *K*]. *a = ipn* and let *E* 2 *M* be the fixed Held of *a.* Further, let *E$_{11}$*lL be the unramified extension of degree *n.* i.e.. the fixed field of *a" =({)'};,By* (5.1), we can then find element5 *{i, il$_1$* E *UE,,* such that

$$u = N_{\Sigma_n|\Sigma}(\tilde{u}) = \tilde{u}^{\sigma_n}, \quad u_i = N_{\Sigma_n|\Sigma}(\tilde{u}_i) = \tilde{u}_i^{\sigma_n}.$$

By (*), the elements $\tilde\pi^{\varphi-1}$ and $\pi_1^{\varphi-1}$ only differ by an element $x \in U_{\tilde L}$ such that $x = 1$. Hence – again by (5.1) – they differ by an element of the form y with $y \in U_{\tilde\Sigma_1}$. We may thus write

$$\tilde\pi^{\varphi-1} = y^{\varphi-1}\pi_1^{\varphi-1} = (y\pi_1)^{\varphi-1}.$$

Applying N gives $N(\tilde u)^{\varphi-1} = N(y\pi_1)^{\varphi-1}$, so that

$$N(\tilde u) = N(y\pi_1)\, z,$$

for some $z \in U_{\tilde K}$ such that $z^{\varphi-1} = 1$; therefore $z \in U_K$. Finally, applying σ, and putting $y' = y = N(y) \in U_\Sigma$, we obtain, observing $n = [M : K]$ and using (5.3), that

$$N(u) = N(\tilde u) = N(y\pi_1) z^{n} = N(y\pi_1)$$
$$= N_{\Sigma|K}(y) N_{M|K}(z) \in N_{M|K}U_M, \qquad \square$$

(5.5) Proposition. *The reciprocity map*

$$r_{L|K} : \mathrm{Frob}(L|K) \to A_K/N_{L|K}A_L$$

is multiplicative.

Proof: Let $\sigma_1\sigma_2 = \sigma_3$ be an equation in $\mathrm{Frob}(L|K)$, $n_i = d_K(\sigma_i)$, Σ_i the fixed field of σ_i and $\pi_i \in A_{\Sigma_i}$ a prime element, for $i = 1, 2, 3$. We have to show that

$$N_{\Sigma_1|K}(\pi_1)N_{\Sigma_2|K}(\pi_2) \equiv N_{\Sigma_3|K}(\pi_3) \mod N_{L|K}A_L.$$

Choose a fixed $\varphi \in G(\tilde L|K)$ such that $d_K(\varphi) = 1$ and put

$$\tau_i = \sigma_i^{-1}\varphi^{n_i} \in G(\tilde L|\tilde K).$$

From $\sigma_1\sigma_2 = \sigma_3$ and $n_1 + n_2 = n_3$, we then deduce that

$$\tau_3 = \sigma_2^{-1}\sigma_1^{-1}\varphi^{n_2+n_1} = \sigma_2^{-1}\varphi^{n_2}(\varphi^{-n_2}\sigma_1\varphi^{n_2})^{-1}\varphi^{n_1}.$$

Putting $\sigma_4 = \varphi^{-n_2}\sigma_1\varphi^{n_2}$, $n_4 = d_K(\sigma_4) = n_1$, $\Sigma_4 = \Sigma_1^{\varphi^{n_2}}$, $\pi_4 = \pi_1^{\varphi^{n_2}} \in A_{\Sigma_4}$ and $\tau_4 = \sigma_4^{-1}\varphi^{n_4}$, we find $\tau_3 = \tau_2\tau_4$ and

$$N_{\Sigma_4|K}(\pi_4) = N_{\Sigma_1|K}(\pi_1).$$

We may therefore pass to the congruence

$$N_{\Sigma_3|K}(\pi_3) \equiv N_{\Sigma_2|K}(\pi_2) N_{\Sigma_4|K}(\pi_4) \bmod N_{\tilde{L}|K} A_{\tilde{L}}$$

the proof of uses the identity $\tau_1 = r_2$r--1. From (5.3), we have Nr,1K(rr,) = Thus, if we put

$$u = \pi_3^{\varphi_{n_3}} \pi_4^{-\varphi_{n_4}} \pi_2^{-\varphi_{n_2}}$$

then the congruence amounts simply to the relation *N(u)* E *N[1KA[,* For this, however. lemma (5.4) gives us all that we need.

Since *if!n,* o (tp - I) = *i:pn,* - I and rr;,'11, 1 = rriT' P 1 '-I= rr,r,-l, we have

$$u^{\varphi - 1} = \pi_3^{\tau_3 - 1} \pi_4^{1 - \tau_4} \pi_2^{1 - \tau_2}$$

From the identity $\tau_1 = \tau_2\tau_4$, it follow5 that (T3 - I)+ (I - T2) + (I - T4) = (I - T2)(I - T--1)- Putting now

$$\pi_3 = u_3\pi_4, \quad \pi_2 = u_2^{-1}\pi_4, \quad \pi_4^{\tau_2} = u_4\pi_4, \quad u, \text{ E } Ur,,$$

we obtain

u'f'-1 = $\prod_{1=2}$ u;•-1.

For the element *x* = *u* mod *lu(LIR)Ul* E Ho(G(lli<). *Ur),* this mcam that *x'P-1* = I, and so *x<P* = *x;* then by (5.4), we do get *N(u)* = *N(x)* E

From the surjectivity of the mapping

Frob(i:IK) - G(LIK)

and the fact that *NrwAL* S; *NL1KAL,* wc now have the

(5.6) **Proposition.** For *every Jinitc* Galois extension LI*K, there is* a *canonical homomorphism*

$$r_{L|K} : G(L|K) \longrightarrow A_K / N_{L|K} A_L$$

given by

rL1K(u) = N1:1drrr) mod *Ni* iK *At,*

where Eis the fixed *field* ofa preimage *a-* E Frob([jK) *ofa* E G(L IK) mid rrr E *Ar is* a prime element. *It* is *called the* **reciprocity homomorphism** *ofLIK.*

Proof: We first show thal the definition of *r1. K(a)* is independent of the choice of the preimage *a* E *Frob(L IK)* of *a.* For thi�. let *a-'* E Frob(L I K) be another preimage, *L'* its fixed field and *7rl.'"* E *Az·* a prime clement. *IfdK(fi) = dK(6¹),* lhen *&IK = &'IK* and Ult.= &'IL, so that *fr= 5¹,* and there is nothing to show. However, if we have, say, *dK(ff) <* then *a-'*= &f for some f E Frob(LIK), and flL = I. The lixed field off contain� *L,* so = N:r;,,1K(nz•,) = I mod *NLIK AL.* It follow� therefore that = *rl₁K(6)r[₁K(f)* = rz:₁K(&).

The fact that the mappi� is a homomorphism now follow� directly from (5.5): if 5₁.52 E Frob(LIK) are preimages of *a₁,a₂* E *G(LIK),* then *ffi = ff1ff2* is a preimage of o-_i = *a1a2.* □

The definition of the reciprocity map cxprcssc� the fundamental principle of clas� field theory to the effect that Frobenius automorphisms correspond to prime clements: the element er= *r.p:r;* E GilL) is map_ped to *lfl."* E *Ar;* for reasons of functoriality, the inclusion G(LIL) '--+ *G* (LI *K)* corresponds to the norm map Nr1K: *A:r;-----+ AK,* So the definition of *rL₁K(cr)* is already forced upon us by these requirements. This principle appears at its purest in the

(5.7) **Proposition.** *If LjK* i.� *an unramified extension, /hen the reciprocity map*

$$r_{L|K} : G(L|K) \longrightarrow A_K/N_{L|K}A_L$$

is given by

$$r_{L|K}(\varphi_{L|K}) = \pi_K \bmod N_{L|K}A_L,$$

and is an *isomorphism.*

Proof: In this case one has *l* =Kand *'PK* E *G(i<IK)* b a prcimage of *'PLIK* with fixed field *K,* i.e., *l"L1K('Pt.1K) = lfK* mod *NL1KAL-* The fact that we have an isomorphism is seen from the composite

G(LIK)------,)- AK/NL1KAL------,)- Z/nZ � *'ll./n'll.,*

with *n* = [/, : *K],* where the �econd map is induced hy the valuation *VK* : *AK -----+* Z because '.;; *nZ.* ll is an isomorphism, for if *VK(a)* = 0 mod *nZ.* then *a=* and 5incc *u* = *NLIK(t,)* for �ome FE *UL,* by (5.1), we flnd *a=* = I mod *N,_₁KAJ.*. On the side of the homomorphisms, the generators *'PL K, nK* mo<l *NLIK AL.* and I mod *nZ* correspond to each other, and everything is proved. D

The reciprocity homomorphism *rt.IK* exhibits the following functorial behaviour.

(5.8) Proposition. *Let $L|K$ and $L'|K'$ be finite Galois extensions, such that $K \subseteq K'$ and $L \subseteq L'$, and let $\sigma \in G$. Then we have the commutative diagrams*

$$\begin{tikzcd} G(L'|K') \arrow[r, "r_{L'|K'}"] \arrow[d] & A_{K'}/N_{L'|K'}A_{L'} \arrow[d, "N_{K'|K}"] \\ G(L|K) \arrow[r, "r_{L|K}"] & A_K/N_{L|K}A_L \end{tikzcd} \qquad \begin{tikzcd} G(L|K) \arrow[r, "r_{L|K}"] \arrow[d, "\sigma^*"] & A_K/N_{L|K}A_L \arrow[d, "\sigma"] \\ G(L^\sigma|K^\sigma) \arrow[r, "r_{L^\sigma|K^\sigma}"] & A_{K^\sigma}/N_{L^\sigma|K^\sigma}A_{L^\sigma} \end{tikzcd}$$

where the vertical arrows on the left are given by $\sigma' \mapsto \sigma'|_L$, resp. by the conjugation $\tau \mapsto \sigma^{-1}\tau\sigma$.

Proof: Let $\sigma' \in G(L'|K')$ and $\sigma = \sigma'|_L \in G(L|K)$. If $\tilde\sigma' \in \mathrm{Frob}(\tilde L'|K')$ is a preimage of σ', then $\tilde\sigma = \tilde\sigma'|_{\tilde L} \in \mathrm{Frob}(\tilde L|K)$ is a preimage of σ such that $d_K(\tilde\sigma) = f\, d_{K'}(\tilde\sigma')$, $f \in \mathbb{N}$. Let Σ' be the fixed field of $\tilde\sigma'$. Then $\Sigma = \Sigma' \cap \tilde L$ is the fixed field of $\tilde\sigma$ and $f_{\Sigma'|\Sigma} = 1$. If now $\pi_{\Sigma'} \in A_{\Sigma'}$ is a prime element of Σ', then $\pi_\Sigma = N_{\Sigma'|\Sigma}(\pi_{\Sigma'}) \in A_\Sigma$ is a prime element of Σ. The commutativity of the diagram on the left therefore follows from the equality of norms

$$N_{\Sigma|K}(\pi_\Sigma) = N_{\Sigma|K}(N_{\Sigma'|\Sigma}(\pi_{\Sigma'})) = N_{\Sigma'|K}(\pi_{\Sigma'}) = N_{K'|K}(N_{\Sigma'|K'}(\pi_{\Sigma'}))$$

On the other hand, let $\tau \in G(L|K)$, and let $\tilde\tau$ be a preimage in $\mathrm{Frob}(\tilde L|K)$ with fixed field Σ, and $\tilde\sigma \in G$ a lifting of σ to $\tilde K$. Then Σ^σ is the fixed field of $\tilde\sigma^{-1}\tilde\tau\tilde\sigma$, and if $\pi \in A_\Sigma$ a prime element of Σ, then $\pi^\sigma \in A_{\Sigma^\sigma}$ is a prime element of Σ^σ. The commutativity of the diagram on the right therefore follows from the equality of norms

$$N_{\Sigma^\sigma|K^\sigma}(\pi^\sigma) = N_{\Sigma|K}(\pi)^\sigma . \qquad \square$$

Another very interesting functorial property of the reciprocity map is obtained via the *transfer (Verlagerung* in German). For an arbitrary group G, let G' denote the commutator subgroup and write

$$G^{ab} = G/G'$$

for the maximal abelian quotient group. If then $H \subseteq G$ is a subgroup of finite index, we have a canonical homomorphism

$$\mathrm{Ver}: G^{ab} \longrightarrow H^{ab},$$

which is called **transfer from G to H**. This homomorphism is defined as follows (see [75], chap. IV, § 1).

Let R be a system of representatives for the left cosets of H in G, $G = \bigcup \rho H$, $1 \in R$. If $\sigma \in G$ we write, for every $\rho \in R$,

$$\sigma\rho = \rho'\sigma_\rho, \quad \sigma_\rho \in H, \quad \rho' \in R,$$

and we define

$$\operatorname{Ver}(\sigma \bmod G') = \prod_{\rho \in R} \sigma_\rho \bmod H'.$$

Another description of the transfer results from the double coset decomposition

$$G = \bigcup_\tau \langle\sigma\rangle\tau H$$

of G in terms of the subgroups $\langle\sigma\rangle$ and H. Letting $f(\tau)$ denote the smallest natural number such that $\sigma_\tau = \tau^{-1}\sigma^{f(\tau)}\tau \in H$, one has $H \cap (\tau^{-1}\langle\sigma\rangle\tau) = \langle\sigma_\tau\rangle$, and we find that

$$\operatorname{Ver}(\sigma \bmod G') = \prod_\tau \sigma_\tau \bmod H'.$$

This formula is obtained from the one above by choosing for R the set $\{\sigma^i\tau \mid i = 0, \dots, f(\tau)-1\}$. Applying this to the reciprocity homomorphism

$$r_{L|K} : G(L|K)^{ab} \longrightarrow A_K/N_{L|K}A_L$$

we get the

(5.9) **Proposition.** Let $L|K$ be a finite Galois extension and K' an intermediate field. Then we have the commutative diagram

$$\begin{tikzcd}
G(L|K')^{ab} \arrow[r, "r_{L|K'}"] & A_{K'}/N_{L|K'}A_L \\
G(L|K)^{ab} \arrow[r, "r_{L|K}"] \arrow[u, "\mathrm{Ver}"] & A_K/N_{L|K}A_L, \arrow[u]
\end{tikzcd}$$

where the arrow on the right is induced by inclusion.

Proof: Let us write temporarily $G = G(\tilde L|K)$ and $H = G(\tilde L|K')$. Let $\sigma \in G(L|K)$, and let $\tilde\sigma$ be a preimage in $\operatorname{Frob}(\tilde L|K)$ with fixed field Σ and $S = G(\tilde L|\Sigma) = \langle\tilde\sigma\rangle$. We consider the double coset decomposition $G = \bigcup S\tau H$ and put $S_\tau = \tau^{-1}S\tau \cap H$ and $\tilde\sigma_\tau = \tau^{-1}\tilde\sigma^{f(\tau)}\tau$ as above. Let

$\bar G = G(L|K)$, $\quad \bar H = G(L|K')$, $\quad \bar S = \langle\sigma\rangle$, $\quad \bar\tau = \tau|_L$ and $\sigma_\tau = \tilde\sigma_\tau|_L$.
Then we obviously have

$$\bar G = \bigcup \bar S\,\bar\tau\,\bar H,$$

and therefore

Ver(a mod $G(LIK)^{1}$) $=$**9** ar mod $G(LIK')'$

For every r. let w, vary over a sy�tem of right co:-.ct representatives of H/S,. Then one has

and G =

Let Er be the fixed field of a-,, i.e., the fixed field of S,. rr is the fixed field of r-^{1}ur so that Er IE' is the unramified subextension of degree f(r) in /,IE'. If now n E A_r is a prime element of E, then :rr' E Azr fr, a prime element of $.E'$, and thus also of $.E$,. In view of the above double cosct decomposition, we therefore find

Nc:1K(rr) � }J,,,W, � 9(D(rr')"") �9 Nr,1K'(rr').

and since a, E Froh(Z'IK') is a preimage of a, E $G(L$ IK'), it follows that

rL1da) = nrLIK'(a,) =r1IK'(f1a,) =r1!K'(Yer(a mod G(LIK')).

D

Exerci<,e **1.** Let /. I K he ahelian and totally ramified. and let JT be a prime ck:mcnt of AL. If then a E $G(LIK)$ and

with y E: Ur., then = $N(y)$ mod $N_{11}KA_1$, where N = NrR (B.D1toRK, �ee [122], chap. XIII,

Exercise **2.** Generalue the theory developed so far m the following way. Let P he a set of prime number� and let G be a pru-P-group, i.e., a protinite group allot who�e G/ N by open normal subgroup� N have order divisible onl) by prnne� P

Let d: Ci ---+ Zp be a surJective humumorphi\m onto the group $\mathbb{Z}_P = \prod_{p \in P} \mathbb{Z}_p$ and let A be a G-module. A **henselian P-\-aluation** wllh respect to d is by definition a homomorphi\m

which sati�lie� the fullowmg propenie\:

=Z2Zand � $Zjr(,£$ for all natural number� n which are only by primes in

(ii) t·(NrnAA·l = {KL fur all finite extemiom Klk, where fK = {d(G): $d(G$�)).

Under the hypothesis that $H^i(G(L|K), U_L) = 1$ for $i = 0, -1$, for all unramified extensions $L|K$, prove the existence of a canonical reciprocity homomorphism $r_{L|K} : G(L|K)^{ab} \to A_K/N_{L|K}A_L$ for every finite Galois extension $L|K$.

Exercise 3. Let $d : G \to \hat{\mathbb{Z}}$ be a surjective homomorphism, A a G-module which satisfies axiom (5.1), and let $v : A_k \to \hat{\mathbb{Z}}$ be a henselian valuation with respect to d.

Let $K|k$ be a finite extension and let spec(K) be the set of **microprimes** of K (see §4, exercise 1-5). Define a canonical mapping

$$r_K : \mathrm{spec}(K) \to A_K/N_{\tilde K|K}A_{\tilde K},$$

and show that, for a finite extension, the diagram

$$\begin{array}{ccc} \mathrm{spec}(L) & \xrightarrow{r_L} & A_L/N_{\tilde L|L}A_{\tilde L} \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle N_{L|K}} \\ \mathrm{spec}(K) & \xrightarrow{r_K} & A_K/N_{\tilde K|K}A_{\tilde K} \end{array}$$

commutes. Show furthermore that, for every finite Galois extension $L|K$, r_K induces the reciprocity isomorphism

$$r_{L|K} : G(L|K) \to A_K/N_{L|K}A_L.$$

Hint: Let $\varphi \in G_K$ be an element such that $d_K(\varphi) \in \mathbb{N}$. Let Σ be the fixed field of φ and

$$\hat A_\Sigma = \varprojlim_\alpha A_{K_\alpha},$$

where K_α varies over the finite subextensions of $\Sigma|K$ and where the projective limit is taken with respect to the norm maps $N_{K_\beta|K_\alpha} : A_{K_\beta} \to A_{K_\alpha}$. Then there is a surjective homomorphism $v_\Sigma : \hat A_\Sigma \to \hat{\mathbb{Z}}$ and a homomorphism $N_{\Sigma|K} : \hat A_\Sigma \to A_K$.

§ 6. The General Reciprocity Law

We now impose on the continuous G-module A the following condition.

(6.1) Class Field Axiom. *For every cyclic extension $L|K$ one has*

$$\#H^i(G(L|K), A_L) = \begin{cases} [L:K] & \text{for } i = 0, \\ 1 & \text{for } i = -1. \end{cases}$$

Among the cyclic extensions, there are in particular the unramified ones. For them the above condition amounts precisely to requiring axiom (5.1), so that one has

(6.2) Proposition. *For a finite unramified extension $L|K$, one has*

$$H^i\big(G(L|K), U_L\big) = 1 \quad \text{for} \quad i = 0, -1.$$

Proof: Since $L|K$ is unramified, a prime element π_K of A_K is also a prime element of A_L. As $H^{-1}(G(L|K), A_L) = 1$, every element $u \in U_L$ such that $N_{L|K}(u) = 1$ is of the form $u = a^{\sigma-1}$ with $a \in A_L$, $\sigma = \varphi_{L|K}$. So writing $a = \varepsilon\pi_K^m$, $\varepsilon \in U_L$, we obtain $u = \varepsilon^{\sigma-1}$. This shows that $H^{-1}(G(L|K), U_L) = 1$.

On the other hand, the homomorphism $v_K : A_K \to \mathbb{Z}$ gives rise to a homomorphism

$$v_K : A_K/N_{L|K}A_L \longrightarrow \mathbb{Z}/n\mathbb{Z},$$

where $n = [L : K] = f_{L|K}$, because $v_K(N_{L|K}A_L) = f_{L|K}\mathbb{Z} = n\mathbb{Z}$. This homomorphism is surjective as $v_K(\pi_K \bmod N_{L|K}A_L) = 1 \bmod n\mathbb{Z}$, and it is bijective as $\#A_K/N_{L|K}A_L = n$. If now $u \in U_K$, then we have $u = N_{L|K}(a)$, with $a \in A_L$, since $v_K(u) = 0$. But $0 = v_K(u) = v_K(N_{L|K}(a)) = n v_L(a)$, so we get in fact $a \in U_L$. This proves that $H^0(G(L|K), U_L) = 1$. □

By definition, a class field theory is a pair of homomorphisms

$$(d : G \to \hat{\mathbb{Z}},\ v : A \to \hat{\mathbb{Z}}),$$

where A is a G-module which satisfies axiom (6.1), d is a surjective continuous homomorphism, and v is a henselian valuation. From proposition (6.2) and §5, we obtain for every finite Galois extension $L|K$, the reciprocity homomorphism

$$r_{L|K} : G(L|K)^{ab} \longrightarrow A_K/N_{L|K}A_L.$$

But the class field axiom yields moreover the following theorem, which represents the main theorem of class field theory, and which we will call the general reciprocity law.

(6.3) Theorem. *For every finite Galois extension $L|K$, the homomorphism*

$$r_{L|K} : G(L|K)^{ab} \longrightarrow A_K/N_{L|K}A_L$$

is an isomorphism.

Proof: If $M|K$ is a Galois subextension of $L|K$, we get from (5.8) the commutative exact diagram

$$\begin{array}{ccccccc}
G(L|M)^{ab} & \longrightarrow & G(L|K)^{ab} & \longrightarrow & G(M|K)^{ab} & \longrightarrow & 1 \\
\downarrow{\scriptstyle r_{L|M}} & & \downarrow{\scriptstyle r_{L|K}} & & \downarrow{\scriptstyle r_{M|K}} & & \\
A_M/N_{L|M}A_L & \xrightarrow{N_{M|K}} & A_K/N_{L|K}A_L & \longrightarrow & A_K/N_{M|K}A_M & \longrightarrow & 1.
\end{array}$$

We use this diagram to make three reductions.

First reduction. We may assume that $G(L|K)$ is abelian. For if the theorem is proved in this case, then, putting $M = L^{ab}$ the maximal abelian subextension of $L|K$, we find $G(L|K)^{ab} = G(M|K)$, and the commutator subgroup $G(L|M)$ of $G(L|K)$ is precisely the kernel of $r_{L|K}$, i.e., $G(L|K)^{ab} \to A_K/N_{L|K}A_L$ is injective. The surjectivity follows by induction on the degree. Indeed, in the case where $G(L|K)$ is solvable, one has either $M = L$ or $[L : M] < [L : K]$, and if $r_{L|M}$ and $r_{M|K}$ are surjective, then so is $r_{L|K}$. In the general case, let M be the fixed field of a p-Sylow subgroup. $M|K$ need not be Galois, but we may use the left part of the diagram, where $r_{L|M}$ is surjective. It then suffices to show that the image of $N_{M|K}$ is the p-Sylow subgroup S_p of $A_K/N_{L|K}A_L$. That this holds true for all p amounts to saying that $r_{L|K}$ is surjective. Now the inclusion $A_K \subseteq A_M$ induces a homomorphism

$$i : A_K/N_{L|K}A_L \longrightarrow A_M/N_{L|M}A_L$$

such that $N_{M|K} \circ i = [M : K]$. As $([M : K], p) = 1$, $S_p \xrightarrow{[M:K]} S_p$ is surjective, so S_p lies in the image of $N_{M|K}$, and therefore of $r_{L|K}$.

Second reduction. We may assume that $L|K$ is cyclic. For if $M|K$ varies over all cyclic subextensions of $L|K$, then the diagram shows that the kernel of $r_{L|K}$ lies in the kernel of the map $G(L|K) \to \prod_M G(M|K)$. Since $G(L|K)$ is abelian, this map is injective and hence the same is true of $r_{L|K}$. Choosing a proper cyclic subextension $M|K$ of $L|K$, surjectivity follows by induction on the degree as in the first reduction for solvable extensions.

Third reduction. Let $L|K$ be cyclic. We may assume that $f_{L|K} = 1$. To see this, let $M = L \cap \tilde{K}$ be the maximal unramified subextension of $L|K$. Then $f_{L|M} = 1$ and $r_{M|K}$ is an isomorphism by (5.7). In the bottom sequence of our diagram, the map $N_{M|K}$ is injective because the groups in this sequence have the respective orders $[L : M]$, $[L : K]$, $[M : K]$ by axiom (6.1). Therefore $r_{L|K}$ is an isomorphism if $r_{L|M}$ is.

Now let $L|K$ be cyclic and totally ramified, i.e., $f_{L|K} = 1$. Let σ be a generator of $G(L|K)$. We view σ via the isomorphism $G(L|K) \cong G(\tilde{L}|\tilde{K})$ as an element of $G(\tilde{L}|K)$, and obtain the element $\tilde{\sigma} = \sigma\varphi_L \in \mathrm{Frob}(\tilde{L}|K)$, which is a preimage of $\sigma \in G(L|K)$ with $d_K(\tilde{\sigma}) = d_K(\varphi_L) = f_{L|K} = 1$. We thus find for the fixed field $\Sigma|K$ of $\tilde{\sigma}$ that $f_{\Sigma|K} = 1$, and so $\Sigma \cap \tilde{K} = K$. Let $M|K$ be a finite Galois subextension of $\tilde{L}|K$ containing Σ and L, let $M^0 = M \cap \tilde{K}$ be the maximal unramified subextension of $M|K$, and put $N = N_{M^0|K}$. As $f_{L|K} = 1 = f_{\Sigma|K}$, one finds $N|_{A_L} = N_{L|K}$, $N|_{A_\Sigma} = N_{\Sigma|K}$ (see the proof of (5.3)).

For the injectivity of $r_{L|K}$, we have to prove this: if $r_{L|K}(\sigma^k) = 1$, where $0 \le k < n = [L:K]$, then $k = 0$.

In order to do this, let $\pi_M \in A_M$, $\pi_L \in A_L$ be prime elements. Since $\tilde{L} \subseteq \tilde{M}$, π_M and π_L are both prime elements of $\tilde{M}$. Putting $\pi_M = u\pi_L$, $u \in U_{\tilde{M}}$, we obtain

$$r_{L|K}(\sigma^k) \equiv N(\pi_M) \equiv N(u)\, N(\pi_L) \equiv N(u) \bmod N_{L|K}A_L.$$

From $r_{L|K}(\sigma^k) = 1$, it thus follows that $N(u) = N(\varepsilon)$ for some $\varepsilon \in U_{\tilde{L}}$, so that $N(u^{-1}\varepsilon) = 1$. From axiom (6.1), we may write $u^{-1}\varepsilon = a^{\varphi-1}$ for some $a \in A_{\tilde{M}}$, and find in $A_{\tilde{M}}$ the equation

$$(\pi_L^{\tau})^{\varphi-1} = (\pi_L\varepsilon)^{\varphi-1} = (\pi_M u^{-1}\varepsilon)^{\varphi-1} = (a^{\varphi-1})^{\varphi-1} = (a^{\varphi-1})^{\tau-1},$$

and so $x = \pi_L\varepsilon \cdot a^{1-\varphi} \in A_{\tilde{M}}$. Now $v_M(x) \in \mathbb{Z}$ and $n \cdot v_M(x) = v_M(x) = k$ imply that one has $k = 0$ and so $r_{L|K}$ is injective. The surjectivity then follows from (6.1). $\square$

The inverse of the mapping $r_{L|K} : G(L|K)^{ab} \to A_K/N_{L|K}A_L$ gives, for every finite Galois extension $L|K$, a surjective homomorphism

$$(\ ,L|K) : A_K \longrightarrow G(L|K)^{ab}$$

with kernel $N_{L|K}A_L$. This map is called the **norm residue symbol** of $L|K$. From (5.8) and (5.9) we have the

(6.4) Proposition. *Let $L|K$ and $L'|K'$ be finite Galois extensions such that $K \subseteq K'$ and $L \subseteq L'$, and let $\sigma \in G$. Then we have the commutative diagrams*

$$\begin{array}{ccc} A_{K'} & \xrightarrow{(\ ,L'|K')} & G(L'|K')^{ab} \\ \downarrow & & \downarrow \\ A_K & \xrightarrow{(\ ,L|K)} & G(L|K)^{ab} \end{array} \qquad \begin{array}{ccc} A_K & \xrightarrow{(\ ,L|K)} & G(L|K)^{ab} \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\sigma^*} \\ A_{K^\sigma} & \xrightarrow{} & G(L^\sigma|K^\sigma)^{ab}. \end{array}$$

and if $K' \subseteq L$, we have the commutative diagram

AK' �   G(LIKf"

r   Iv«

AK �   G(l.lK)"".

The definition of the nonn residue symbol automatically extends to infinite Galois extensions LI *K.* For if *L;* I *K* varies over the finite Galois subextensions, then

$$G(L|K)^{ab} = \varprojlim G(L_i|K)^{ab}$$

(see §2, exercise 6). Af, *(a,L₁,1K)l1,il! = (a,L₁lK)* for *L₁,* 2 *L,,* the individual norm residue symbols *(a.* L₁IK), *a* E *AK,* determine an element

$$(a,LIK) \in G(LIKJ'''',$$

In the special case of the extem,ion KI *K,* we find the following intimate connection between the maps *dK, VK,* and (, *i<IK).*

(6.5) Proposition. *One has*

$$(a,KIK)=<p/(a), \quad andthus \quad dKo(,KIK)=VK.$$

Proof: Let *LIK* be the subextension of *RIK* of degree *f.* As *Z/f"Z* = *Z/fZ,* we have 1JK(a) = *n* + with *n* E Z, *z* E Z; that is, *a= un;ht,* with *u* E *UK, h* E *AK.* From we obtain

$$(a, RIK)IL = (a,LIK) = (nK, LIK)n(h, LIK)^1 = <f!2iK = \text{'P?(a)} IL.$$

Thmwe must have *(a, i<IK)* = 'P?fol_ □

The main goal of field theory is to classify all algebraic extensions of a given field *K.* The law governing the constitution of extension& of *K* is hidden in the inner �tructure of the base field *K* itself, and should therefore be expres5cd in terms of entitief, directly associated with it. Class field theory wives this problem as far as the abelian exten&ions of *K* arc concerned. It establishes a I - I-correspondence between these extensions and certain subgroups of *AK.* More precisely, this b done as follows.

For every field *K,* we equip the group *AK* with a topology by declaring the co&etf, *aNL:K AL* to be a basis of neighbourhoods of *a* E *AK* , where *L* I*K* varie<, over all finite Galois extensions of *K.* We call this topology the **norm topology** of *AK.*

(6.6) **Proposition.** (i) *The open* subgroups of *AK* are *precisely /he clo8ed rnhgroups* of *finite index.*

(ii) The *valuation VK* : *AK* ---+ Z is *continuous.*

(iii) *If $L|K$ is a finite extension, then $N_{L|K}: A_L \to A_K$ is continuous.*

(iv) *A_K is Hausdorff if and only if the group*

$$A_K^0 = \bigcap_L N_{L|K} A_L$$

of universal norms is trivial.

Proof: (i) If $\mathcal{N}$ is a subgroup of A_K, then

$$\mathcal{N} = A_K \setminus \bigcup_{a \notin \mathcal{N}} a\mathcal{N}.$$

Now, if $\mathcal{N}$ is open, so are all cosets $a\mathcal{N}$, so that $\mathcal{N}$ is closed, and since $\mathcal{N}$ has to contain one of the neighbourhoods $N_{L|K}A_L$ of the basis of neighbourhoods of 1, $\mathcal{N}$ is also of finite index. If, conversely, $\mathcal{N}$ is closed and of finite index, then the union of the finitely many cosets $a\mathcal{N} \neq \mathcal{N}$ is closed, and so $\mathcal{N}$ is open.

(ii) The groups $f\hat{\mathbb{Z}}$, $f \in \mathbb{N}$, form a basis of neighbourhoods of $0 \in \hat{\mathbb{Z}}$ (see § 2), and if $L|K$ is the unramified extension of degree f, then it follows from (4.7) that

$$v_K(N_{L|K}A_L) = f\, v_L(A_L) \subseteq f\hat{\mathbb{Z}},$$

which shows the continuity of v_K.

(iii) Let $N_{M|K}A_M$ be an open neighbourhood of $1 \in A_K$. Then

$$N_{L|K}(N_{ML|L}A_{ML}) = N_{ML|K}A_{ML} \subseteq N_{M|K}A_M,$$

which shows the continuity of $N_{L|K}$.

(iv) is self-evident. □

The finite abelian extensions $L|K$ are now classified as follows.

(6.7) **Theorem.** *Associating*

$$L \longmapsto \mathcal{N}_L = N_{L|K}A_L$$

sets up a 1-1-correspondence between the finite abelian extensions $L|K$ and the open subgroups $\mathcal{N}$ of A_K. Furthermore, one has

$$L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}.$$

The field L corresponding to the subgroup $\mathcal{N}$ of A_K is called the **class field** associated with $\mathcal{N}$. By (6.3), it satisfies

$$G(L|K) \cong A_K/\mathcal{N}.$$

Proof of (6.7): If L$_I$ and *L2* are ahelian extensions of *K.* then the transitivity of the norm implies}\V,.$_1$L$_2$ <;;;; *.NL$_1$ n}/L-::.·* If, conversely, *a* ∈ N,.$_1$ n/VL$_2$, then the element *(a, L$_1$L2IK)* ∈ G(L$_1$*L2IK)* projects trivially onto *G(L, IK).* that is,(a,L$_1$IK) = I fori = 1.2. *Thus(a,L1L2IK)* = l.i.e.,a E./\·L$_{11.,.}$ We therefore have /1.lt,$_{1\,2}^{\ 1}$ = *NL*$_{\mathrm{I}}$ n ./'ir,$_2$ and so -

NL$_1$ 2N,," {=::}/,f"J.$_1$ *nJVL$_2$ =JV1.$_1$$_{L_2}$ =NL$_2$* {=::} *lL1L2: KJ*

= [L2: Kl{=::} L1 £ *L2.*

Thi" shows the injectivity of the correspondence *L* i---+ /'v*L.*

If *JV* is any open ?ubgroup, then it contains the norm groupJVL = *NLIK AL* of some Galois extension *LIK.* (6.3) implies that *NL = .,Vf',h,* so we may a%ume LI *K* to be abelian. But (.,V. LI K) = G(LIL') for some intermediate field *L'* of LI*K.* Since *J\./* 2 *J,/L.* the group *JV* is the full preimage of G(LIL') under the map (*.LIK): AK---+* G(LIK), and thus it is the full kernel of (*. L'jK)* : *AK ---+ G(L'IK).* Thus *Ar= JVt ,*. This shows that the correspondence *L* i---+ *NL* is wrjective.

Finally, the equality *Ni.* $_{r_1 jL;,\_}$ = .V, is obtained as follows. LI *n L2* £ *L,* implies that *,',./L$_1$··t.$_2$* 2 *)\·L,.* and thus

/'vl.1riL-:. "2.JVt.1ArL$_2$.

As;\h/'r..t.$_2$ is open, we have just shown *thatf,/L$_1$Ar1.$_2$=}../L* for some finite ahelian extension LI *K.* Bu,t*VL$_1$ £.ML* implies *L £* L$_I$ *n L2,* ?o that

$$\mathcal{N}_{L_1}\mathcal{N}_{L_2} = \mathcal{N}_L \supseteq \mathcal{N}_{L_1\cap L_2}\,. \qquad \square$$

Exercise **l.** Let *n* be number, an<l a??ume = ll; E *A* I *l;"* = 1) of order 11. *A? A".* Let *K* be a field μ_{11} C; and !et the maximal abelian excen?ion ot exponent *n.* If *l.IK* 1? linite, one ha? = *Al--*

Exercise 2. Under the hypothe\e\ of exercise I, Kummer theory and cla?? field theory via Poniryagin duality *G(LIK)* x Hom(G(LIK),/1,,l----,- *p,,,* a nondegcncrate n1apping (the ab?cracl "'Hilhert \ymbol")

(.) : *AK/A;* x *AK/;\;-----+ tt,,.*

Exercise 3. Lei *p* he a prime number and (d: *(;* ----,- '6$_{1,.}$ *v* : *A;* -,- field 1heory in the ?en\c of §5. exerei?c 2. Let *d'* : *G* ----,- 2$_1$, be homo111orph1?m, and **f'IK** Che 2$_1$,-exten?ion defined by *d'.* Let ii': *A,---;.* Z" he Che composite ot

*A,_(*____? C(R'IK)? 'E,,.

Then *(d'.v')* i¾ abo a p-cla.\? field theory. The norm re?idue ?ymbol, (d. *v)* and *(d'.v')* (No ?1a!cmcnt hold, in lhc case or field !hcone, *(d G* ----,- *v* ; *A$_1$* ---;.

Exercise 4. (Generalization to infinite extensions.) Let $(d : G \to$ V: A,→ Zi be a class field theory. We assume that the kernel U_k of $v_k : A, \to$ compm:t for every finite extension $K|k$. For an infinite extension $K|k$, psi

AK=)jQt AK,,,

where varies over the finite suhextension� of K lk and the projective limit i� taken respect to the norm map� NKolK": AK�→ AKd· Show:

I) For every (finite or infinite) extcn�1on LIK. one ha� a norm map

N1.11< A1. → A...-.

and 1f LIK i� finite, there is an injection $i_{L|K}$: AK → A_1· If furthemmre LIK i� Gal01�, then one ha� AK � $\widehat{A}_{I.}^{G(L \cdot K)}$.

2) For every extension Klk with finite inertia degree fK = [K nl: .l..], (d, v) induces a cla�� field theory (d...- : GK → $\widehat{\mathbb{Z}}$, $v_K : \widehat{A}_K \to \widehat{\mathbb{Z}}$).

3) If $K \subseteq K'$ are extensions of k with f_K, $f_{K'} < \infty$, and $L|K$ and $L'|K'$ are (finite or infinite) Galois extensions with $L \subseteq L'$, then one has a commutative diagram

$$\widehat{A}_{K'} \xrightarrow{(\ ,L'|K')} G(L'|K')^{ab}$$

1

-' ·-"-"- G(LIK)"n_

Exercise 5, If LIK 1� a finite Galm� extension, then Gt 1s a G(LIK)-module ma canomcal way, and the tran�fer from G...- to G_1 is a homomorphism

Ver: G�I• → (G1"/'1111<J.

Exercise 6. (Tautological class field theory.) Assume that 1he profinitc group G �ali�lie� the condition: for every finite Galoi� cxtemion,

Ver: Gl'.' → (G't'f11IK1

is an isomorphism. (These are the groups cohomological dimen- ,ion 2"' (see 11451, chap. 111, th. Put All = and form the direct limit A= !!.!!] Ax via the transfer. A,, 1s identified A(;,_

Show that for every cyclic extension LI K one hd�

#H'(G(LIK).Ai.)=111L:KI r��;:�·1.

and that for every �UTJective homomorphism d : G → Z, the induced map = G"" → Z is a hen�elian valuation with respect to d. The corre�ponding rec1-map r1 IK: G(LIK) → A...-/NL1...-A1 i� e�sentially the identity.

Abstract cla�s field theory act.Juire, d much broader range of applir.:at1on� if 11 i, gcneraliLed a, follows.

Exercise 7, Let (; be a prolinite group and R(G) the category of finite G-,eh. i.e., of finite �et� X with a continuous Ci-operation. Show that the tran�1tivc G-,els in $B(G)$ are, up to i�omorphi�m. the �ets -...here GA open �ubgroup of G, and G operate, via multipl1cat1on on

If X i� a finite G-set and x E X, then

$$n1(X,x) = G, = \{rr\ EGlax = x)$$

is called the fundamental group of X with ba�e point x. For a map / : X ---J- Y m B(G), we put

$$G(XIY) = Autr(X).$$

f is called if X and Y arc connected and G(XIY) operates tran�itively on the fibres

Exercise 8. Lct $f : X$ ---J- Y be a map of conneucd finite G-�els, and let x E X, E Y. Show that f i� Galoi.� if and only if 1r1 $(X. ,1,)$ i� a nonnal subgroup In this case, one has a canonical i�omorphism

$$G(X|Y) \cong \pi_1(Y,y)/\pi_1(X,x).$$

A palf of functor�

$$A = (A..,A.): B(G)---J- (ah),$$

con�1s1ing of a contravariant functor A� and a covariant functor A, from $B((;J$ to the category *(ah)* of ahelian groups is called a double functor if

$$A�(Xl = A,(X) =: A(X)$$

for all X E B(G). We define

$$AK = A(G/GI().$$

If/ ; X ---J- Y 1s a morphism in $B(G)$, then we put

$$A^*(f) = f^* \quad \text{and} \quad A,(f) = f\bullet.$$

A homomorphi�m h A ---J- B of double functors 1� a of homomorphisms $h(X) : A(X)$ ---J- $B(X)$ representing natural tran.5formations ---J- B^* and $A.$ ---J- $B\bullet$.

A G-modulation 1� defined to be a double functor A �uch that

(i) $A(X$ tJ $Y) = A(X)$ x $A(Y)$.

(ii) It among the two diagram�

$$\begin{tikzcd} X & X' \arrow[l, "g'"'] \arrow[d, "f'"] \\ Y \arrow[u, leftarrow, "f"] & Y' \arrow[l, "g"] \end{tikzcd} \quad \text{and} \quad \begin{array}{cc} A(X) � & A(X') \\ /,1 & 1'' \\ A(Y) � & A(Y') \end{array}$$

m B(G), re�p. *(ah)*, the one on the left 1� carte�ian, then the one on the right i� commutative.

Remark: G-modulat1on� were introduced in a general context by A DRt ..11 under the name of Mackey functors (sec 132])

Exerci�c 9, G-modulat1on� form an abelian c,ltegory.

Exercise 10. If A is a G-module, then the function $A(G/G_K) = A^{G_K}$ extends to a G-modulation A in such a way that, for an extension $L|K$, the map $f^* : A_K \to A_L$, resp. $f_* : A_L \to A_K$, induced by $f : G/G_L \to G/G_K$, is the inclusion, resp. the norm $N_{L|K}$.

The rule *AM A* is an c4mvalence between the category of G-modules and the category of G-modulation5 with '·Gai01� descent'·, 1.c.. of those CJ-modulations; *A* such that

r: *A(Y)* _.. *A(xt1x1y1,*

forevery Galois; mapping $f : X$ --+ *Y,* is an i5omorphi�rn.

Exercise **11.** G-modulations are explicitly given by the following data. I.et $B_0(G)$ be the whose object� are the G-�ets *G/U.* where *U* varic� over the open subgroups ·of G, and who�e morphi�m� are the $\tau : G/U \to G/V$ for $U \subseteq V$, a<; well as the map<; *c(a)* : $\tau U \mapsto \tau U\sigma^{-1} = \tau\sigma^{-1}(\sigma U\sigma^{-1})$, fora E G.

Let $A = (A^*, A_*) : B_0(G) \to (ab)$ be a double functor and for π : *G/U--+ G/V* $(U \subseteq V)$, resp. $c(\sigma) : G/U \to G/\sigma U\sigma^{-1}$ $(\sigma \in G)$, define

Ind(' = A,(n): *A{G/U)--+* A(G/V),

Resj_1 = A*(n): A(G/V)--+ *A(G/U).*

*c(o)** = A,(da)): A(G/U)--+ *A(G/rrUa-1).*

If for any three open suhgroup� *U.* V � *W* of G, one has the *mdm tion formula*

Resf o Ind� = lnd!',r·,,,-i,, '�c(a), o Re<,-,,,

1hen *A* extends uni4uely to a G-modulation *A:* R(G) -→ *(ah).*

Hint: If Xi� an arbitrary finite G-set, then the di5Jomt union

Ax= *x*� A(G/G,)

i� again a G-sct, became c(o),A(G/G,) = A(G/G,,,). Define A(X) 10 be the group

A(X) = Homx(X.Ax)

of all G-e4mvariant �ections *X*--,. *Ax* of the projcc:tion A.1 --+ *X.*

Exercise **12.** The function *n''1'(GfGK) =* G';/' extends to a G-modulation

rr''1·: B(GJ--+ *(pro-ah)*

into the of pro-ahelian Thus, for an extension LI *K.* the map� /*: G'j'--+ rer.p. f.: *Gt--+* induced by f: G/G,--+ G/G;.. are given by the transfer. re�p. the inclur.ion G_1 --+ *(;K·*

Exercise **13.** Let *A* be a G-modulation. For every connected finite G-\et *X,* let

N A(X) = ∩ *l*,A(Y).

where the inter\ection is taken over all Galoi� map<; *f* : *Y* _,. *X.* Show that the function *N A(X)* define� a G-<;ubmodulation *NA* of *A,* the **modulation of unh•err.al**

Exerci<,e **14.** If *A* ir. a G-modulatJon, then the **completion** Ai" again a G-modulation which, for connected *X,* i� given by

A(X) = � *A(X)/f�A(Y).*

where the projective limit ir. taken over all Gal01� maps f : *Y* _,. *X.*

For the following, let $d : G$ ----,. $\mathbb{Z}$ he a fixed surJective homomorphism. Let f: X----,. Y be a map of connected finite G-;,cts and x EX, $y = /\{x)$ E Y. The **inertia** degree, resp. the **ramification index,** of /" i� defined hy

$f''x1r =$ (d((;,): d(G�)), re�p. $ex1) = (!,,: /,).$

where/,, $f_{,}$ 1s the kernel or d: G,, ➔ Z, rc'>p. d: G,----,. Z. j is called **unramificd** $=$ J .

Exercise **IS.** d defines a G-modulat1on Z ;,uch that the maps f^*, corre;,pondrng to a mapping / : X ----,. Y ot connected G-scts, are given by

$$Z(n = Z \qquad Z=Z(X).$$

This give� a homornorphi;,m of G-rnodulatiom

$$d \quad :rr''i,\text{------+} \ Z.$$

Exercise **16.** An unram1ficd map /" : X ----,. Y of connected fimte G-�et, is Galois. and d induces an i,omorph1�m

$$G(XIY) \ � \ Z/fx1yZ.$$

Let *(fix y* E G(XIY) he the element which i.., mapped to I mod $fx_1 yZ$.

Let A be a G-modulation. We define a *he11�d11m 1·af11ation* of A to be a homomorphism

$$v: \ A\text{---},. \ Z$$

�uch the submodulation of Z comes from a subgroup Z <; Z which contains and ;,ati;,fics $Z/nZ =$ for all II E N. Let U denote the kernel of A.

Exercise 17. Compare this delinil1on with the definition (4.6) or a hcnselian valuation ot a G-module A.

Exercise **18.** As;,ume that for every unramified map f : X ----,. Y of connected finite G-;,cts. the �equem:c

$$()\text{----},. \ U(Y) \ .!:\_.. \ U(X)� \qquad U(X) \ \_l.:..c,. \ U(Y) \text{-------},. \ 0$$

s exact, and that $A(Y)^{[X:Y]} \subseteq f_*A(X)$ for every Galois mapping j : X ----,. Y (the atter is a consequence of the condition which will he imposed in exerci..e Then he pair (d, v) gives, for every Cialoi., mapping /" : X ----,. Y, a canonical iomomorphism"

$$\hat{}_{X|Y} : G(X|Y) \to A(Y)/f_*A(X).$$

Exercise **19.** A,.,umc, beyond the condition required rn exercise that for every Gal01., mapping/ X----,. Y with cyclic Galoi\ group G(XIY), one

$$(A(Y): f�A(X)) = [X \ \ Y) \quad \text{and} \quad \ker /. = 1m(a¥ - I).$$

where [X : Y] $=$ # / ^{1}(y). wnh y E Y, and a i� ct generator ot *G(XIY)*. Then i;, an isomorphism for every Galoi\ mapping / : X ----,. Y of prime degree [X :

$$\text{rw:} \quad G(XIY)''1, \_,. \ A(Y)/j�A(X),$$

for every Galm� mapping $f : X$ ➔ Y.

Exercise 20. Under the hypotheses of exerci�e 18 and 19 one obtains a canonical homomorphVim of G-modu!ations

who�e kernel 1s the G-modulation *NJ\.* of universal nonns (�ee exercise 13). It induce� an 1�omorphism

A_::: _, n''''

of the completion *A*of *A* (see exercise 14).

Remark: The theory skct<.:hed above and conlamed in the exercises ha� a very interestmg application to higher dimensional class field theory. In chap. V, (1.3), we will show that, for a Galois cxtcmion LI *K* of local field�. there 1� a reciprocity 1somorphi�m

$$G(L|K)^{ab} \cong K^*/N_{L|K}L^*.$$

The multiplicative group K^* may be interpreted m *K-theury* a� the group $K_1(K)$ of the field *K.* The group $K_2(K)$ i� defined to be the quotient group

K2(K) = *(K* 0 K�)/R,*

where *R* is generated by all element� of the form *x* 0 (1 - .1). Treatmg Galoi� exten�ion� *LIK* of "2-local fields" - these arc di,cretoly valued complete field� with residue cla�� field a local field (e.g., Ql'((..1.)), Fp((x})((y))) - the Japane�e mathematician *K4LI r,i KAJo* (see [!BJ) h1.� e�tahli�hed • c1.nonic1.I i,omorphi1m

G(LIK)''n � K2(K)/N1.1i,:K1(L).

Kato\ proof 1s intricate and needs heavy machinery. It was simplified by the Ru�sian mathematician/. *FViHIKO* (�ce [36], l371, 1381). His proof may be viewed a� a �pecial case of the theory sketched above. The hasic idea i� the following. The corrc�pondence *K* � $K_2(K)$ may he extended to a G-modula110n K_2. It doe� not .,ati.,fy the hypothe-�is of exerci�e 15, �o that one may not apply the ab�tract theory directly to K_2. But *F*,11,vrn consider� on K_2 the finc�t topology for which the canonical map ( ) : *K** x *K*----+* $K_2(K)$ 1s scqucncially continuous. and for which one has *x,. + y.* ----+ 0, *-x₁₁* ----+ 0 whenever.(,, ----+ 0, *y,,* ----+ 0. He puh

K�uμ(K) = *K2(K)/A2(K).*

where $A_2(K)$ i.� the inter�ection of all open neighhourhood.� of 1 in $K_2(K)$, and he show� 1hat

$$K_2^{\mathrm{top}}(K)/N_{L|K}K_2^{\mathrm{top}}(L) \cong K_2(K)/N_{L|K}K_2(L)$$

tor every Galoi� extension *LIK,* and that *Kt'(K)* �atistie� propcrtic� which imply the hypothe�i, of cxerc1�e 18 and 19 when viewing K;op a� a G-modulation. Thi� makes *K,110'�* theorem into a �pecial case of the theory developed above.

§ 7. The Herbrand Quotient

The preceding section concluded abstract class field theory. In order to be able to apply it to the concrete �ituations encountered in number theory, it is all important to verify the *class field axiom* (6.1) in these contexts. An excellent tool for this is the **Herbrand quotient.** It is a group-theoretic formalism, which we develop here for future use.

Let G be a finite cyclic group of order n, let σ be a generator, and A a G-module. As before, we form the two groups

$$H^0(G,A) = A^G/N_G A \quad\text{and}\quad H^{-1}(G,A) = {}_{N_G}A/I_G A,$$

where

$$A^G = \{a \in A \mid a^\sigma = a\}, \qquad N_G A = \{N_G a \mid a \in A\},$$

$${}_{N_G}A = \{a \in A \mid N_G a = 1\}, \qquad I_G A = \{a^{\sigma-1} \mid a \in A\}.$$

(7.1) **Proposition.** *If* $1 \to A \to B \to C \to 1$ *is an exact sequence of G-modules, then we obtain an exact hexagon*

$$\begin{tikzcd}[column sep=small]
& H^0(G,A) \arrow[rr, "f_1"] & & H^0(G,B) \arrow[dr, "f_2"] & \\
H^{-1}(G,C) \arrow[ur, "f_6"] & & & & H^0(G,C) \arrow[dl, "f_3"] \\
& H^{-1}(G,B) \arrow[ul, "f_5"] & & H^{-1}(G,A) \arrow[ll, "f_4"] &
\end{tikzcd}$$

Proof: The homomorphisms f_1, f_4 and f_2, f_5 are induced by $A \xrightarrow{i} B$ and $B \xrightarrow{j} C$. We identify A with its image in B so that i becomes the inclusion. Then f_3 is defined as follows. Let $c \in C^G$ and let $b \in B$ be an element such that $j(b) = c$. Then we have $j(b^{\sigma-1}) = c^{\sigma-1} = 1$ and $N_G(b^{\sigma-1}) = N_G(b^\sigma)/N_G(b) = 1$, so that $b^{\sigma-1} \in {}_{N_G}A$. f_3 is thus defined by $c \bmod N_G C \mapsto b^{\sigma-1} \bmod I_G A$. In order to define f_6 let $c \in {}_{N_G}C$, and let $b \in B$ be an element such that $j(b) = c$. Then $j(N_G b) = N_G c = 1$, so that $N_G b \in A$. The map f_6 is now given by $c \bmod I_G C \mapsto N_G b \bmod N_G A$.

We now prove exactness at the place $H^0(G,A)$. Let $a \in A^G$ such that $f_1(a \bmod N_G A) = 1$; in other words, $a = N_G b$ for some $b \in B$. Writing $c = j(b)$, we find $f_6(c \bmod I_G C) = a \bmod N_G A$. Exactness at $H^{-1}(G,A)$ is deduced as follows: let $a \in {}_{N_G}A$ and $f_4(a \bmod I_G A) = 1$, i.e., $a = b^{\sigma-1}$, with $b \in B$. Writing $c = j(b)$, we find $f_3(c \bmod N_G C) = a \bmod I_G A$. The exactness at all other places is seen even more easily. $\square$

(7.2) **Definition.** *The* **Herbrand quotient** *of the G-module A is defined to be*

$$h(G,A) = \frac{\#H^0(G,A)}{\#H^{-1}(G,A)},$$

provided that both orders are finite.

The salient property of the Herbrand quotient is its *multiplicativity.*

(7.3) **Proposition.** *If $1 \longrightarrow A \to B \to C \longrightarrow 1$ is an exact sequence of G-modules, then one has*

$$h(G,B) = h(G,A)h(G,C)$$

in the sense that, whenever two of these quotients are defined, so is the third and the identity holds.

For a finite G-module A, one has $h(G,A) = 1$.

Proof: We consider the exact hexagon (7.1). Calling n_i the order of the image of f_i, we find

$$\#H^0(G,A)=n_6n_1, \quad \#H^0(G,B)=n_1n_2, \quad \#H^0(G,C)=n_2n_3,$$
$$\#H^{-1}(G,A)=n_3n_4, \quad \#H^{-1}(G,B)=n_4n_5, \quad \#H^{-1}(G,C)=n_5n_6.$$

and thus

$$\#H^0(G,A)\cdot\#H^0(G,C)\cdot\#H^{-1}(G,B) = \#H^0(G,B)\cdot\#H^{-1}(G,A)\cdot\#H^{-1}(G,C).$$

At the same time, we see that if any two of the quotients are well-defined, then so is the third. And from the last equation, we obtain $h(G,B) = h(G,A)h(G,C)$. Finally, if A is a finite G-module, then the exact sequences

$$1 \longrightarrow A^G \longrightarrow A \xrightarrow{I_G} I_GA \longrightarrow 1, \quad 1 \longrightarrow {}_{N_G}A \longrightarrow A \xrightarrow{N_G} N_GA \longrightarrow 1,$$

show that $\#A = \#A^G \cdot \#I_GA = \#_{N_G}A \cdot \#N_GA$, and $h(G,A) = 1$. □

If G is an arbitrary group and g a subgroup, then to any g-module B, we may associate the so-called **induced G-module**

$$A = \mathrm{Ind}_G^g(B).$$

It consists of all functions $f : G \to B$ such that $f(\tau x) = f(x)^\tau$ for all $\tau \in g$. The operation of $\sigma \in G$ is given by

$$f^\sigma(x) = f(\sigma x).$$

If $g = \{1\}$, we write $\mathrm{Ind}_G(B)$ instead of $\mathrm{Ind}_G^g(B)$. We have a canonical g-homomorphism

$$\pi : \mathrm{Ind}_G^g(B) \longrightarrow B, \quad f \longmapsto f(1),$$

which maps the g-submodule

$$B' = \{ f \in \mathrm{Ind}_G^g(B) \mid f(x) = 1 \ \text{for} \ x \notin g \}$$

isomorphically onto B. We identify B' with B. If g is of finite index, we find

$$\mathrm{Ind}_G^g(B) = \prod_{\sigma \in G/g} B'^\sigma,$$

where the notation $\sigma \in G/g$ signifies that σ varies over a system of left coset representatives of G/g.

Indeed, for any $f \in \mathrm{Ind}_G^g(B)$ we have a unique factorization $f = \prod_\sigma f_\sigma^\sigma$, where f_σ denotes the function in B' which is determined by $f_\sigma(1) = f(\sigma^{-1})$.

If conversely A is a G-module with a g-submodule B such that A is the direct product

$$A = \prod_{\sigma \in G/g} B^\sigma,$$

then $A \cong \mathrm{Ind}_G^g(B)$ via $B \cong B'$.

(7.4) Proposition. *Let G be a finite cyclic group, g a subgroup and B a g-module. Then we have canonically*

$$H^i\big(G, \mathrm{Ind}_G^g(B)\big) \cong H^i(g, B) \quad \text{for} \quad i = 0, -1.$$

Proof: Let $A = \mathrm{Ind}_G^g(B)$ and let R be a system of right coset representatives for G/g with $1 \in R$. We consider the g-homomorphisms

$$\pi : A \to B, \quad f \mapsto f(1); \qquad \nu : A \to B, \quad f \mapsto \prod_{\rho \in R} f(\rho).$$

Both admit the g-homomorphism

$$s : B \longrightarrow A, \quad b \longmapsto f_b(\sigma) = \begin{cases} b^\sigma & \text{for } \sigma \in g, \\ 1 & \text{for } \sigma \notin g, \end{cases}$$

as a section, i.e., $\pi \circ s = \nu \circ s = \mathrm{id}$, and we have

$$\circ N_G = N_g \circ \nu,$$

because one finds that. for f E A,

(Ncf)O) � n n JP'(!)� TTTT/(pr) � nm /(p))' �N,(v(f)).
TEI/ ptR T p T p

If f E AG, then $f(a) = f(I)$ for all a E G, and /(I)= f(r) = /(l)r for all r E g. The map Jr therefore induces an isomorphism

1r: AG-------+ B''.

It sends Ne A onto $N''B$, for one has $n(Nc;A) = Ng(vA)$ S; $N''B$ on the one hand, and on the other, $Nx(B) = Ng(vsB) = n(Nc;(sB))$ t;: $n(NcA)$. Therefore H⁰(G. A)= H⁰(f?. B).

As Ng o v = Jr o NG, the g-homomorphism v : A ---+ B induces a g-homomorphism

v: N<,-A-------+ t,1,1B.

It is surjective since v o s = id. We �how that le A is the prcimage of /11 B. le A consists of all elements EA, a E G. for if G = (an) and $a = a()$, then /o -1 = $f^{(1+\sigma_0+\cdots+\sigma_0^{i-1})(\sigma_0-1)} \in I_G A$. In the same one has $l,;B$ = {h-r--i | h E B, $\tau \in g$}. Writing now $\sigma\rho = \rho'\tau_p$, with , ER. Tp E $f?$, we obtain

v(Ja-•)� TT f(op)�n /(p')'•�n hJ'-•E lgB.
pcR f(p) p' f(p') p

On the other hand, for hr-I E $l,;B$, the function r-1, with f = sh, is a prcimage as v(fr-l) = $vs(hy$-1 = br-1. After this it remains to show kcr(v) S; lcA. Let G = (rp), n = (G: g), R = {1,ip, .,l/'.Jn-1 1. Let f ENG A be such that $v(f)$ = TT7''''<: rp' = I. Define the function h EA by h(I) = I, $h(1./') =$ n1�i' $f(ip^1)$. Then $f(ipk) = h(ipk)/h(ipk-1) =$ h(r/---1)1 <P I for 0 < k < n, and f(l)h<P-1-1(1) = nt:;: $f(ipi)$ =I.Hence f = h1_'f-i E lcA. Thus we finally get H 1(G,A) = H-1(g,B). □

Exercise 1. Let f, g be endomorphi�ms of an ahclian group A such that $f \circ g = g \circ f = 0$. Make sense of the following �tatement. The quot1cnl

(ker f: im;;)
qr.�(A) = (kcr::: imf)

i� multiplicative.

Exercise 2. !,et f,g be two commuting endomorph1�m� of an ahelian group A. Shov. that

$$q_{0,gf}(A) = q_{0,g}(A)q_{0,f}(A)$$

provided all quot1cnl� are defined.

Exercise 3, Let G be a cyclic group of prime order p, and let A be a G-module ;,uch that $q_{0,1,}$(A) is detined. Show that

$$h(G, A)P \ ^1 = qn \ _{\mathrm{p}'}(\mathrm{Ac;})\mathrm{I}' / q_{11,,}(\mathrm{A}).$$

Hint: Use the exact ;,cquence

$$0 \text{-----,} \ A(' \text{-----+} \ A \text{�} \quad Aa\text{-}i \text{ -----,} \ 0.$$

Lee $N = \mathrm{I} + er + \ldots + a^{1\cdot -1}$ in the group ring Z[GI. Show that the ring *Z[G]/ZN* is i;,omorphic to Z[(I, for (, a primitive p-th root of unity, and that in this ring one ha�

$$p = (\sigma - 1)^{p-1}\varepsilon,$$

wheres i;, a unit in Z[G]/ZN.

Exercise **4.** Lee LI K he a cyclic exten�ion of prime U;,mg exercise 3, compute the Herbrand quotient of the group ot unib of L, viewed as a G(LIK)-module.

Exercise 5. If G is g a normal wbgroup and A a g-modu!e, then H^1(G, !nd�(A)) �

Chapter V

Local Class Field Theory

§ 1. The Local Reciprocity Law

The abstract class field theory that we have developed in the last chapter is now going to be applied to the case of a *local field*, i.e., to a field which is complete with respect to a discrete valuation, and which has a finite residue class field. By chap. II, (5.2), these are precisely the finite extensions K of the fields $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. We will use the following notation. Let

v_K be the discrete valuation normalized by $v_K(K^*) = \mathbb{Z}$,

$\mathcal{O}_K = \{a \in K \mid v_K(a) \geq 0\}$ the valuation ring,

$\mathfrak{p}_K = \{a \in K \mid v_K(a) > 0\}$ the maximal ideal,

$\kappa = \mathcal{O}_K/\mathfrak{p}_K$ the residue class field,

$U_K = \{a \in K^* \mid v_K(a) = 0\}$ the unit group,

$U_K^{(n)} = 1 + \mathfrak{p}_K^n$, the group of n-th higher units, $n = 1, 2, \dots$,

$q = q_K = \#\kappa$,

$|a|_{\mathfrak{p}} = q^{-v_K(a)}$ the normalized $\mathfrak{p}$-adic absolute value,

μ_n the group of n-th roots of unity, and $\mu_n(K) = \mu_n \cap K^*$.

π_K, or simply π, denotes a prime element of K, i.e., $\mathfrak{p}_K = \pi\mathcal{O}_K$.

In local class field theory, the rôle of the profinite group G of abstract class field theory is taken by the absolute Galois group $G(\bar{k}|k)$ of a fixed local field k, and that of the G-module A by the multiplicative group $\bar{k}^*$ of the separable closure $\bar{k}$ of k. For a finite extension $K|k$ we thus have $A_K = K^*$, and the crucial point is to verify for the multiplicative group of a local field the class field axiom:

(1.1) Theorem. *For a cyclic extension $L|K$ of local fields, one has*

$$\#H^i(G(L|K), L^*) = \begin{cases} [L:K] & \text{for } i = 0, \\ 1 & \text{for } i = -1. \end{cases}$$

Proof: For i = -1 thi:;. is the claim of proposition (3.5) ("Hilbert 90") in chap. IV. So all we have to show is that the Hcrbrand quotient i<; *h(G.L*)* = #H⁰(G.L*) = [L : *KJ,* where we have put G = G(LIK). The exact sequence

$$1 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$$

in which Z has to be viewed as the trivial G-module, yields, by chap. IV, (7.3),

h(G,C) � *h(G,Z)h(G,UL)* �IL, *Klh(G,UL).*

Hence we have to show that *h(G, UL)* = I. For this we choose a nonnal basis *{aa* I *er* E G} of *LIK* (see [93], chap. VIII, § 12, th. 20), *a* E and consider in *t)L* the open (and dosed) *C* -module *M* = *L,ncG* Then the open sets

vn=l+nKM, n=i,2..

form a basis of open neighbourhoods of I in *UL.* Since Mis open, we have *n';j 01.* S; *M* for suitable *N,* and for *n* 2: *N* the *V"* are even subgroups (of finite index) of *UL,* becau:;.e we have

(n;MHn;M) = *n'f,f1M Ms; ni"oL* S; *n}n-N Ms; nKM.*

Hence *vnyn* S; *V11,* and since **l** *-n;μ,* forμ EM. lies in *V".* so does (I - *rrKJL)-1* = I + *rrK(L�1 11'nt* lJ)_ Via the correspondence I +*rrKa* i---+ *a* mod *ITKM,* we obtain G-isomorphisms as in II, (3.10),

V"/V"+¹ ::::::: *M/nKM* = ffi(oK/PK)a" =lndc;(oK/PK).
osG

So by chap.IV. (7.4), we have *H1(G.V11/vn+1* =) I for i = 0. - I and *n* 2: *N.* This in tum implies that *H'(G,* V") = I for *i* = 0. - I and *n* 2: *N.* Indeed, if for instance i = 0 and *a* E *(V")c;,* then *a= (Nch0)a1.* with ho E a1 E (V¹¹+¹**f',** and thus a1 = *(NGh1)a2,* for some h1 E ***V11+1.*** *a2* E etc.; in general,

a,= (Nc;h,)a,+1- *h,* E *vn+i.* a,+I E (V¹¹+¹+l)G

This yields *a* = *Nc;h,* with the convergent product *h* = E *V",* so that *H⁰(G,* V") = I. In the same we have for *a* E such that *Nc;a* = I, that *a= ha-1.* for some *h* E where *a* is a generator of G. Thus *H-1(G, vn)* =I.We now obtain

$$h(G, U_L) = h(G, U_L/V^n)\, h(G, V^n) = 1$$

because *UL/V11* is finite. □

(1.2) Corollary. *If L* IK *is* an *unramificd extemion* of *local fields. then* for i =0, -1,onehas

H'(G(LjK),U1,) � I *and* H'(G(LjK),u)"') � 1 fo, *n* � 1,2,

In particular,

$$N_{L|K} U_L = U_K \quad \text{and} \quad N_{I.|K} U_L^{(n)} = U_K^{(n)}$$

Proof: Let G = G(LIK). We have already seen that *H'(G,Ui,)* = I in chap. IV, (6.2). In order to prove H'(G,utl) =I.we first show that

H;(G,A)* = I and *Hi(G,A)* = I,

for the residue class field A of *L.* It fr, enough to prove this for i = -1, as A is finite, and so h(G,A*) = *h(G,A)* = I. We have *H* [1](G.A*) = I by Hilbert 90 (see chap. IV, (3.5)). Let *f* = [A: K] be the degree of A over the residue class field *K* of *K,* and let *r.p* be the Frobenius automorphism of AIK. Then we have

#NGA=#{ *x* EA / $\overset{/-1}{L}$ .t'P' = $\overset{/-1}{L}$ *x'''* = 0f �*ql* I

and

#(r.p-l)A=qf-1,

since the map A � A has kernel *K,* Therefore H-¹(G,A)= *N(;A/(rp -* !)A �],

Applying now the exact hexagon of chap. IV, (7.1), to the exact sequence of G -modules

1-ul¹J____,..uL---+A*____,..1_

we obtain *H;(G,* u£¹l) = H'(G, *UL)*= I, because *H¹(G,A*)* = I. If *n* is a prime element of *K.* then *n* is abo a prime element of *L,* �o the map *utl---+* A given by I +*an"* r-+ *a* mod *PL* is a C-homomorphi�m. From the exact sequence

1 __,.. uf1+¹i __,.. uf'J---+;,, __,.. 1,

we now deduce by induction just as above, because *H'* (G, A)= 0, that

Hi(G,ut-+l)) = *Hi(c.uj_n))* =I,

since fl'(G.Uj_¹¹) = I. □

We now consider the maximal unramified extension *klk* over the ground field *k*. By chap. II, §9, the residue class field of *k* is the algebraic closure *K* of the residue cla% field *K* of *k*. By chap. **11,** (9.9), we get a canonical isomorphism

G(klk) ""G(,ZIK) '''Z.

It associates to the clement I E Z the Frobenius automorphism *x* 1--+ r'f in G(KIK), and the Frobenius automorphism *<fit...* in *G(klk)* which is given by

a'P' =a'f mod P);, *a* E *or.*

For the absolute Galois group *G* = *G(klk)* we therefore obtain the continuom, and surjective homomorphism

d:G--+2.

Thus the abstract notions of chap. IV, §4, based on this homomorphism, like "unramified", "ramification index", "inenia degree", etc.. do agree, in the case at hand, with the corresponding concrete notions defined in chap. IL

As stated above we choose *A* = *J:** to be our G-module. Hence *AK* = *K*,* for every finite extension KIL The usual normalized exponcnlial valuation *v,(: k** --,,. Z is then henselian with respect to *d,* in the sense of chap. IV. (4.6). For, given any finite extcn�ion *K* lk, *�vK* is the extension of *vf...* to *K�*, and by chap. II, (4.8).

__!_vK(K) = 1 - -vdNK1AK*) = 1 - -. vtJNK1t...K�).*
CK [K: kj CK.!K

i.e., *vdNK1tK*) = .f"KvK(K�) = f"KZ.* The pair of homomorphisms

(d: *G* --,,. .*i,* *VJ* : *J...**--,,. Z)

therefore salisties all the properties of a class field theory, and we obtain the **Local Reciprocity Law:**

(l.3) Theorem. *For every finite Galois exlcmion L* IK of *Joe.ii field.�* we have a *canonical i8omorp/Jism*

$$r_{L|K} : G(L|K)^{ab} \xrightarrow{\sim} K^*/N_{L|K}L^*.$$

The general definition of the reciprocity map in chap. IV. (5.6), wa� actually inspired by the case of local cla,;s field theory. This is why it is especially transparent in this case: let *a* E *G(L* IK), and let *5-* be an extension of *a* to the maximal unramified extension L|*K* of *L* such that *dK (ii)* E N or, in other words, $\tilde\sigma|_{\tilde K} = \varphi^n$ for some $n \in \mathbb{N}$. If Σ is the fixed field of $\tilde\sigma$ and $\pi_\Sigma \in \Sigma$ a prime element, then

$$r_{L|K}(\sigma) = N_{\Sigma|K}(\pi_\Sigma) \bmod N_{L|K}L^*.$$

Inverting $r_{L|K}$ gives us the **local norm residue symbol**

$$(\ ,L|K) : K^* \longrightarrow G(L|K)^{ab}.$$

It is surjective and has kernel $N_{L|K}L^*$.

In global class field theory we will have to take into account the field $\mathbb{R} = \mathbb{Q}_\infty$ along with the p-adic number fields $\mathbb{Q}_p$. It also admits a reciprocity law: for the unique non-trivial Galois extension $\mathbb{C}|\mathbb{R}$ we define the norm residue symbol

$$(\ ,\mathbb{C}|\mathbb{R}) : \mathbb{R}^* \longrightarrow G(\mathbb{C}|\mathbb{R})$$

by

$$(a,\mathbb{C}|\mathbb{R})\sqrt{-1} = \sqrt{-1}^{\,\operatorname{sgn}(a)}.$$

The kernel of $(\ ,\mathbb{C}|\mathbb{R})$ is the group $\mathbb{R}_+^*$ of all positive real numbers, which is again the group of norms $N_{\mathbb{C}|\mathbb{R}}\mathbb{C}^* = \{z\bar z \mid z \in \mathbb{C}^*\}$.

The reciprocity law gives us a very simple classification of the abelian extensions of a local field K. It is formulated in the following

(1.4) Theorem. *The rule*

$$L \longmapsto \mathcal{N}_L = N_{L|K}L^*$$

gives a 1–1-correspondence between the finite abelian extensions $L|K$ and the open subgroups $\mathcal{N}$ of finite index in K^*. Furthermore:

$$L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}, \quad \mathcal{N}_{L_1\cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}.$$

Proof: By chap. IV, (6.7), all we have to show is that the subgroups $\mathcal{N}$ of K^* which are open in the norm topology are precisely the subgroups of finite index which are open in the valuation topology. A subgroup $\mathcal{N}$ which is open in the norm topology contains, by definition a group of norms $N_{L|K}L^*$. By (1.3), this has finite index in K^*. It is also open because it contains the subgroup $N_{L|K}U_L$ which itself is open, for it is closed, being the image of the compact group U_L, and has finite index in U_K. We prove the converse first in

The case char(K) $\nmid n$. Let $\mathcal{N}$ be a subgroup of finite index $n = (K^* : \mathcal{N})$. Then $K^{*n} \subseteq \mathcal{N}$, and it is enough to show that K^{*n} contains a group of norms. For this we use Kummer theory (see chap. IV, §3). We may assume that K contains the group μ_n of n-th roots of unity. For if it does not, we put $K_1 = K(\mu_n)$. If K_1 contains a group of norms $N_{L_1|K_1}L_1^*$, and $L|K$ is a Galois extension containing L_1, then

$$N_{L|K}L^* = N_{K_1|K}(N_{L|K_1}L^*) \subseteq N_{K_1|K}(N_{L_1|K_1}L_1^*) \subseteq N_{K_1|K}(K_1^*) \subseteq \mathcal{N}.$$

So let $\mu_n \subseteq K$, and let $L = K(\sqrt[n]{K^*})$ be the maximal abelian extension of exponent n. Then by chap. IV, §3, we have

$$\operatorname{Hom}(G(L|K),\mu_n) \cong K^*/K^{*n}.$$

By chap. II, (5.8), K^*/K^{*n} is finite, and then so is $G(L|K)$. Since $K^*/N_{L|K}L^*$ is isomorphic to $G(L|K)$ and has exponent n, we have that $K^{*n} \subseteq N_{L|K}L^*$ and (*) yields

$$\#K^*/K^{*n} = \#G(L|K) = \#K^*/N_{L|K}L^*,$$

and therefore $K^{*n} = N_{L|K}L^*$.

The case $\operatorname{char}(K) = p \mid n$. In this case the proof will follow from Lubin-Tate theory which we will develop in §4. But it is also possible to do without this theory, at the expense of *ad hoc* arguments which turn out to be somewhat elaborate. Since the result has no further use in the remainder of this book, we simply refer the reader to the beautiful treatment in [122], chap. XI, §5, and chap. XIV, §6. □

The proof also shows the following

(1.5) Proposition. *If K contains the n-th roots of unity, and if the characteristic of K does not divide n, then the extension $L = K(\sqrt[n]{K^*})|K$ is finite, and one has*

$$N_{L|K}L^* = K^{*n} \quad \text{and} \quad G(L|K) \cong K^*/K^{*n}.$$

Theorem (1.4) is called the **existence theorem**, because its essential statement is that, for every open subgroup $\mathcal{N}$ of finite index in K^*, there exists an abelian extension $L|K$ such that $N_{L|K}L^* = \mathcal{N}$. This is the "class field" of $\mathcal{N}$. (Incidentally, when $\operatorname{char}(K) = 0$, every subgroup of finite index is automatically open - see chap. II, (5.7).) Every open subgroup of K^* contains some higher unit group $U_K^{(n)}$, as these form a basis of neighbourhoods of 1 in K^*. We put $U_K^{(0)} = U_K$ and define:

(1.6) Definition. *Let $L|K$ be a finite abelian extension, and n the smallest number ≥ 0 such that $U_K^{(n)} \subseteq N_{L|K}L^*$. Then the ideal*

$$\mathfrak{f} = \mathfrak{p}^n$$

is called *the* **conductor** of $L|K$.

(1.7) Proposition. *A finite abelian extension $L|K$ is unramified if and only if its conductor is $\mathfrak{f} = 1$.*

Proof: If $L|K$ is unramified, then $U_K = N_{L|K}U_L$ by (1.2), so that $\mathfrak{f} = 1$. If conversely $\mathfrak{f} = 1$, then $U_K \subseteq N_{L|K}U_L$ and $\pi^n \in N_{L|K}L^*$, for $n = (K^* : N_{L|K}L^*)$. If $M|K$ is the unramified extension of degree n, then $N_{M|K}M^* = (\pi^n) \times U_K \subseteq N_{L|K}L^*$, and then $M \supseteq L$, i.e., $L|K$ is unramified. □

Every open subgroup $\mathcal{N}$ of finite index in K^* contains a group of the form $(\pi^f) \times U_K^{(n)}$. This is again open and of finite index. Hence every finite abelian extension $L|K$ is contained in the class field of such a group $(\pi^f) \times U_K^{(n)}$. Therefore the class fields for the groups $(\pi^f) \times U_K^{(n)}$ are particularly important. We will characterize them explicitly in §5, as immediate analogues of the cyclotomic fields over $\mathbb{Q}_p$. In the case of the ground field $K = \mathbb{Q}_p$, the class field of the group $(p) \times U_{\mathbb{Q}_p}^{(n)}$ is precisely the field $\mathbb{Q}_p(\mu_{p^n})$ of p^n-th roots of unity:

(1.8) Proposition. *The group of norms of the extension $\mathbb{Q}_p(\mu_{p^n})|\mathbb{Q}_p$ is the group $(p) \times U_{\mathbb{Q}_p}^{(n)}$.*

Proof: Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\mu_{p^n})$. By chap. II, (7.13), the extension $L|K$ is totally ramified of degree $p^{n-1}(p-1)$, and if ζ is a primitive p^n-th root of unity, then $1-\zeta$ is a prime element of L of norm $N_{L|K}(1-\zeta) = p$. We now consider the exponential map of $\mathbb{Q}_p$. By chap. II, (5.5), it gives an isomorphism

$$\exp : p^\nu \mathbb{Z}_p \longrightarrow U_K^{(\nu)}$$

for $\nu \geq 1$, provided $p \neq 2$, and for $\nu \geq 2$, even if $p = 2$. It transforms the isomorphism $p^\nu \mathbb{Z}_p \to p^{\nu+1}\mathbb{Z}_p$ given by $a \mapsto (p-1)a$ into the isomorphism $U_K^{(\nu)} \to U_K^{(\nu+1)}$ by $x \mapsto x^{p-1}$, so that $(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}$ if $p \neq 2$, and $(U_K^{(2)})^{2^{n-2}} = U_K^{(n)}$ if $p = 2$, $n > 1$

(the case $p = 2$, $n = 1$ is trivial). Consequently, we have $U_K^{(n)} \subseteq N_{L|K}L^*$ if $p \neq 2$. For $p = 2$ we note that

$$U_K^{(2)} = U_K^{(3)} \cup 5U_K^{(3)} = (U_K^{(1)})^2 \cup 5(U_K^{(1)})^2,$$

because a number that is congruent to 1 mod 4 is congruent to 1 or 5 mod 8. Hence

$$U_K^{(n)} = (U_K^{(1)})^{2^{n-1}} \cup 5^{2^{n-2}}(U_K^{(2)})^{2^{n-1}}.$$

It is easy to show that $5^{2^{n-2}} = N_{L|K}(2+i)$, so $U_K^{(n)} \subseteq N_{L|K}L^*$ holds also in case $p = 2$. Since $p = N_{L|K}(1-\zeta)$, we have $(p) \times U_K^{(n)} \subseteq N_{L|K}L^*$, and since both groups have index $p^{n-1}(p-1)$ in K^*, we do find that $N_{L|K}L^* = (p) \times U_K^{(n)}$ as claimed. □

As an immediate consequence of this last proposition, we obtain a local version of the famous theorem of *Kronecker-Weber*, to the effect that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

(1.9) Corollary. *Every finite abelian extension of $L|\mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$, where ζ is a root of unity. In other words:*

The maximal abelian extension $\mathbb{Q}_p^{ab}|\mathbb{Q}_p$ is generated by adjoining all roots of unity.

Proof: For suitable f and n, we have $(p^f) \times U_{\mathbb{Q}_p}^{(n)} \subseteq N_{L|K}L^*$. Therefore L is contained in the class field M of the group

$$(p^f) \times U_{\mathbb{Q}_p}^{(n)} = \big((p^f) \times U_{\mathbb{Q}_p}\big) \cap \big((p) \times$$

By (1.4), M is the composite of the class field for $(p^f) \times U_{\mathbb{Q}_p}$ - this being the unramified extension of degree f - and the class field for $(p) \times$
M is therefore generated by the $(p^f - 1)p^n$-th roots of unity.

From the local Kronecker-Weber theorem, one may readily deduce the global, classical **Theorem of Kronecker-Weber.**

(1.10) Theorem. *Every finite abelian extension $L|\mathbb{Q}$ is contained in a field*

Q(() *generated by a root* of uniry (.

Proof: Let S be the set of all prime numbers p that are ramified in L, and let L_p be the completion of L with respect to some prime lying above p. Then $L_p|\mathbb{Q}_p$ is abelian, and therefore $L_p \subseteq \mathbb{Q}_p(\mu_{n_p})$, for a suitable n_p. Let p^{e_p} be the precise power of p dividing n_p, and let

$$n = \prod_{p \in S} p^{e_p}.$$

We will show that $L \subseteq \mathbb{Q}(\mu_n)$. For this let $M = L(\mu_n)$. Then $M|\mathbb{Q}$ is abelian, and if p is ramified in $M|\mathbb{Q}$, then p must lie in S. If M_p is the completion with respect to a prime of M above p whose restriction to L gives the completion L_p, then

$$M_p = L_p(\mu_n) = \mathbb{Q}_p(\mu_{p^{e_p}n'}) = \mathbb{Q}_p(\mu_{p^{e_p}})\mathbb{Q}_p(\mu_{n'}),$$

with $(n', p) = 1$. $\mathbb{Q}_p(\mu_{n'})|\mathbb{Q}_p$ is the maximal unramified subextension of $\mathbb{Q}_p(\mu_{p^{e_p}n'})|\mathbb{Q}_p$. The inertia group I_p of $M_p|\mathbb{Q}_p$ is therefore isomorphic to the group $G(\mathbb{Q}_p(\mu_{p^{e_p}})|\mathbb{Q}_p)$, and consequently has order $\varphi(p^{e_p})$, where φ is Euler's function. Let I be the subgroup of $G(M|\mathbb{Q})$ generated by all I_p, $p \in S$. The fixed field of I is then unramified, and hence by Minkowski's theorem from chap. III, (2.18), it equals $\mathbb{Q}$, i.e., $I = G(M|\mathbb{Q})$. On the other hand we have

$$\#I \le \prod_{p \in S} \#I_p = \prod_{p \in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}],$$

and therefore $[M : \mathbb{Q}] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$, so that $M = \mathbb{Q}(\mu_n)$. This shows that $L \subseteq \mathbb{Q}(\mu_n)$. □

The following exercises 1-3 presuppose exercises 4-8 of chap. IV, §3.

Exercise 1. For the Galois group $I = G(\bar{K}|\tilde{K})$, one has canonically

$$H^1(I, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \quad \text{and} \quad H^1(I, \mu_n) \cong U_{\tilde{K}}\tilde{K}^{*n}/\tilde{K}^{*n},$$

the latter provided that n is not divisible by the residue characteristic.

Exercise 2. For an arbitrary field K and a G_K-module A, put

$$H^1(K, A) = H^1(G_K, A).$$

If K is a $\mathfrak{p}$-adic number field and n a natural number, then there exists a nondegenerate pairing

$$H^1(K, \mathbb{Z}/n\mathbb{Z}) \times H^1(K, \mu_n) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

of finite groups given by

$$(\chi, a) \mapsto \chi((a, \bar{K}|K)).$$

If n is not divisible by the residue characteristic p, then the orthogonal complement of

$$H^1_{nr}(K, \mathbb{Z}/n\mathbb{Z}) := H^1(G(\tilde{K}|K), \mathbb{Z}/n\mathbb{Z}) \subseteq H^1(K, \mathbb{Z}/n\mathbb{Z})$$

is the group

$$H^1_{nr}(K, \mu_n) := H^1(G(\tilde{K}|K), \mu_n) \subseteq H^1(K, \mu_n)$$

Exercise 3. If LI K is a finite exten�ion of p-adic numher field�, then one has a commutative diagr;im

$$
\begin{array}{ccccc}
//^1(L.Z/nZ) & \times & l/^1(L.\mu,.) & & ZjnZ \\
 & & 1,,' & & \\
H^1(K.Z/nZ) & \times & H^1(K.\mu'') & & Z/nZ.
\end{array}
$$

Exercise 4 (Local Tate Duality). Show that the statement� of cxcrci�c� 2 and 3 generalize to an arbitrary finite GK-module A instead of $Z/n'J'$.., and $A' =$ Hom(A, i<*) in�tcad ofμ''.

Hint: lhe exercises 4-8 of chap. IV, §3.

Exercise 5. Let LI K be the compo�itc of all Zr-extensions of a p-adic numher field K with Galoi� group i�omorphic to Show that the Galoi� group is a free, finitely generated Z_1,-module and it� rank

Hint: Use chap. IL (5.7).

Exercise 6. There i� only one unramitied 2_1,-extem,ion of K. Generate *it* by roob of unity.

Exercise 7. Let p be the re�idue charackri�li<.: of K, ,md let L be the field generated by all rootf,, of ot p-power order. The tixed tield of the tor,ion subgroup of G(LIK) is a It i� called che cydotomic Z,,-extension.

Exercise 8. Let $\widehat{\mathbb{Q}}_p|\mathbb{Q}_p$ be the eyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, let $G(\mathbb{Q}_p|\mathbb{Q}_p) \cong \mathbb{Z}_p$ be a chosen and let J : G:rJ$_{1'}$ → z/! be the homomorphism of the absolute group. Show:

For a �uitable topological generator II of che group of principal unit� of Q\,.

$$\hat{v} : \mathbb{Q}_p^* \to \mathbb{Z}_p \quad \bar{v}(a) = \frac{\log a}{\log u},$$

defines a henf,,clian valuation with to J, m the f,,enf,,e of ab,tract p-claf,,f,, tield theory (see chap. IV, §5, exercise

Exercise 9. Detcnnine all p-class field theories (d: GK→ $Z_{1,}$, �: K^*--+ Zp) over a p-adic number tield K.

Exercif.e IO. Determine all cla,, field theories *(d:* GK→ Z, 11 *Ky*→ Z) over a p-adic number field K.

Exercise 11, The Weil group of a local field K is the preimage W_K of Z under the mapping d_K: GK---+ Z. Show:

The norm re�idue �ymbol (,K"1,IK) of the maximal abclian extension K''^1'IK yields an i�omorph1sm

$$(\ ,K^{ab}|K) : K^* \xrightarrow{\sim} W_K^{ab},$$

which maps the group UK onto the inertia group $I(KunjK)$, and the group of principal units onto the ramification group $R(K^{n}|K)$.

§ 2. The Norm Residue Symbol over *QJP*

If (is a primitive m-th root of unity, with *(m, p)* = I, then Qlp(OIQ,, is unramified, and the norm residue symbol is obviou<;ly given by

$$\big(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p\big)\zeta = \zeta^{p^{v_p(a)}}.$$

But if (is a primitive *p¹¹*-lh root of unity, then we obtain the norm residue symbol for the extem,ion Ql'(()IQI' explicitly in the <;imple form

(a.(!,,(Ol(l1t,), � ,,,-,.

where *a* = and (" ¹ is the power (' with any rational integer *r* = u-¹ mod This result is important, not only in the local situation, but it will play an essential rOle when we develop global class field theory (:,ee chap. VI, S5). Unfortunately, there is no direct algebraic proof of this fact known to date. We have to invoke a transcendental method which makes use of the *completion* R of the maximal unramified extension i of a local lield *K.* We extend the Frobenius <*p* E G('ilK) to f by continuity. First we prove the

(2.1) Lemma. *For* every *c* E *OR,* resp. every *c* E *UR, the equation*

r<P - *x* = *c.* ref,p. *x<f-l* = *c,*

admits a solution in OR, resp. in UR. Ifx<P = *x* for .l E *OR, then x* E *OK.*

Proof: Let *Jr* be a prime element of *K.* Then *n* is also a prime element **off,** and we have the (f-invariant isomorphisms

$$U_{\tilde K}^{(n)}/U_{\tilde K}^{(n+1)} \cong \bar{K}$$

(see chap. II, (3.10)). Let *c EUR* and i" = *c* mod *PK.* Since the residue class field *K* of R is algebraically closed, the equation *X'P* = -�*pi* = *X* • (' *(q* = *(JK)* has a solution *-1-* 0 in *K* = *OR IPR-* i.e.,

c=*xi* ¹a1, X1 E *Uf(,* a1 E

For similar reasons, we find that a₁ = *x,f-¹a?.,* for some *x₂* E and *a?.* E *u}21,* so that *c* = (x1t2)'P ¹a2. Indeed, putting a₁ = I + h₁rr, .\2 = I+)'2Jr, gives *a₁x*�-*<P*= I - *(yf* - *Y2* - hi)rr mod rr². i.e., we have to solve the congruence *yf* - *y₂* - h₁ = 0 mod rr, or equivalently the

equation $Yi - y_2 - h_1 = 0$ in K. This is possible becau�e K is algebraically closed. Continuing in thi� way, we get

$$c = (x_1 x_2 \cdots x_n)^{\varphi - 1} a_n, \quad x_n \in U_{\tilde{K}}^{(n-1)}, \quad a_n \in$$

and passing to tbe limit finally $(" = x^{\varphi - 1}$, where $X =$ n:=I Xn E Uf. The solvability of the equation - $x = r$ follow� analogously, using the isomorphisms P[/Pr1 � K.

Now letx E CJi and $x'^{\circ} = x$. Then, for every n � I, one has

(*) $x=x_{,,}+rr^{11}y_{11}$ withx,,EOKandynEOK.

Indeed, for $n =$ I we have $x = a+$ rrh, with a E $OR\_$, h E $Of($, and $1<P = x$ implies $a'^{\circ}= a$ mod rr. Hence $a=$ -1:1 $+rrc$, with x_1 E OK, c E therefore $x = x_1+rr(h+() = .,_1+rry_1$, y_1 Ent, The equation x implies furthennore that $y,'; = y_{11}$, so that we get a� above with c_{11} E OK, d_{11} E of, and therefore $x = (x_{,,} +$ $+ rr^{11+1}J_{11} =$ $X11+1 + rr^{11+1}Yn+I$, for 5ome $X11+1$ E OK, $Yn+l$ E OR. Now passing to the limit in the equation(*) give� $x = \lim_{11.....,o}$ t,, E OK, bccaw,e K is complete. D

For a power series $F(X1, \ldots, X_{11})$ E odfX1, .. ,X11l], let $F'P$ be the power scric� in oRff $X_1, \ldots, X_{11}$JJwhich arises from F by applying rp to the coefficient� uf F. A **Lubin-Tate** series for a prime element rr of K is by definition a power series $e(X)$ E OK[IXI] with the properties

$$e(X) = rr X \text{ mod deg } 2 \quad \text{and} \quad e(X) = XI/ \text{ mod rr},$$

where $q = l/K$ denotes, as alway�, the number of element<; in the residue class field of K. The totality of all Lubin-Tate series is denoted by S,r. In Err there are in particular the polynomiab

$$e(X) = uXI/ + rr(a_{,1\_1}X'^{1\_1} + \quad +a2X^2) + rr X,$$

where $u.a_1$ E OK and $u =$ I mod rr. The�e are called the **Lubin-Tate polynomials.** The simplest one among them b, the polynomial $X'' + n X$. In the case $K =$ for example, $e(X) = (I+ \quad X)^{1'}$ - I is a Lubin-Tate polynomial for the element p.

(2.2) **Proposition.** *Let* rr *and If* be *prime clement.,* of R, *and* let c(X) E £", *i!(X)* E *Err be Lubin-Tate* series. Let $L(X_1, \ldots, X11) =$ I:=;$^1_{=1} a_1 X_1$ *be* a *linear* form *with coctYicients a,* E *OR* such *that*

$$\pi L(X_1, \ldots, X_n) = \overline{\pi} L^{\varphi}(X_1, \ldots, X_n),$$

Then *there is a uniquely determined* power series $F(X_1,\dots,X_n) \in \mathcal{O}[[X_1,\dots,X_n]]$ *satisfying*

$$F(X_1,\dots,X_n) \equiv L(X_1,\dots,X_n) \bmod \deg 2,$$

$$e\big(F(X_1,\dots,X_n)\big) = F^{\varphi}\big(\bar e(X_1),\dots,\bar e(X_n)\big).$$

If the coefficients of $e, \bar e, L$ *lie in a complete subring* $\mathcal{O}_0$ *of* $\mathcal{O}$ *such that* $\mathcal{O}_0^{\varphi} = \mathcal{O}_0$, *then* F *has coefficients in* $\mathcal{O}_0$ *as well.*

Proof: Let $\mathcal{O}_0$ be a complete subring of $\mathcal{O}$ such that $\mathcal{O}_0^{\varphi} = \mathcal{O}_0$, which contains the coefficients of $e, \bar e, L$. We put $X = (X_1,\dots,X_n)$ and $\bar e(X) = (\bar e(X_1),\dots,\bar e(X_n))$. Let

$$F(X) = \sum_{\nu=1}^{\infty} E_\nu(X) \in \mathcal{O}_0[[X]]$$

be a power series, $E_\nu(X)$ its homogeneous part of degree ν, and let

$$F_r(X) = \sum_{\nu=1}^{r} E_\nu(X).$$

Clearly, $F(X)$ is a solution of the above problem if and only if $F_1(X) = L(X)$ and

(1) $$e(F_r(X)) \equiv F_r^{\varphi}(\bar e(X)) \bmod \deg(r+1)$$

for every $r \geq 1$. We determine the polynomials $E_\nu(X)$ inductively. For $\nu = 1$ we are forced to take $E_1(X) = L(X)$. Condition (1) is then satisfied for $r = 1$ by hypothesis. Assume that the $E_\nu(X)$, for $\nu = 1,\dots,r$, have already been found, and that they are uniquely determined by condition (1). We then put $F_{r+1}(X) = F_r(X) + E_{r+1}(X)$ with a homogeneous polynomial $E_{r+1}(X) \in \mathcal{O}_0[X]$ of degree $r+1$ which has yet to be determined. The congruences

$$e(F_{r+1}(X)) \equiv e(F_r(X)) + \pi E_{r+1}(X) \bmod \deg(r+2),$$

$$F_{r+1}^{\varphi}(\bar e(X)) \equiv F_r^{\varphi}(\bar e(X)) + \pi^{r+1} E_{r+1}^{\varphi}(X) \bmod \deg(r+2)$$

show that $E_{r+1}(X)$ has to satisfy the congruence

(2) $$G_{r+1}(X) + \pi E_{r+1}(X) - \pi^{r+1} E_{r+1}^{\varphi}(X) \equiv 0 \bmod \deg(r+2)$$

with $G_{r+1}(X) = e(F_r(X)) - F_r^{\varphi}(\bar e(X)) \in \mathcal{O}_0[[X]]$. We have $G_{r+1}(X) \equiv 0 \bmod \deg(r+1)$ and

(3) $$G_{r+1}(X) \equiv F_r(X)^q - F_r^{\varphi}(X^q) \equiv 0 \bmod \pi$$

because $e(X) \equiv \bar e(X) \equiv X^q \bmod \pi$ and $a^\varphi \equiv a^q \bmod \pi$ for $a \in \mathcal{O}$. Now let $X^i = X_1^{i_1}\cdots X_n^{i_n}$ be a monomial of degree $r+1$ in $\mathcal{O}[X]$. By (3), the coefficient of X^i in G_{r+1} is of the form $\pi\beta$, with $\beta \in \mathcal{O}$. Let α be the coefficient of the same monomial X^i in E_{r+1}. Then $\bar\pi\alpha - \pi\alpha^\varphi$ is the coefficient of X^i in $\bar\pi E_{r+1} - \pi E^\varphi_{r+1}$. Since $G_{r+1}(X) \equiv 0 \bmod \deg(r+1)$, (2) holds if and only if the coefficient α of X^i in E_{r+1} satisfies the equation

$$-\pi\beta + \pi\alpha - \bar\pi^{r+1}\alpha^\varphi = 0 \tag{4}$$

for every monomial X^i of degree $r+1$. This equation has a unique solution α in $\mathcal{O}_{\tilde K}$, which actually belongs to $\mathcal{O}$. For if we put $\gamma = \pi^{-1}\bar\pi^{r+1}$, we obtain the equation

$$\alpha - \gamma\alpha^\varphi = \beta,$$

which is clearly solved by the series

$$\alpha = \beta + \gamma\beta^\varphi + \gamma^{1+\varphi}\beta^{\varphi^2} + \cdots \in \mathcal{O}$$

(the series converges because $v_{\tilde K}(\gamma) \geq 1$). If α' is another solution, then $\alpha - \alpha' = \gamma(\alpha-\alpha')^\varphi$, hence $v_{\tilde K}(\alpha-\alpha') = v_{\tilde K}(\gamma) + v_{\tilde K}((\alpha-\alpha')^\varphi)$, i.e., $v_{\tilde K}(\alpha-\alpha') = \infty$ because $v_{\tilde K}(\gamma) \geq 1$, and therefore $\alpha = \alpha'$. As a consequence, for every monomial X^i of degree $r+1$, equation (4) has a unique solution α in $\mathcal{O}$, i.e., there exists a unique $E_{r+1}(X) \in \mathcal{O}[X]$ satisfying (2). This finishes the proof. □

(2.3) **Corollary.** *Let π and $\bar\pi$ be prime elements of K, and let $e \in \mathcal{E}_\pi$, $\bar e \in \mathcal{E}_{\bar\pi}$ be Lubin-Tate series with coefficients in $\mathcal{O}_K$. Let $\bar\pi = u\pi$, $u \in U_K$, and $u = \varepsilon^{\varphi-1}$, $\varepsilon \in U_{\tilde K}$. Then there is a uniquely determined power series $\theta(X) \in \mathcal{O}_{\tilde K}[[X]]$ such that $\theta(X) \equiv \varepsilon X \bmod \deg 2$ and*

$$\bar e \circ \theta = \theta^\varphi \circ e.$$

Furthermore, there is a uniquely determined power series $[u](X) \in \mathcal{O}_K[[X]]$ such that $[u](X) \equiv uX \bmod \deg 2$ and

$$e \circ [u] = [u] \circ e.$$

They satisfy

$$\theta^\varphi = \theta \circ [u].$$

Proof: Putting $L(X) = \varepsilon X$, we have $\bar\pi L(X) = \pi L^\varphi(X)$ and the first claim follows immediately from (2.2). In the same way, with the linear form $L(X) = uX$, one obtains the existence and uniqueness of the power series $[u](X) \in \mathcal{O}_K[[X]]$. Finally, defining $\theta_1 = \theta^{\varphi^{-1}} \circ [u]$, we get

$$\bar e \circ \theta_1 = (\bar e \circ \theta)^{\varphi^{-1}} \circ [u] = (\theta^\varphi \circ e)^{\varphi^{-1}} \circ [u] = (\theta^{\varphi^{-1}} \circ [u])^\varphi \circ e = \theta_1^\varphi \circ e,$$

and thus, $\theta_1 = \theta$ because of uniqueness. Hence $\theta^\varphi = \theta \circ [u]$. □

(2.4) **Theorem.** *Let $a = up^{v_p(a)} \in \mathbb{Q}_p^*$ and let ζ be a primitive p^n-th root of unity.* Then one has

$$\big(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p\big)\,\zeta = \zeta^{u^{-1}}.$$

Proof: As $\mathbb{N}$ is dense in $\mathbb{Z}_p$, we may assume that $u \in \mathbb{N}$, $(u, p) = 1$. Let $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\zeta)$, and let $\sigma \in G(L|K)$ be the automorphism defined by

$$\zeta^{\sigma} = \zeta^{u^{-1}}.$$

Since $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ is totally ramified, we have $G(L|K) \cong G(\tilde L|\tilde K)$, and we view σ as an element of $G(\tilde L|K)$. Then $\tilde\sigma = \varphi_{\tilde L|L}\,\sigma \in \mathrm{Frob}(\tilde L|K)$ is an element such that $d_K(\tilde\sigma) = 1$ and $\tilde\sigma|_L = \sigma$. The fixed field Σ of $\tilde\sigma$ is totally ramified because $f_{\Sigma|K} = d_K(\tilde\sigma) = 1$ by chap. IV, (4.5). The proof of the theorem is based on the fact that the field Σ can be explicitly generated by a prime element π_Σ which is given by the power series θ of (2.3).

In order to do this, assume σ and $\varphi = \varphi_{\tilde L|L}$ have been extended continuously to the completion $\hat L$ of $\tilde L$, and consider the two Lubin-Tate polynomials

$$e(X) = upX + X^p \quad \text{and} \quad f(X) = (1+X)^p - 1$$

as well as the polynomial $[u]_f(X) = (1+X)^u - 1$. Then $f([u]_f(X)) = (1+X)^{up} - 1 = [u]_f(f(X))$. By (2.3), there is a power series $\theta(X) \in \mathcal{O}_{\hat L}[[X]]$ such that

$$e \circ \theta = \theta^{\varphi} \circ f \quad \text{and} \quad \theta^{\varphi} = \theta \circ [u]_f.$$

Substituting the prime element $\lambda = \zeta - 1$ of L, we obtain a prime element of Σ by

$$\pi_\Sigma = \theta(\lambda).$$

Indeed, $[u]_f(\lambda^\sigma) = (1+\lambda^\sigma)^u - 1 = (\zeta^{\sigma})^u - 1 = \zeta - 1 = \lambda$, and therefore

$$\pi_\Sigma^{\tilde\sigma} = \theta^{\varphi}(\lambda^{\sigma}) = \theta([u]_f(\lambda^{\sigma})) = \theta(\lambda) = \pi_\Sigma,$$

i.e., $\pi_\Sigma \in \Sigma$. We will show that

$$P(X) = e^{n-1}(X)^{p-1} + up \in \mathbb{Z}_p[X]$$

is the minimal polynomial of π_Σ, where $e^\nu(X)$ is defined by $e^0(X) = X$ and $e^\nu(X) = e(e^{\nu-1}(X))$. $P(X)$ is monic of degree $p^{n-1}(p-1)$ and irreducible by Eisenstein's criterion, as $e(X) \equiv X^p \bmod p$, and so $e^{n-1}(X)^{p-1} \equiv X^{p^{n-1}(p-1)} \bmod p$. Finally, $e^n(X) = e^{n-1}(X)\,(up + e^{n-1}(X)^{p-1}) = e^{n-1}(X)P(X)$, so that

$$P(\pi_\Sigma)\,e^{n-1}(\pi_\Sigma) = e^n(\pi_\Sigma).$$

Since $e^n(\pi_\Sigma) = e^n(\theta(\lambda)) = \theta^{\varphi^n}(f^n(\lambda)) = \theta^{\varphi^n}((1+\lambda)^{p^n} - 1) = 0$, we have $e^n(\pi_\Sigma) = 0$, $e^{n-1}(\pi_\Sigma) \neq 0$, and thus $P(\pi_\Sigma) = 0$.

Observing thal NLid(-1) = (- 1/ *p,d* = IL : *K* J (see chap. II, (7.13)), we obtain

Nx K(ni;) = (-l)J P(0) = (-1)"*pu* = *u* mod *N1.wL**

and therefore *rLIK* (rr) = 11 mod *Nt.lK L **, i.e., *(u,* LI *K)* = (a, LIK) =*a,* required. D

In order to really understand this proof of theorem (2.4), one ha� to read §4. Let us note that one would get a direct, purely algebraic proof, if one could show without using the power series *0* that the splilting field of the polynomial e[11](X) is abelian, and that its elements are all flxcd under *0* = *rrtpL.* This splitting field would then have to be equal to the fieldr and every zero of *P(X)* = *e"(X)/e"* 1(X) would have to be a prime clement *nx* Er �uch that *Nx,K(nr;)* = *u* mod *NL1KL**, in which ca�e *l'LIK (rr)* = *u* mod *NL KL**, and so (11, *L* IK) = *rr.*

Exercise **l.** The p-cla�\ field theory *(d: (;IJ,, --+ Z/!,* v: **Q;,---+** Z) for the unramili.cd z,,-extcnsion of IQ,,, and the p-cla•� field theory (J: *GQ,,* --+ Z1,, D: Q�,---+ Z1,} for the cyclocomic Zp-exten•1on of **Q** , (�cc � 1, e;i;.erci�e 7) yield the same nomi residue ,ymhol (. *LIK).*

Hint: Show that thi��tatemcnt is equivalent to fornmla (2.4): *(u.* Q1,((l lG1i,)(= (" _,

Exercise 2. Let *LIK* be a 1011.lly ramified Gal01s e:w..te�ion, andjet *[* (1-c.p. *Ri* be che completion of the mt1:i:.imal unramitied extensmn *L* (re•p. K) of /. (re•p. *K)* Show that *Nt.1;[•* = *K•,* and that c\ocry *y* E *[*� with Np1;(r) =Ii� ofthe form *y=TT,.:::;'* 1.rr, EG(LIK).

Exercise 3 **(Theorem** of *D""oRK).* Let LI *K* be **a** totally ramified abelian e:i:.temion of p-adie number liekk Let.(EK' and *y* EL• \ueh that *Nr1k(y)* = .1. Let::, E *[•* ,.ind choose *a1* E G(LIK) such that

_vfl l =n<"

Putting rr = **n,** rr,, one ha� (t. LIKJ = rr-1.

Hint: See chap. IV, §5, cxen:1�e 1.

Exerei�e **4.** Deduce from exere1�e� 2 and 3 the formula (u,iQ ,(()IQI')(= (" 1, fur wme p"-th romofunity (.

§ 3. The Hilbert Symbol

Let K be a local field, or $K = \mathbb{R}$, $K = \mathbb{C}$. We assume that K contains the group μ_n of n-th roots of unity, where n is a natural number which is relatively prime to the characteristic of K (i.e., n can be arbitrary if char(K) $= 0$). Over such a field K we then have at our disposal, on the one hand, Kummer theory (see chap. IV, §3), and on the other, class field theory. It is the interplay between both theories which gives rise to the "Hilbert symbol". This is a highly remarkable phenomenon which will lead us to a generalization of the classical reciprocity law of Gauss, to n-th power residues.

Let $L = K(\sqrt[n]{K^*})$ be the maximal abelian extension of exponent n. By (1.5), we then have

$$N_{L|K}L^* = K^{*n},$$

and class field theory gives us the canonical isomorphism

$$G(L|K) \cong K^*/K^{*n}.$$

On the other hand, Kummer theory gives the canonical isomorphism

$$\mathrm{Hom}(G(L|K),\mu_n) \cong K^*/K^{*n}.$$

The bilinear map

$$G(L|K) \times \mathrm{Hom}(G(L|K),\mu_n) \longrightarrow \mu_n, \quad (\sigma,\chi) \longmapsto \chi(\sigma),$$

therefore defines a nondegenerate bilinear pairing

$$\left(\frac{\ ,\ }{\mathfrak p}\right) : K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mu_n$$

(bilinear in the multiplicative sense). This pairing is called the Hilbert symbol. Its relation to the norm residue symbol is described explicitly in the following proposition.

(3.1) Proposition. *For $a,b \in K^*$, the Hilbert symbol $\left(\frac{a,b}{\mathfrak p}\right) \in \mu_n$ is given by*

$$(a, K(\sqrt[n]{b})|K)\sqrt[n]{b} = \left(\frac{a,b}{\mathfrak p}\right)\sqrt[n]{b}.$$

Proof: The image of a under the isomorphism $K^*/K^{*n} \cong G(L|K)$ of class field theory is the norm residue symbol $\sigma_a = (a, L|K)$. The image of b under the isomorphism $K^*/K^{*n} \cong \mathrm{Hom}(G(L|K),\mu_n)$ of Kummer theory is the character $\chi_b: G(L|K) \to \mu_n$ given by $\chi_b(\sigma) = \sigma\sqrt[n]{b}/\sqrt[n]{b}$. By definition of the Hilbert symbol, we have

$$\left(\frac{a,b}{\mathfrak p}\right) = \chi_b(\sigma_a) = \sigma_a\sqrt[n]{b}/\sqrt[n]{b},$$

hence $(a, K(\sqrt[n]{b})|K)\sqrt[n]{b} = (a, L|K)\sqrt[n]{b} = \left(\frac{a,b}{\mathfrak p}\right)\sqrt[n]{b}$. □

The Hilbert 5ymhol hm, the following fundamental properties:

(3.2) **Proposition.**

(i) C'''/) �(¥)("/),

(ii) (" ;h') �(¥)("Ph}

(i) (¥) = 1-¢::=:}aisanormfromtheextensionK(√h)IK,

(iv) (¥)�("fr',

(v) ("·Ip-a)� I and(";")� I,

(vi) If(¥)= I forallh EK*, then a E KM.

Proof: (i) and (ii) arc clear from lhc definition, (iii) follows from (3.1), and (vi) reformulates the nomlegencrateness of the Hilbert symbol.

If h E K^* and x E K �uch that xn - h #- 0, then

$$x'' - h \text{ � } \prod_{1=0}^{a-1} (x - (' f), \qquad fi'' \text{ � } h,$$

for some primitive n -th root of unity (. Let d be the greatest divisor of n such that y'' = h has a solution in K, and let n = dm. Then the extension K (fi)IK is cyclic of degree m. and the conjugates of_\ - (^1fi are the elements x - (J $f3$ such that j == i mod d. We may therefore write

$$-h= \prod_{1=0}^{d-1} NKun1dx-('f3).$$

Hence x^{11} -his anorm from $K(vfi)IK$, i.e..

$$\left(\frac{x^n - b, b}{\mathfrak{p}}\right) = 1$$

Choosing x = I, h = 1 - a, and \- = 0, h = $-a$ then yield (v). (iv) finally follows from

(a/)(\")�(a ;")("/)(h/)t· ;h)

$$= \underline{(a, :ah)(h, :ah) = (ah, :ah) =} 1. \qquad \square$$

In the case $K = \mathbb{R}$ we have $n = 1$ or $n = 2$. For $n = 1$ one finds, of course, $\left(\frac{a,b}{\mathfrak p}\right) = 1$, and for $n = 2$ we have

$$\left(\frac{a,b}{\mathfrak p}\right) = (-1)^{\frac{\operatorname{sgn} a - 1}{2}\cdot\frac{\operatorname{sgn} b - 1}{2}},$$

because $(a, \mathbb{R}(\sqrt{b})|\mathbb{R}) = 1$ for $b > 0$, and $= (-1)^{\frac{\operatorname{sgn} a-1}{2}}$ for $b < 0$. Here the letter $\mathfrak p$ symbolically stands for an infinite place.

Next we determine the Hilbert symbol explicitly in the case where K is a local field $(\neq \mathbb{R}, \mathbb{C})$ whose residue characteristic p does not divide n. We call this the case of the tame Hilbert symbol. Since $\mu_n \subseteq K$ one has $n \mid q-1$ in that case. First we establish the

(3.3) Lemma. *Let $(n, \mathfrak p) = 1$ and $x \in K^*$. The extension $K(\sqrt[n]{x})|K$ is unramified if and only if $x \in U_K K^{*n}$.*

Proof: Let $x = uy^n$ with $u \in U_K$, $y \in K^*$, so that $K(\sqrt[n]{x}) = K(\sqrt[n]{u})$. Let κ' be the splitting field of the polynomial $X^n - u \bmod \mathfrak p$ over the residue class field κ, and let $K'|K$ be the unramified extension with residue class field κ' (see chap. II, §9, p. 173). By Hensel's lemma, $X^n - u$ splits over K' into linear factors, so $K(\sqrt[n]{u}) \subseteq K'$ is unramified. Assume conversely that $L = K(\sqrt[n]{x})$ is unramified over K, and let $x = u\pi^r$, where $u \in U_K$ and π is a prime element of K. Then $v_L(\sqrt[n]{\pi^r}) = \frac{r}{n} v_L(\pi) = \frac{r}{n} \in \mathbb{Z}$, hence $n \mid r$, i.e., $\pi^r \in K^{*n}$, and thus $x \in U_K K^{*n}$. □

Since $U_K = \mu_{q-1} \times U_K^{(1)}$, every unit $u \in U_K$ has a unique decomposition

$$u = \omega(u)\langle u\rangle$$

with $\omega(u) \in \mu_{q-1}$ and $\langle u\rangle \in U_K^{(1)}$, $u \equiv \omega(u) \bmod \mathfrak p$. With this notation we will now prove the

(3.4) Proposition. *If $(n, \mathfrak p) = 1$ and $a, b \in K^*$, then*

$$\left(\frac{a,b}{\mathfrak p}\right) = \omega\Big((-1)^{\alpha\beta}\frac{b^\alpha}{a^\beta}\Big)^{(q-1)/n},$$

where $\alpha = v_K(a)$, $\beta = v_K(b)$.

Proof: The function

$$(a,b) := \omega\Big((-1)^{\alpha\beta}\frac{b^{\alpha}}{a^{\beta}}\Big)^{(q-1)/n}$$

is obviously bilinear (in the multiplicative sense). We may therefore assume that a and b are prime elements: $a=\pi$, $b=-\pi u$, $u\in U_K$. Since clearly $(\pi,-\pi) = \big(\frac{\pi,-\pi}{\mathfrak p}\big) = 1$, we may restrict to the case $a=\pi$, $b=u$. Let $y=\sqrt[n]{u}$ and $K'=K(y)$. Then we have

$$(\pi,u) = \omega(u)^{(q-1)/n} \quad\text{and}\quad (\pi, K'|K)y = \Big(\frac{\pi,u}{\mathfrak p}\Big)y.$$

By (3.3), we see that $K'|K$ is unramified and by chap. IV, (5.7), $(\pi, K'|K)$ is the Frobenius automorphism $\varphi=\varphi_{K'|K}$. Consequently,

$$\Big(\frac{\pi,u}{\mathfrak p}\Big) = \frac{\varphi y}{y} \equiv y^{q-1} = u^{(q-1)/n} \equiv \omega(u)^{(q-1)/n} = (\pi,u) \bmod \mathfrak p,$$

hence $\big(\frac{\pi,u}{\mathfrak p}\big) = (\pi,u)$, because μ_{q-1} is mapped isomorphically onto κ^* by $\varepsilon \mapsto \varepsilon \bmod \mathfrak p$. □

The proposition shows in particular that the Hilbert symbol

$$\Big(\frac{\pi,u}{\mathfrak p}\Big) = \omega(u)^{(q-1)/n}$$

(in the case $(n,p)=1$) is independent of the choice of the prime element π. We may therefore put

$$\Big(\frac{u}{\mathfrak p}\Big) := \Big(\frac{\pi,u}{\mathfrak p}\Big) \quad\text{for } u\in U_K,$$

$\big(\frac{u}{\mathfrak p}\big)$ is the root of unity determined by

$$\Big(\frac{u}{\mathfrak p}\Big) \equiv u^{(q-1)/n} \bmod \mathfrak p.$$

We call it the **Legendre symbol**, or the *n-th* **power residue symbol**. Both names are justified by the

(3.5) **Proposition.** *Let $(n,p)=1$ and $u\in U_K$. Then one has*

$$\left(\frac{u}{\mathfrak{p}}\right) = 1 \quad \Longleftrightarrow \quad u \text{ is an } n\text{-th power } \bmod \mathfrak{p}_K . \qquad \blacksquare$$

Proof: Let ζ be a primitive $(q-1)$-th root of unity, and let $m = \frac{q-1}{n}$. Then ζ^n is a primitive m-th root of unity, and

$$\left(\frac{u}{\mathfrak p}\right) = \omega(u)^m = 1 \iff \omega(u) \in \mu_m \iff \omega(u) = (\zeta^n)^\nu$$

$$\iff u \equiv \omega(u) = (\zeta^\nu)^n \mod \mathfrak p_K \qquad \square$$

It is an important, but in general difficult problem to find explicit formulae for the Hilbert symbol $\left(\frac{a,b}{\mathfrak p}\right)$ also in the case $\mathfrak p \mid n$. Let us look at the case where $n = 2$ and $K = \mathbb Q_p$. If $a \in \mathbb Z_2$, then $(-1)^a$ means

$$(-1)^a = (-1)^r,$$

where r is a rational integer $\equiv a \bmod 2$.

(3.6) **Theorem.** *Let $n = 2$. For $a, b \in \mathbb Q_p^*$, we write*

$$a = p^\alpha a', \quad b = p^\beta b', \quad a', b' \in U_{\mathbb Q_p}.$$

If $p \neq 2$, then

$$\left(\frac{a,b}{p}\right) = (-1)^{\alpha\beta\varepsilon(p)}\left(\frac{a'}{p}\right)^\beta\left(\frac{b'}{p}\right)^\alpha.$$

In particular, one has $\left(\frac{p,p}{p}\right) = (-1)^{\varepsilon(p)}$ and $\left(\frac{p,u}{p}\right) = \left(\frac{u}{p}\right)$, if u is a unit. If $p = 2$, and $a, b \in U_{\mathbb Q_2}$, then

$$\left(\frac{2,a}{2}\right) = (-1)^{\omega(a)},$$

$$\left(\frac{a,b}{2}\right) = (-1)^{\varepsilon(a)\varepsilon(b)}.$$

Proof: The claim for the case $p \neq 2$ is an immediate consequence of (3.4), and will be left to the reader. So let $p = 2$. We put $\omega(a) = \frac{a^2-1}{8}$ and $\varepsilon(a) = \frac{a-1}{2}$. An elementary computation shows that

$$\omega(a_1a_2) \equiv \omega(a_1) + \omega(a_2) \bmod 2 \quad \text{and} \quad \varepsilon(a_1a_2) \equiv \varepsilon(a_1) + \varepsilon(a_2) \bmod 2.$$

Thus both sides of the equations we have to prove are multiplicative in a and b, and it is enough to check the claim for a set of generators of $U_{\mathbb Q_2}/U_{\mathbb Q_2}^2$. $\{5, -1\}$ is such a set. We postpone this for the moment and define $(a, b) = \left(\frac{a,b}{2}\right)$.

We have = I if and only if xis a norm from (b(R)I(f2, i.e., x = + V. z E Since 5 = 4 + 1 and 2 = 1 + I, we find that (-1,2) = = I. we had (-1, - 1) = L then it would follow that *(-1.x)* = 1 for all *x,* i.e., -1 would be a square in IQ2,, which i� not the case. Therefore we have (-1, - I) = - 1.

We have (2.2) = (2. - 1) = I and (5,5) = (5, - I)= I. It remains therefore to Jetennine = I would imply (2, _\) = I for all *X,* which is not the case. Hence (2, 5) = -1.

By direct verification one sees that the values we ju�l found coincide with those of (-1)'1("l, resp. (-If(aJi(hl, in the respective cases.

It remains to show that *U\hl* Uj, j<; generated by {5, - I}. We <;et *U* = *U.:;:,;,_, u(n!* =*Utt* By chap. IL (5.5) , exp: *2nz?---+ U(nl* j._ an isomorphism for *n* > I. Since *a* i---+ *2a* defines an isomorphi<;m 2^2Z_2 ---+ $2^1 2_2$, *x* i + defines an isomorphi�m *UM* ----,. ur'1. It follows that ()('1 £ U^2. Since \I, -1,5, -5} is a�y<;tem of representative<; of U/U('l, *U/U*^{2} is generated by-land5. □

It is much more difficult to determine the n-th Hilbert symbol in the general ca1se. It was discovered only in 1964 by the mathematician *Hn.,\Wi BNUCK.',I N.* Since the result has not previously been published in an easily accessible place, we state it here without proof for the case 11 = *pv* of odd residue characteristic *p* of *K.*

So let *Jlp"* £ *K,* choose a prime element *Jr* of *K,* and let *W* be the ring of integer� of the maximal unramified �ubextension *T* of *K* IIQ,, (i.e., the ring of Witt vectors over the residue class field of K). Then every element r E *K* can be written in the form

x � f(rr),

with a Laurent series /(X) E W((X)).

For an arbitrary Laurent serie� *f(X)* = *L* $a_1 X^1$ E *W((X)),* let *lP (X)* denote the �eries

$$f^{\mathcal{P}}(X) = \sum a_i^{\varphi} X^{ip},$$

where *I.{!* is the Frobenius automorphism of *W.* Further, let Res(/'dX) E *W* denote the re�idue of the differential *fdX,*

d log *l* :=

and

$$\log f := \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(f-1)^i}{i},$$

;1 *f* E I+ pWl[XJJ.

Now let ζ be a primitive p^n-th root of unity. Then $1-\zeta$ is a prime element of $\mathbb{Q}_p(\zeta)$, and thus

for some unit ε of K, where e is the ramification index of $K|\mathbb{Q}_p(\zeta)$. Let $\varphi(X) \in W[[X]]$ be a power series such that

$$\varepsilon = \varphi(\pi),$$

and let $h(X)$ be the series

$$h(X) = \frac{1}{2}\,\frac{1+(1-X^e\varphi(X))^{p^n}}{1-(1-X^e\varphi(X))^{p^n}} = \sum_{i=-\infty} a_i X^i,\ a_i \in W,\ \lim_{i\to-\infty} a_i = 0.$$

With this notation we can now state BRÜCKNER's formula for the p^n-th Hilbert symbol $\left(\frac{x,y}{\mathfrak{p}}\right)$, $p = \operatorname{char}(\kappa) \neq 2$.

(3.7) **Theorem.** *If $x, y \in K^*$ and $f, g \in W((X))^*$ such that $f(\pi) = x$ and $g(\pi) = y$, then*

$$\left(\frac{x,y}{\mathfrak{p}}\right) = \zeta^{w(x,y)}$$

where

$$w(x,y) = \operatorname{Tr}_W \operatorname{Res} h\cdot\Big(\frac{1}{p}\log\frac{f^p}{f^P}\,d\log g - \frac{1}{p}\log\frac{g^p}{g^P}\,\frac{1}{p}\,d\log f^P\Big) \bmod p^n.$$

For the proof of this theorem, we have to refer to [20] (see also [69] and [135]). BRÜCKNER has also deduced an explicit formula for the case $n = 2^m$, but it is much more complicated. A more recent treatment of the theorem, which also includes the case $n = 2^m$, has been given by G. HENNIART [69].

It would be interesting to deduce from these formulae the following classical result of IWASAWA [80], ARTIN and HASSE (see [9]) relative to the field

where ζ is a primitive p^n-th root of unity ($p \neq 2$). Putting $\pi = 1-\zeta$ and denoting by S the trace map from Φ_n to $\mathbb{Q}_p$, we obtain for the p^n-th Hilbert symbol $\left(\frac{x,y}{\mathfrak{p}}\right)$ of the field Φ_n the

(3.8) Proposition. *For a* E *and h* E *<tii one hm,*

$$\text{(I)} \qquad \left(\frac{a,b}{\mathfrak{p}}\right) = \zeta^{S(\zeta \log a\; D \log b)/p^{\nu}},$$

where D $\log h$ *denotes the fomial logarithmic* deriw1tive *in* IT of an *arbitrary representation ofh* as *an integral* power series *inn with coefficients* in *Zp.*

Fora EU�, one has *furthermore the* two **supplementary theorems**

$$\text{(2)} \qquad \left(\frac{\zeta, a}{\mathfrak{p}}\right) = \zeta^{S(\log a)/p^{\nu}},$$

$$\text{(3)} \qquad \left(\frac{a, \pi}{\mathfrak{p}}\right) = \zeta^{S((\zeta/\pi)\log a)/p^{\nu}}.$$

The supplcmentmy theorems (2) and (3) go back to *ART!•V* and *HAsst* 191. The formula (I) was proved independently by *AHii,',*' [10] and *H1tsst* 161] in the case $v = 1$, and by */WA\AWA* [80] in general. In the case $v =$ I. for instance, one can indeed obtain the formulae from *BRUCKNt.H's* theorem (3.7). Since

-^{I}S((rr') � 11 mod *p.* i = *p-1.*
p *Omodp,* i *-1-1,-1,* and $\log a =$ 0 mod p^2,

one may also inlcrpret the (-exponent in the formulae (I)--{3) as the *(p-* I)-st coefficient of a rr-adic expansion of $\log a$ $D \log h$. In this way it appears as a fonnal residue Res$_{11}$ --;;ſ $\log a$ $D \log h$. As to the '-upplcmentary theorems. one ha� to define also $D \log (= -(^{-1}$, Dlogn = rr^{-1}.

Exercise **1.** For $n = 2$ the Hilbert symbol ha" the following concrete meaning:

(¥) = I <=:::> *u.1.*2 + */1y"* - :" = O ha� a nontrivial '-Olution m *K.*

Exercise 2. Deduce proposition (3.8) from theorem (3.7).

Exercise 3. Let K be a lornl field of characteristic *p.* let K be it\ "eparable clo�ure. and let $W_n(\overline{K})$ he the ring of Witt vectors of length *n.* wilh the operator t,J: *W,,(J<).....;.* $W_n(\overline{K})$, $\wp a = Fa - a$ (�ee chap. IV. §3. exerci�c, 2 and 3). Show that one has $\ker(\wp) = W_n(\mathbb{F}_p)$.

Excrcir.e **4.** Ah�tracl Kummer theory IV.(3.3)) yields for the maximal ahehan exlcn�ion LI *K* ot exponent *II* a ,urJectivc **honmmocpl,,sm**

W,,(K) _,,. Hom(G(l,lK), W$_{11}$(1�'$_{1}$)), 1 f--* *X,,*

where one ha,
�uch that p� = ,(.

Exercise 5. Deline, for x E $W''(K)$ and a EK*. thesymbol $[x.a)$ E $W,,W_{1)}$ by

$$[r.a) := x,((a.LIK)),$$

where (, LIK) i� lhe nonn rc�idue \ymbol. Show;

(i) [x,a) = (a.K(!;)[K)!; -!;, iq E$W_{11}(i<)$ with r,Ji'; =X.

(i1) [r+y,a)=lx,a)+fv.a).

(iii) I-Lah)= [,1.,a) + [.1,h).

(iv) = 0 -¢==} a E NkiOlkK(l;)*, where/; E $W,,(i<)$ i� an ekment \Ueh that

(v)[J,a)=OforallaEK* {=::} 1 E,pW,,(K).

(vi) (r.a) = 0 for all .1 E $W,,(K)$-¢==} a E $K^{*1\cdots}$

Exercise **6.** Let κ be the re�iduc class field of K and n a prune elemcrn �uch that $K = \kappa((n))$. Let

$$d:K---;.Q11K'' \quad jf------*df,$$

he the rnnonical map to the differential module of K IK (�ee chap. Ill, * 2, p.200) For every f E K one ha�

$$df = f'_\pi d\pi\,,$$

where i� the formal derivative of/ 111the expansion according to powers of π with m K. Show that for r,J = $\sum_{i>-\infty} a_i\pi^i)d\pi$, the *residue*

$$\text{Rescv:=a-1}$$

doe� not depend on the choice of the prime clement n.

Exercir.e 7. Show that in the ca�c $n = 1$ the symbol [r.aJ i� given by

$$[r.a) = Tr�11fi',,$$

Remark: Su<.:h a tonnula can also be given for n:::: I (P. *Koutt* 1881).

§ 4. Formal Groups

The mo�t explicit realization of local cla�s field theory we have encountered for the case of cyclotomic fields over the field i.e.. with the ex- where (is a p''-th root of unity. notion of formal group us construct �uch an explicit cyclotomic theory over an arbitrary local field K by introducing a new kind of roots of unity which are "division points" that do the same for the field K as the p^{11}-th rooh of unity do for the field '!Jlp-

(4.1) Definition. *A (1-dimensional, commutative)* **formal group** *over a ring* $\mathfrak{o}$ is *a* formal power *series* $F(X,Y) \in \mathfrak{o}[[X,Y]]$ *with the* following properties:

(i) $F(X,Y) \equiv X + Y \mod \deg 2$,

(ii) $F(X,Y) = F(Y,X)$ "*commutativity*",

(iii) $F(X, F(Y,Z)) = F(F(X,Y),Z)$ "*associativity*".

From a formal group one gets an ordinary group by evaluating in a domain where the power series converge. If for instance $\mathfrak{o}$ is a complete valuation ring and $\mathfrak{p}$ its maximal ideal, then the operation

$$x \underset{F}{+} y := F(x,y)$$

defines a new structure of abelian group on the set $\mathfrak{p}$.

Examples:

1. $\hat{\mathbb{G}}_a(X,Y) = X + Y$ (the formal additive group).

2. $\hat{\mathbb{G}}_m(X,Y) = X + Y + XY$ (the formal multiplicative group). Since

$$X + Y + XY = (1+X)(1+Y) - 1,$$

we have

$$(x \underset{\hat{\mathbb{G}}_m}{+} y) + 1 = (x+1)\cdot(y+1).$$

So the new operation $\underset{\hat{\mathbb{G}}_m}{+}$ is obtained from multiplication via the translation $x \mapsto x + 1$.

3. A power series $f(X) = a_1X + a_2X^2 + \cdots \in \mathfrak{o}[[X]]$ whose first coefficient a_1 is a unit admits an "inverse", i.e., there exists a power series

$$f^{-1}(X) = a_1^{-1}X + \cdots \in \mathfrak{o}[[X]],$$

such that $f^{-1}(f(X)) = f(f^{-1}(X)) = X$. For every such power series,

$$F(X,Y) = f^{-1}(f(X) + f(Y))$$

is a formal group.

(4.2) Definition. *A* **homomorphism** $f: F \to G$ *between two formal groups is a power series* $f(X) = a_1X + a_2X^2 + \cdots \in \mathfrak{o}[[X]]$ *such that*

$$f(F(X,Y)) = G(f(X), f(Y)).$$

In example 3, for instance, the power series f is a homomorphism of the formal group F to the additive group $\hat{\mathbb{G}}_a$. It is called the *logarithm* of F.

A homomorphism $f : F \to G$ is an *isomorphism* if $a_1 = f'(0)$ is a unit, i.e., if there is a homomorphism $g = f^{-1} : G \to F$ such that

$$f(g(X)) = g(f(X)) = X.$$

If the power series $f(X) = a_1X + a_2X^2 + \cdots$ satisfies the equation $f(F(X,Y)) = G(f(X), f(Y))$, but its coefficients belong to an extension ring $\mathfrak{o}'$, then we call this a homomorphism *defined over* $\mathfrak{o}'$. The following proposition is immediately evident.

(4.3) Proposition. *The homomorphisms $f : F \to F$ of a formal group F over $\mathfrak{o}$ form a ring $\operatorname{End}_{\mathfrak{o}}(F)$ in which addition and multiplication are defined by*

$$(f +_F g)(X) = F(f(X), g(X)), \quad (f \circ g)(X) = f(g(X)).$$

(4.4) Definition. *A* **formal $\mathfrak{o}$-module** *is a formal group F over $\mathfrak{o}$ together with a ring homomorphism*

$$\mathfrak{o} \to \operatorname{End}_{\mathfrak{o}}(F), \quad a \mapsto [a]_F(X),$$

such that $[a]_F(X) \equiv aX \bmod \deg 2$.

A homomorphism (over $\mathfrak{o}' \supseteq \mathfrak{o}$) between formal $\mathfrak{o}$-modules F, G is a homomorphism $f : F \to G$ of formal groups (over $\mathfrak{o}'$) in the sense of (4.2) such that

$$f([a]_F(X)) = [a]_G(f(X)) \quad \textit{for all } a \in \mathfrak{o}.$$

Now let $\mathfrak{o} = \mathfrak{o}_K$ be the valuation ring of a local field K, and write $q = (\mathfrak{o}_K : \mathfrak{p}_K)$. We consider the following special formal $\mathfrak{o}_K$-modules.

(4.5) Definition. *A* **Lubin-Tate module** *over $\mathfrak{o}_K$ for the prime element π is a formal $\mathfrak{o}_K$-module F such that*

$$[\pi]_F(X) \equiv X^q \bmod \pi.$$

This definition reflects once more the dominating principle of class field theory, to the effect that prime elements correspond to Frobenius elements. In fact, if we reduce the coefficients of some formal $\mathfrak o$-module F modulo π, we obtain a formal group $\bar F(X,Y)$ over the residue class field $\mathbb F_q$. The reduction mod π of $[\pi]_F(X)$ is an endomorphism of $\bar F$. But on the other hand, $\varphi(X) = X^q$ is clearly an endomorphism of $\bar F$, its *Frobenius endomorphism*. Thus F is a Lubin-Tate module if the endomorphism defined by a prime element π gives via reduction the Frobenius endomorphism of $\bar F$.

Example: The formal multiplicative group $\hat{\mathbb G}_m$ is a formal $\mathbb Z_p$-module with respect to the mapping

$$\mathbb Z_p \to \operatorname{End}_{\mathbb Z_p}(\hat{\mathbb G}_m), \quad a \mapsto [a]_{\hat{\mathbb G}_m}(X) = (1+X)^a - 1 = \sum_{\nu=1}^{\infty}\binom{a}{\nu}X^\nu.$$

$\hat{\mathbb G}_m$ is a Lubin-Tate module for the prime element p because

$$[p]_{\hat{\mathbb G}_m}(X) = (1+X)^p - 1 \equiv X^p \mod p.$$

The following theorem gives a complete and explicit overall view of the totality of all Lubin-Tate modules. Let $e(X), \bar e(X) \in \mathcal O_K[[X]]$ be Lubin-Tate series for the prime element π of K, and let

$$F_e(X,Y) \in \mathcal O_K[[X,Y]] \quad\text{and}\quad [a]_{e,\bar e}(X) \in \mathcal O_K[[X]]$$

($a \in \mathcal O_K$) be the power series (uniquely determined according to (2.2)) such that

$$F_e(X,Y) \equiv X + Y \mod \deg 2, \qquad e(F_e(X,Y)) = F_e(e(X), e(Y)),$$

$$[a]_{e,\bar e}(X) \equiv aX \mod \deg 2, \qquad e([a]_{e,\bar e}(X)) = [a]_{e,\bar e}(\bar e(X)).$$

If $e(X) = \bar e(X)$ we simply write $[a]_{e,e}(X) = [a]_e(X)$.

(4.6) Theorem. (i) *The Lubin-Tate modules for π are precisely the series $F_e(X,Y)$, with the formal $\mathcal O_K$-module structure given by*

$$\mathcal O_K \longrightarrow \operatorname{End}_{\mathcal O_K}(F_e), \quad a \longmapsto [a]_e(X).$$

(ii) *For every $a \in \mathcal O_K$ the power series $[a]_{e,\bar e}(X)$ is a homomorphism*

$$[a]_{e,\bar e} : F_{\bar e} \longrightarrow F_e$$

of formal $\mathfrak o$-modules, and it is an isomorphism if a is a unit.

Proof: If F is any Luhin~Tate module, then e(X) := [rr)F(X) E £71 and F = F,, becam,e e(F(X, Y)) = F(c(X),e(Y)). and because of the uniqueness statement of (2.2). For the other claims of the theorem one has to show the following formulae.

(I) F,(X, Y) � F,.(Y,X),

(2) F,(X. c;.(Y, Z)) � F,.(F,.(X. Y). ZJ,

(3) [a[,. ,(Fa(X, Y)J � F,.([a[,. a(X). [a],.,(YJJ,

(4) [a+ hJc.o(X) � F,([u],..,(X). [h[,. ,(X)).

(5)[ahl,J(X) � [al, ,([hi, i(X)J.

(6) [,r [,.(X) � c(XJ.

(I) and (2) �how that Fe is a fonnal group. (3), (4), and (5) 5how that

OK.._ EndoK (Fe), a!-------'>- [a],,,

is a homomorphi�m of rings, i.e., that F,, b a formal OK-module, and that [ale.<' is a homomorphi5m of formal 0K-module5 from Fe to F,,. Finally, (6) show� that F,, is a Lubin-Tate module.

The proof5 of these formulae all follow the same pattern. One checks that both sides of each fonnula are solutions of the same problem of (2.2). and then deduces their equality from the uniqueness 5talcment. In (6) for instance, both power series commence with the linear fonn rr X and satisfy the condition e([rrl,.(X)) = rrrl,(e(X)), resp. e(e(X)) = e(f(X)). □

Exercise I. End_0(G,,) consist\ of all aX such that a E ci.

Exercise 2. Let R be a commuta1ive Q-algcbra. Then for every formal group F(X, Y) over R, there cx1stq a unique isomorphism

log1 : F------>- G,,,

such 1ha1 $\log_1$ (X) = X mod deg 2. the **logarithm** of F.

Hint: Let $F_1 = \partial F/\partial Y$. Differentiating $F(F(X,Y),Z) = F(X,F(Y,Z))$ yield\ $\equiv 1$ mod deg 1. Let $\psi(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in R[[X]]$ be the power series that $\psi(X)F_1(X,0) = 1$. Then $\log_F(X) = X + \sum_{n=1}^{\infty} \frac{a_n}{n} X^n$ does what we want.

Exercise 3. log,:_.:,,,(X) = $\sum_{=1}^{\infty}(-1)^{n+1}\frac{X^n}{n} = \log(1+X)$.

Exercise **4.** Let ,r a prime element of the local lield K, and le! f(X) = X + ,r 'X" + .. Then

F(X.Y)=J ¹(/(XJ+f(Y)), [a]1-(X)=/ ¹(<1/"(X)), aEOK,

define\ a Lubin-Tt-1tc module with logarithm log $_1$= r

Exercise 5. Two Lubin-Tate modules over the valuation ring $\mathcal{O}_K$ of a local field K, but for different prime elements π and $\bar\pi$, are never isomorphic.

Exercise 6. Two Lubin-Tate modules F_π and $F_{\bar\pi}$ for prime elements π and $\bar\pi$ always become isomorphic over $\tilde{\mathcal{O}}$, where $\tilde K$ is the completion of the maximal unramified extension $\tilde K|K$.

Hint: The power series θ of (2.3) yields an isomorphism $\theta : F_\pi \to F_{\bar\pi}$.

§ 5. Generalized Cyclotomic Theory

Formal groups are relevant for local class field theory in that they allow us to construct a perfect analogue of the theory of the p^n-th cyclotomic field $\mathbb{Q}_p(\zeta)$ over $\mathbb{Q}_p$ with its fundamental isomorphism

$$G\big(\mathbb{Q}_p(\zeta)|\mathbb{Q}_p\big) \xrightarrow{\ \sim\ } (\mathbb{Z}/p^n\mathbb{Z})^*$$

(see chap. II (7.13)), replacing $\mathbb{Q}_p$ by an arbitrary local ground field K. The formal groups furnish a generalization of the notion of p^n-th root of unity, and provide an explicit version of the local reciprocity law in the corresponding extensions.

A formal $\mathcal{O}_K$-module gives rise to an ordinary $\mathcal{O}_K$-module if we read the power series over a domain in which they converge. We now choose for this the maximal ideal $\bar{\mathfrak{p}}$ of the valuation ring of the algebraic closure $\bar K$ of the given local field K. If $G(X_1,\dots,X_n)\in\mathcal{O}_K[[X_1,\dots,X_n]]$ is a power series with constant coefficient 0, and if $x_1,\dots,x_n\in\bar{\mathfrak{p}}$, then the series $G(x_1,\dots,x_n)$ converges in the complete field $K(x_1,\dots,x_n)$ to an element in $\bar{\mathfrak{p}}$. From the definition of the formal $\mathcal{O}$-modules and their homomorphisms we therefore obtain immediately the

(5.1) Proposition. *Let F be a formal $\mathcal{O}_K$-module. Then the set $\bar{\mathfrak{p}}$ with the operations*

$$x \underset{F}{+} y = F(x,y) \quad\text{and}\quad a \underset{F}{\cdot} x = [a]_F(x),$$

$x, y \in \bar{\mathfrak{p}}$, $a \in \mathcal{O}_K$, *is an $\mathcal{O}_K$-module in the usual sense.* We denote it *by $\bar{\mathfrak{p}}_F$*

If *f* : *F* ----+ *(J* is a homomorphism (isomorphism) of fonnal OK-modules, then

f:IJF-------+Pc, *xi--------+f(x),*

is a homomorphism (bomorphism) of ordinary OK-modules.

The opcralions in p*F,* and particularly scalar multiplication *o • x = [a],. (x),* must of course nol be confused with the usual operation� in the field *K.*

We now consider a Lubin-Tate module *F* for the prime element *n* of *OK.* We define the group of n"-division points by

$$F(n) = \{\lambda \in \overline{\mathfrak{p}}_F \mid \pi^n \cdot \lambda = 0\} = \ker([\pi^n]_F)$$

This is an OK-module, and an *oK/TrnOK-module* because it i� killed by *n"oK.*

(5.2) Proposition. F(11) *i.\;1freeoK/TrnOK-moduleofrnnk* l.

Proof: An isomorphism *f"* *F* ----+ *(J* of Lubin-Tate module� obviously induce� isomorphi5ms *f* • *IJF* ----+ Pc and *f* F(n) � *G(n)* of *OK*-modules. By (4.6), Lubin-Tate modules for the same prime element ;r are all i�omorphic. We may therefore assume that *F = Fe,* with *e(X) = X'I +n X =* lnlF(X). *F(n)* then consists of the *q"* zeroes of the iterated polynomial e"(X) = (e o • • o e)(X) = Ln"J,. (X), which is ea�ily shown, by induction on *n,* to be separable. Now if A,. E F(11) "- *F(n* - 1), then

OK-------+F(n). of------fa•An,

is a homomorphi�m of OK-modules with kernel *n"oK.* It induces a bijective homomorphism *OK /n"vK* ----+ *F(n)* because both sides arc of order *q".* fJ

(5.3) Corollary. *A.�.mciatingo* f--+ lo]F *we obtain canonical isomorphism.�*

$$\mathcal{O}_K/\pi^n\mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K}(F(n)) \quad \text{and} \quad U_K/U_K^{(n)} \longrightarrow \mathrm{Aut}_{\mathcal{O}_K}(F(n))$$

Proof: The map on the left is an isomorphism since *vK /nnoK* � *F(n)* and *End$_0$K(oK/HnOK)* = *oK/n"oK.* The one on the right is obtained by taking the unit groups of these rings. D

Given a Lubin-Tate module F for the prime element π, we now define the **field of π^n-division points** by

$$L_n = K(F(n)).$$

Since $F(n) \subseteq F(n+1)$ we get a tower of fields

$$K \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_\pi := \bigcup_{n=1}^{\infty} L_n .$$

These fields are also called the **Lubin-Tate extensions.** They only depend on the prime element π, not on the Lubin-Tate module F. For if G is another Lubin-Tate module for π, then by (4.6), there is an isomorphism $f : F \to G$, $f \in \mathcal{O}_K[[X]]$ such that $G(n) = f(F(n)) \subseteq K(F(n))$, and hence $K(G(n)) = K(F(n))$. If F is the Lubin-Tate module F_e belonging to a Lubin-Tate polynomial $e(X) \in \mathcal{E}_\pi$, then $e(X) = [\pi]_F(X)$ and $L_n|K$ is the splitting field of the n-fold iteration

$$e^n(X) = (e \circ \dots \circ e)(X) = [\pi^n]_F(X).$$

Example: If $\mathcal{O}_K = \mathbb{Z}_p$ and F is the Lubin-Tate module $\hat{\mathbb{G}}_m$, then

$$e^n(X) = [p^n]_{\hat{\mathbb{G}}_m}(X) = (1+X)^{p^n} - 1.$$

So $\hat{\mathbb{G}}_m(n)$ consists of the elements $\zeta - 1$, where ζ varies over the p^n-th roots of unity. $L_n|K$ is therefore the p^n-th cyclotomic extension $\mathbb{Q}_p(\mu_{p^n})|\mathbb{Q}_p$. The following theorem shows the complete analogy of Lubin-Tate extensions with cyclotomic fields.

(5.4) Theorem. *$L_n|K$ is a totally ramified abelian extension of degree $q^{n-1}(q-1)$ with Galois group*

$$G(L_n|K) \cong \operatorname{Aut}_{\mathcal{O}_K}(F(n)) \cong U_K/U_K^{(n)},$$

i.e., for every $\sigma \in G(L_n|K)$ there is a unique class $u \bmod U_K^{(n)}$, with $u \in U_K$ such that

$$\lambda^\sigma = [u]_F(\lambda) \quad \text{for} \quad \lambda \in F(n).$$

Furthermore the following is true: let F be the Lubin-Tate module F_e associated to the polynomial $e(X) \in \mathcal{E}_\pi$, and let $\lambda_n \in F(n) \setminus F(n-1)$. Then λ_n is a prime element of L_n, i.e., $L_n = K(\lambda_n)$, and

$$\varphi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = X^{q^{n-1}(q-1)} + \dots + \pi \in \mathcal{O}_K[X]$$

is its minimal polynomial. In particular one has $N_{L_n|K}(-\lambda_n) = \pi$.

Proof: If

$$e(X) = X^q + \pi(a_{q-1}X^{q-1}+\cdots+a_2X^2)+\pi X$$

is a Lubin-Tate polynomial, then

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = e^{n-1}(X)^{q-1}+\pi(a_{q-1}e^{n-1}(X)^{q-2}+\cdots+a_2e^{n-1}(X))+\pi$$

is an Eisenstein polynomial of degree $q^{n-1}(q-1)$. If F is the Lubin-Tate module associated to e, and $\lambda_n \in F(n) \setminus F(n-1)$, then λ_n is clearly a zero of this Eisenstein polynomial, and is therefore a prime element of the totally ramified extension $K(\lambda_n)|K$ of degree $q^{n-1}(q-1)$. Each $\sigma \in G(L_n|K)$ induces an automorphism of $F(n)$. We therefore obtain a homomorphism

$$G(L_n|K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_K}\big(F(n)\big) \cong U_K/U_K^{(n)}.$$

It is injective because L_n is generated by $F(n)$, and it is surjective because

$$\#G(L_n|K) \ge \big[K(\lambda_n):K\big] = q^{n-1}(q-1) = \#U_K/U_K^{(n)}.$$

This proves the theorem. □

Generalizing the explicit norm residue symbol of the cyclotomic fields (see (2.4)), we obtain the following explicit formula for the symbol of the Lubin-Tate extensions.

(5.5) **Theorem.** *For the field $L_n|K$ of π^n-division points and for $a = u\pi^{v_K(a)} \in K^*$, $u \in U_K$, one has*

$$(a, L_n|K)\lambda = [u^{-1}]_F(\lambda), \quad \lambda \in F(n).$$

Proof: The proof is the same as that of (2.4). Let $\sigma \in G(L_n|K)$ be the automorphism such that

$$\lambda^\sigma = [u^{-1}]_F(\lambda), \quad \lambda \in F(n).$$

Let $\tilde\sigma$ be an element in $\mathrm{Frob}(\tilde L_n|K)$ such that $\tilde\sigma|_{L_n} = \sigma$ and $d_K(\tilde\sigma) = 1$. We view $\tilde\sigma$ as an automorphism of the completion $\hat L_n = L_n\hat{\tilde K}$ of $\tilde L_n$. Let Σ be the fixed field of $\tilde\sigma$. Since $d_K(\tilde\sigma) = 1$, $\Sigma|K$ is totally ramified. It has degree $q^{n-1}(q-1)$ because $\Sigma\cap\tilde K = K$ and $\tilde\Sigma = \Sigma\tilde K = \tilde L_n$. Consequently $[\Sigma:K] = [\tilde L_n:\tilde K] = [L_n:K]$.

Now let *e* E *En, e* E *Err* be Lubin-Tate series over *OK,* where Jr= *urf,* and let $F = F,;$. By (2.3), there exi&ls a power series 0(X) =*EX+* E OR[[X]]. with EE *UK,* such that

0'-P = 0 o [ulF and *0'-P ::iC = eo0* (tp = tpK}.

Let *An* E *F(n)* "- *F(n -* I). i\.11 is a prime element of *L11*. and

i5 a prime element of *E* because

rrf = *0<f(A�) = 0q'(* [u-^{1}JrCAn)) = *0(An)* = rrr;.

Since *ei(0(An))* = *()rf'* (e"'(A,1)) = 0 for i = *n,* and# 0 fori = *n* - 1, we have JrJ; E *F,,(n)* "- *F,,(n -* I). Hence *E* = K(rrr;) is the field of *rrn*-division points of *Fe,* and *Nr;1K(-nr;)* = Jr = *urf* by (5.4). Since rr = *NLn1d-An)* E *N1.,,wL�,* we get

rL/JIK(a) = *Nr:1K(-rrr;)* = Jr a= 11 tnod *NL,,1KL;.*

and thw,

$$(a, L_n|K) = (\pi^{v_K(a)}, L_n|K)(u, L_n|K) = (u, L_n|K) = \sigma . \qquad \square$$

(5.6) **Corollary.** *The field Ln* I*K* ofrr11*-divi.<,ion poinls* i1> *the class field* relative *tothegroup(rr)* x *Ut*^{1}s; *K*.*

Proof: For *a= urr"K(a)* we have

aEN1,wL;-<==}(a,LnlK)=i{::::::::}f11-^{1}]F(A)=A forallAEF(n)
{=::::} [u-^{1}JJ, = *idf"(n)* -¢=:} 11-1 EU¼!)-<==} *a* E (rr) *XU¼,).*

$\square$

For the maximal abelian extension *K""IK,* thb give& the following generalization of the local Kronecker-Weber theorem (1.9):

(5.7) **Corollary.** *The maximal abelian extension of K* is *the compo.�ite*

K"h= f<Lrr,

where *Ln is /he union* LJ�1 *Ln* of *the fields L,,* ofrrn-division *point.�.*

Proof: Let $L|K$ be a finite abelian extension. Then we have $\pi^f \in N_{L|K}L^*$ for suitable f. Since $N_{L|K}L^*$ is open in K^*, and since the $U_K^{(n)}$ form a basis of neighbourhoods of 1, we have $(\pi^f)\times U_K^{(n)} \subseteq N_{L|K}L^*$ for a suitable n. Hence L is contained in the class field of the group $(\pi^f)\times U_K^{(n)} = ((\pi)\times U_K^{(n)}) \cap ((\pi^f)\times U_K)$. The class field of $(\pi)\times U_K^{(n)}$ is L_n, and that of $(\pi^f)\times U_K$ is the unramified extension K_f of degree f. It follows that $L \subseteq K_f L_n \subseteq \widetilde{K} L_\pi$. □

Exercise 1. Let $F = F_\pi$ be the Lubin-Tate module for the Lubin-Tate series $e \in \mathcal{E}_\pi$ with the endomorphisms $[a] = [a]_F$. Let $S = \mathcal{O}_K[[X]]$ and $S^* = \{g \in S \mid g(0) \in U_K\}$. Show:

(i) If $g \in S$ is a power series such that $g(F(1)) = 0$, then g is divisible by $[\pi]$, i.e., $g(X) = [\pi](X)h(X)$, $h(X) \in S$.

(ii) Let $g \in S$ be a power series such that

$$g(X +_F \lambda) = g(X) \quad \text{for all } \lambda \in F(1),$$

where we write $X +_F \lambda = F(X,\lambda)$. Then there exists a unique power series $h(X)$ in S such that

$$g = h \circ \pi.$$

Exercise 2. If $h(X)$ is a power series in S, then the power series

$$h_1(X) = \prod_{\lambda \in F(1)} h(X +_F \lambda)$$

also belongs to S, and one has $h_1(X +_F \lambda) = h_1(X)$ for all $\lambda \in F(1)$.

Exercise 3. Let $N(h) \in S$ be the power series (uniquely determined by exercise 1 and exercise 2) such that

$$N(h)\circ[\pi] = \prod_{\lambda \in F(1)} h(X +_F \lambda).$$

This mapping $N : S \to S$ is called Coleman's **norm** operator. Show:

(i) $N(h_1h_2) = N(h_1)N(h_2)$.

(ii) $N(h) \equiv h \bmod \mathfrak{p}$.

(iii) $h \in X^iS^*$ for $i \geq 0 \Rightarrow N(h) \in X^iS^*$.

(iv) $h \equiv 1 \bmod \mathfrak{p}^\nu$ for $\nu \geq 1 \Rightarrow N(h) \equiv 1 \bmod \mathfrak{p}^{\nu+1}$.

(v) For the operators $N^0(h) = h$, $N^\nu(h) = N(N^{\nu-1}(h))$, one has

$$N^\nu(h)([\pi^\nu]) = \prod_{\lambda \in F(\nu)} h(X +_F \lambda), \quad \nu \geq 0.$$

(vi) If $h \in X^iS^*$, $i \geq 0$, then $N^{\nu+1}(h)/N^\nu(h) \in S^*$ and

$$N^{\nu+1}(h) \equiv N^\nu(h) \bmod \mathfrak{p}^{\nu+1}, \quad \nu \geq 0.$$

Exercise 4. Let $\lambda \in F(n+1) \setminus F(n)$, $n \geq 0$, and $\lambda_i = [\pi^{n-i}](\lambda) \in F(i+1)$ for $0 \leq i \leq n$. Then λ_i is a prime element of the Lubin-Tate extension $L_{i+1} = K(F(i+1))$, and $\mathcal{O}_{i+1} = \mathcal{O}[\lambda_i]$ is the valuation ring of L_{i+1}, with maximal ideal $\mathfrak{p}_{i+1} = \lambda_i \mathcal{O}_{i+1}$. Show:

Let $\beta_i \in \pi^{n-i}\mathfrak{p}_1\mathcal{O}_{i+1}$, $0 \leq i \leq n$. Then there exists a power series $h(X) \in \mathcal{O}[[X]]$ such that

$$h(\lambda_i) = \beta_i \quad \text{for} \quad 0 \leq i \leq n.$$

Hint: Write $\beta_i = \pi^{n-i}\lambda_0 h_i(\lambda_i)$, with $h_i(X) \in \mathcal{O}[X]$ and put, for $0 \leq i \leq n$: $g_i(X) = [\pi^{n+1}][\pi^i]/[\pi^{i-1}]$. Then $h = \sum_{i=0}^{n} h_i g_i$ is a solution.

Exercise 5. Let $\lambda \in F(n+1) \setminus F(n)$ and $\lambda_i = [\pi^{n-i}](\lambda)$, $0 \leq i \leq n$. For every $u \in U_{L_{n+1}}$, there exists a power series $h(X) \in \mathcal{O}[[X]]$ such that

$$N_{n,i}(u) = h(\lambda_i) \quad \text{for} \quad 0 \leq i \leq n,$$

where $N_{n,i}$ is the norm from L_{n+1} to L_{i+1}.

Hint: Write $u = h_1(\lambda)$, $h_1(X) \in \mathcal{O}[X]$, and put $h_2 = N^n(h_1) \in S^*$. Show that $\beta_i = N_{n,i}(u) - h_2(\lambda_i) \in \pi^{n-i}\mathfrak{p}_1\mathcal{O}_{i+1}$. Then by exercise 4 there is a $h_3(X) \in \mathcal{O}[[X]]$ such that $\beta_i = h_3(\lambda_i)$, $0 \leq i \leq n$. Show that $h = h_2 + h_3$ works.

Remark: The solutions of these exercises are discussed in detail in [79], 5.2.

§ 6. Higher Ramification Groups

Considering the homomorphism

$$(\ ,L|K) : K^* \to G(L|K)$$

defined for an abelian extension $L|K$ of local fields by the norm residue symbol, it is striking that both groups are equipped with a canonical filtration: in the group K^* on the left we have the descending chain

$$K^* \supseteq U_K = U_K^{(0)} \supseteq U_K^{(1)} \supseteq U_K^{(2)} \supseteq \cdots$$

of *higher unit groups* $U_K^{(n)}$, and on the right there is the descending chain

$$(**) \qquad G(L|K) \supseteq G^0(L|K) \supseteq G^1(L|K) \supseteq G^2(L|K) \supseteq \cdots$$

of *ramification groups* $G^t(L|K)$ in the upper numbering (see chap. II, § 10). The latter arose from the ramification groups in the lower numbering

$$G_s(L|K) = \{\sigma \in G(L|K) \mid v_L(\sigma a - a) \geq s+1 \quad \text{for all } a \in \mathcal{O}_L\}$$

via the strictly increasing function

$$\eta_{L|K}(s) = \int_0^s \frac{dt}{(G_0 : G_t)}$$

by the rule
$$G^i(L|K) = G_{\psi_{L|K}(i)}(L|K),$$
where ψ is the inverse function of φ. We will now prove the remarkable arithmetic fact that the norm residue symbol $(\ ,L|K)$ relates both filtrations (*) and (**) in a precise way. To this end we determine (generalizing chap. II, § 10, exercise 1) the higher ramification groups of the Lubin-Tate extensions.

(6.1) Proposition. *Let $L_n|K$ be the field of π^n-division points of a Lubin-Tate module for the prime element π. Then*
$$G_i(L_n|K) = G(L_n|L_k) \quad \text{for } q^{k-1} \le i \le q^k - 1.$$

Proof: By (5.4) and (5.5), the norm residue symbol gives an isomorphism $U_K^{(k)}/U_K^{(n)} \xrightarrow{\sim} G(L_n|L_k)$ for every k. Hence $G(L_n|L_k) = (U_K^{(k)}, L_n|K)$. We therefore have to show that
$$G_i(L_n|K) = (U_K^{(k)}, L_n|K) \quad \text{for } q^{k-1} \le i \le q^k - 1.$$
Let $\sigma \in G_1(L_n|K)$ and $\sigma = (u^{-1}, L_n|K)$. Then we have necessarily $u \in U_K^{(1)}$ because $(\ ,L_n|K): U_K/U_K^{(n)} \to G(L_n|K)$ maps the p-Sylow subgroup $U_K^{(1)}/U_K^{(n)}$ onto the p-Sylow subgroup $G_1(L_n|K)$ of $G(L_n|K)$. Let $u = 1 + \varepsilon\pi^m$, $\varepsilon \in U_K$, and $\lambda \in F(n) \setminus F(n-1)$. Then λ is a prime element of L_n and from (5.4) we get that
$$\lambda^\sigma = [u]_F(\lambda) = F(\lambda, [\varepsilon\pi^m]_F(\lambda)).$$
If $m \ge n$, then $\sigma = 1$, so that $i_{L_n|K}(\sigma) = \infty$. If $m < n$, then $\lambda_0 = [\pi^m]_F(\lambda)$ is a prime element of L_{n-m} and therefore also $[\varepsilon\pi^m]_F(\lambda) = [\varepsilon]_F(\lambda_0)$. As $L_n|L_{n-m}$ is totally ramified of degree q^m we may write $\lambda_0 = \varepsilon_0\lambda^{q^m}$ for some $\varepsilon_0 \in U_{L_n}$. Since $F(X,0) = X$, $F(0,Y) = Y$, we have $F(X,Y) = X + Y + XYG(X,Y)$ with $G(X,Y) \in o_K[[X,Y]]$. Thus
$$\lambda^\sigma - \lambda = F(\lambda, [\varepsilon]_F(\lambda_0)) - \lambda = \varepsilon_0\lambda^{q^m} + a\lambda^{q^m+1}, \quad a \in o_{L_n},$$
i.e.,
$$i_{L_n|K}(\sigma) := v_{L_n}(\lambda^\sigma - \lambda) = \begin{cases} q^m, & \text{if } m < n,\\ \infty, & \text{if } m \ge n.\end{cases}$$
By chap. II, § 10, we have $G_i(L_n|K) = \{\sigma \in G(L_n|K) \mid i_{L_n|K}(\sigma) \ge i+1\}$. Now let $q^{k-1} \le i \le q^k - 1$. If $u \in U_K^{(k)}$, then $m \ge k$, i.e., $i_{L_n|K}(\sigma) \ge q^k \ge i+1$, and thus $\sigma \in G_i(L_n|K)$. This proves the inclusion $(U_K^{(k)}, L_n|K) \subseteq G_i(L_n|K)$. If conversely $\sigma \in G_i(L_n|K)$ and $\sigma \ne 1$, then $i_{L_n|K}(\sigma) = q^m \ge i + 1 > q^{k-1}$, i.e., $m \ge k$. Consequently $u \in U_K^{(k)}$, and this shows the inclusion $G_i(L_n|K) \subseteq (U_K^{(k)}, L_n|K)$. □

From this proposition we get the following result, which may be considered the main theorem of higher ramification theory.

(6.2) Theorem. *If $L|K$ is a finite abelian extension, then the norm residue symbol*

$$(\ ,L|K): K^* \to G(L|K)$$

maps the group $U_K^{(n)}$ onto the group $G^n(L|K)$, for $n \ge 0$.

Proof: We may assume that $L|K$ is totally ramified. For if $L^0|K$ is the maximal unramified subextension of $L|K$, then we have on the one hand $G^n(L|K) = G^n(L|L^0)$ because $\psi_{L^0|K}(s) = s$ and $\psi_{L|K}(s) = \psi_{L|L^0}(\psi_{L^0|K}(s)) = \psi_{L|L^0}(s)$ (see chap. II, (10.8)). On the other hand, by chap. IV, (6.4), and chap. V, (1.2), we have

$$(U_{L^0}^{(n)}, L|L^0) = (N_{L^0|K}U_{L^0}^{(n)}, L|K) = (U_K^{(n)}, L|K),$$

so we may replace $L|K$ by $L|L^0$.

If now $L|K$ is totally ramified and π_L is a prime element of L, then $\pi = N_{L|K}(\pi_L)$ is a prime element of K and $(\pi) \times U_K^{(m)} \subseteq N_{L|K}L^*$ for m sufficiently big. Therefore $L|K$ is contained in the class field of $(\pi) \times U_K^{(m)}$, which, by (5.6), is equal to the field L_m of π^m-division points of some Lubin-Tate module for π. In view of chap. II, (10.9), and chap. IV, (6.4), we may even assume that $L = L_m$. By (6.1), the norm residue symbol maps the group $U_K^{(n)}$ onto the group

$$G(L_m|L_n) = G_i(L_m|K) \quad \text{for} \quad q^{n-1} \le i \le q^n - 1.$$

But we have (see chap. II, § 10)

$$\psi_{L|K}(q^n - 1) = \frac{1}{g_0}(g_1 + \cdots + g_{q^n-1})$$

with $g_i = \#G_i(L|K) = \#G(L_m|L_n) = q^{m-n}$ for $q^{n-1} \le i \le q^n - 1$. This yields $\psi_{L|K}(q^n - 1) = n$ and thus $(U_K^{(n)}, L|K) = G_{q^n-1}(L|K) = G^n(L|K)$. □

Higher ramification groups $G^t(L|K)$ were introduced for arbitrary real numbers $t \ge -1$. Thus we may ask for which numbers they change. We call these numbers the *jumps* of the filtration $\{G^t(L|K)\}_{t \ge -1}$ of $G(L|K)$. In other words, t is a jump if for all $\varepsilon > 0$, one has

$$G^t(L|K) \ne G^{t+\varepsilon}(L|K).$$

(6.3) **Proposition** *(IIA\SI: -A11r).* For *a finite abelian* exten.�ion LI *K, the* jumps of *the filtration* $/G^1(L\,|K)\}_{1\cdot,-1}$ *ofG(L* IK) *are rntional* integers.

Proof: As in the proof of (6.2), we may assume (since $G^1(LIK)$ $G^1(LII.^0)$) that *LIK* is totally ramified and contained in a Lubin-Tate extension L_{111}IK. If *nowt* is a jump of $\{G^1(L\,IK)\}$. then by chap. II (10.9), *t* is also a jump of $\{G^1(Lm\,IK)\}$. Since by (6.1), the jump5 of *{Gv(Lm* IK)) are the number5 *qn* - I. for $n = 0, \ldots, m-1$ (q = 2 is an O is not a jump), the jumps of $\{G^1(L_{,,,}IK)\}$ are the numbers - 1) = *n*, for n = ()_ ,*m* - I. D

The theorem of *HASSE-Aki'* has an important application to *Artin L-series,* which we will study in chap. VII (see chap. Vil, (11.4)).

Chapter VI

Global Class Field Theory

§ 1. Ideles and Idele Classes

The r61c held in local class field theory by the multiplicative group of the base lldd is taken in global class field theory by the idele class group. The notion of idele is a modification of the notion of ideal. It was introduced by the French mathematician *CL,W/J: CHt.\ALIYY* (1909-1984) with a view to providing a suilable basis for the important local-to-global principle, i.e., for the principle which reduces problems concerning a number field K to analogous problems for the various completions K_p. *C@YA111 Y* used the tcnn "ideal clement", which was abbreviated as id. el.

An adele of K - this curious expression, which has the strc,� on the second syllable, is derived from the original term "additive idele" - is a family

$$a = (a_p)$$

of elements $a_p \in K_p$ where p runs lhrough all primes of K, and a_p is integral in K_p for almost all p. The adClcs form a ring, which is denoted by

$$A_K = \prod_p K_p .$$

Addition and multiplication are defined componentwise. This kind of producl is called the "restricted product" of the K_p with respect to the 5ubring� $O_p \subseteq K_p$,

The idele group of K is defined to be the unit group

Thus an idele i� a family

of elements $a_p \in K_p^*$ where is a unit in the ring O_p of integers of K_p, for almost all p. In analogy with we write the ide!e group as the restricted product with respect to the unit groups $\mathcal{O}_\mathfrak{p}^*$. For every finite set of primes S, I_K contains the subgroup

$$I_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}$$

of S-ideles, where $U_\mathfrak{p} = K_\mathfrak{p}^*$ for $\mathfrak{p}$ infinite complex, and $U_\mathfrak{p} = \mathbb{R}_+^*$ for $\mathfrak{p}$ infinite real. One clearly has

$$I_K = \bigcup_S I_K^S,$$

if S varies over all finite sets of primes of K.

The inclusions $K \hookrightarrow K_\mathfrak{p}$ allow us to define the diagonal embedding

$$K^* \longrightarrow I_K,$$

which associates to $a \in K^*$ the idele $a \in I_K$ whose $\mathfrak{p}$-th component is the element a in $K_\mathfrak{p}$. We thus view K^* as a subgroup of I_K and we call the elements of K^* in I_K principal ideles. The intersection

$$K^S = K^* \cap I_K^S$$

consists of the numbers $a \in K^*$ which are units at all primes $\mathfrak{p} \notin S$, $\mathfrak{p} \nmid \infty$, and which are positive in $K_\mathfrak{p} = \mathbb{R}$ for all real infinite places $\mathfrak{p} \notin S$. They are called S-units. In particular, for the set S_∞ of infinite places, K^{S_∞} is the unit group $\mathcal{O}_K^*$ of $\mathcal{O}_K$. We get the following generalization of Dirichlet's unit theorem.

(1.1) Proposition. *If S contains all infinite places, then the homomorphism*

$$\lambda : K^S \longrightarrow \prod_{\mathfrak{p}\in S} \mathbb{R}, \quad a \longmapsto (\log|a|_\mathfrak{p})_{\mathfrak{p}\in S},$$

has kernel $\mu(K)$, and its image is a complete lattice in the $(s-1)$-dimensional trace-zero space $H = \{(x_\mathfrak{p}) \in \prod_{\mathfrak{p}\in S} \mathbb{R} \mid \sum_{\mathfrak{p}\in S} x_\mathfrak{p} = 0\}$, $s = \#S$.

Proof: For the set $S_\infty = \{\mathfrak{p} \mid \infty\}$, this is the claim of chap. I, (7.1) and (7.3). Let $S_f = S \setminus S_\infty$, and let $J(S_f)$ be the subgroup of J_K generated by the prime ideals $\mathfrak{p} \in S_f$. Associating to every $a \in K^S$ the principal ideal $(a) \in J(S_f)$, we obtain the commutative diagram

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mathcal{O}_K^* & \longrightarrow & K^S & \longrightarrow & J(S_f) \\
 & & & & & & \\
0 & \longrightarrow & \prod_{\mathfrak{p}\mid\infty} \mathbb{R} & \longrightarrow & \prod_{\mathfrak{p}\in S} \mathbb{R} & \longrightarrow & \prod_{\mathfrak{p}\in S_f} \mathbb{R}
\end{array}$$

with exact rows. The map λ'' on the right is given by

$$\lambda''\Big(\prod_{\mathfrak p\in S_f}\mathfrak p^{\nu_{\mathfrak p}}\Big)=\prod_{\mathfrak p\in S_f}-\nu_{\mathfrak p}\log\mathfrak N(\mathfrak p)$$

(observe that $|a|_{\mathfrak p}=\mathfrak N(\mathfrak p)^{-v_{\mathfrak p}(a)}$), and maps $J(S_f)$ isomorphically onto the complete lattice spanned by the vectors

$$e_{\mathfrak p}=(0,\dots,0,\log\mathfrak N(\mathfrak p),0,\dots,0),$$

for $\mathfrak p\in S_f$. It follows that $\ker(\lambda)=\ker(\lambda')=\mu(K)$, and we obtain the exact sequence

$$0\longrightarrow \operatorname{im}(\lambda')\longrightarrow \operatorname{im}(\lambda)\xrightarrow{\ i\ }\operatorname{im}(\lambda''),$$

where the groups on the left and on the right are lattices. This implies that the group in the middle is also a lattice. For if $x\in\operatorname{im}(\lambda)$, and U is a neighbourhood of $i(x)$ which contains no other point of $\operatorname{im}(\lambda'')$, then $i^{-1}(U)$ contains the coset $x+\operatorname{im}(\lambda')$, and no other. It is discrete since $\operatorname{im}(\lambda')$ is discrete.

For every $\mathfrak p\in S_f$, if h is the class number of K, then $\mathfrak p^h$ belongs to $i(K^S)$, i.e.,

$$J(S_f)^h\subseteq i(K^S)\subseteq J(S_f).$$

The groups on the left and on the right have rank $\#S_f$, hence so does $i(K^S)$. In the sequence (*), the image of i therefore has rank $\#S_f$, and the kernel has rank $\#S_\infty-1$. Hence $\operatorname{im}(\lambda)$ is a lattice of rank $\#S_f+\#S_\infty-1=\#S-1$. It lies in the $(\#S-1)$-dimensional trace-zero space H, since $\prod_{\mathfrak p\in S}|a|_{\mathfrak p}=\prod_{\mathfrak p}|a|_{\mathfrak p}=1$ for $a\in K^S$. □

(1.2) Definition. *The elements of the subgroup K^* of I_K are called* **principal ideles** *and the quotient group*

$$C_K=I_K/K^*$$

is called the **idele class group** *of K.*

The relation between the ideal class group Cl_K and the idele class group C_K is as follows. There is a surjective homomorphism

$$(\ ):I_K\longrightarrow J_K,\quad \alpha\longmapsto(\alpha)=\prod_{\mathfrak p\nmid\infty}\mathfrak p^{v_{\mathfrak p}(\alpha_{\mathfrak p})},$$

from the idele group I_K to the ideal group J_K. Its kernel is

$$I_K^{S_\infty}=\prod_{\mathfrak p\mid\infty}K_{\mathfrak p}^*\times\prod_{\mathfrak p\nmid\infty}U_{\mathfrak p}.$$

It induces a surjective homomorphism

with kernel $I_K^S K^*/K^*$. We may also consider the surjective homomorphism

$$I_K \to J(\bar{\mathcal{O}}), \quad \alpha \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})},$$

onto the *replete* ideal group $J(\bar{\mathcal{O}})$. Its kernel is

$$I_K^0 = \{ (\alpha_{\mathfrak{p}}) \in I_K \mid |\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = 1 \text{ for all } \mathfrak{p} \}$$

(see chap. III, § 1). It takes principal ideles to replete principal ideals and induces a surjective homomorphism

$$C_K \to Pic(\bar{\mathcal{O}})$$

onto the replete ideal class group, with kernel $I_K^0 K^*/K^*$. We therefore have the

(1.3) Proposition. $Cl_K \cong I_K/I_K^S K^*$, and $Pic(\bar{\mathcal{O}}) \cong I_K/I_K^0 K^*$.

In contrast to the ideal class group, the idele class group is not finite. But the finiteness of the former is reflected in terms of the latter as follows.

(1.4) Proposition. $I_K = I_K^S K^*$, i.e., $C_K = I_K^S K^*/K^*$, if S is a *sufficiently big finite* set of places of K.

Proof: Let $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ be ideals representing the h classes of J_K/P_K. They are composed of a finite number of prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_m$. Now if S is any finite set of places containing these prime, and the places at infinity, then one has $I_K = I_K^S K^*$.

In order to see this, we use the isomorphism $I_K/I_K^\infty \cong J_K$. If $\alpha \in I_K$, then the corresponding ideal $(\alpha) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$ belongs to some class $\mathfrak{a}_i P_K$, i.e., $(\alpha) = \mathfrak{a}_i(a)$ for some principal ideal (a). The idele $\alpha' = \alpha a^{-1}$ is mapped by $I_K \to J_K$ to the ideal $\mathfrak{a}_i = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha'_{\mathfrak{p}})}$. Since the prime ideals occurring in $\mathfrak{a}_i$ lie in S, we have $v_{\mathfrak{p}}(\alpha'_{\mathfrak{p}}) = 0$, i.e., $\alpha'_{\mathfrak{p}} \in U_{\mathfrak{p}}$ for all $\mathfrak{p} \notin S$. Hence $\alpha' = \alpha a^{-1} \in I_K^S$, and thus $\alpha \in I_K^S K^*$. □

The idele group comes equipped with a canonical topology. A basic system of neighbourhoods of $1 \in I_K$ is given by the sets

$$\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}} \subseteq I_K,$$

where S runs through the finite sets of places of K which contain all $\mathfrak{p}|\infty$, and $W_{\mathfrak{p}}$ is a basic system of neighbourhoods of $1 \in K_{\mathfrak{p}}^*$. The groups $U_{\mathfrak{p}}$ are compact for $\mathfrak{p}\nmid\infty$. Therefore the same is true of the group $\prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$. If the $W_{\mathfrak{p}}$, for $\mathfrak{p}|\infty$, are bounded, then $\prod_{\mathfrak{p}|\infty} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$ is a neighbourhood of 1 in I_K whose closure is compact. Therefore I_K is a **locally compact topological group.**

(1.5) Proposition. *K^* is a discrete, and therefore closed, subgroup of I_K.*

Proof: It is enough to show that $1 \in I_K$ has a neighbourhood which contains no other principal idele besides 1.

$$\mathfrak{U} = \{\alpha \in I_K \mid |\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = 1 \text{ for } \mathfrak{p}\nmid\infty,\ |\alpha_{\mathfrak{p}} - 1|_{\mathfrak{p}} < 1 \text{ for } \mathfrak{p}|\infty\}$$

is such a neighbourhood. For if we had a principal idele $x \in \mathfrak{U}$ different from 1, then we get the contradiction

$$1 = \prod_{\mathfrak{p}} |x-1|_{\mathfrak{p}} = \prod_{\mathfrak{p}\nmid\infty} |x-1|_{\mathfrak{p}} \prod_{\mathfrak{p}|\infty} |x-1|_{\mathfrak{p}} < \prod_{\mathfrak{p}\nmid\infty} |x-1|_{\mathfrak{p}} \le \prod_{\mathfrak{p}\nmid\infty} \max\{|x|_{\mathfrak{p}}, 1\} = 1.$$

That the subgroup is closed follows for a completely general reason: since $(\alpha,\beta) \mapsto \alpha\beta^{-1}$ is continuous, there is a neighbourhood $\mathfrak{V}$ of 1 such that $\mathfrak{V}\mathfrak{V}^{-1} \subseteq \mathfrak{U}$. For every $y \in I_K$, the neighbourhood $y\mathfrak{V}$ then contains at most one $x \in K^*$. Indeed, from $x_1 = yv_1$, $x_2 = yv_2 \in K^*$, with $x_1 \neq x_2$, we deduce $x_1x_2^{-1} = v_1v_2^{-1} \in \mathfrak{U}$, a contradiction. □

As K^* is closed in I_K, the fact that I_K is a locally compact Hausdorff topological group carries over to the idele class group $C_K = I_K/K^*$. For any idele $\alpha = (\alpha_{\mathfrak{p}}) \in I_K$, its class in C_K will be denoted by $[\alpha]$. We define the **absolute norm** of α to be the real number

$$\mathfrak{N}(\alpha) = \mathfrak{N}\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}\Big) = \prod_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}}^{-1}.$$

If $x \in K^*$ is a principal idele, then we find by chap. III, (1.3), that $\mathfrak{N}(x) = \prod_{\mathfrak{p}} |x|_{\mathfrak{p}}^{-1} = 1$. We thus have a continuous homomorphism

$$\mathfrak{N}: C_K \longrightarrow$$

It b related to the absolute norm on the replete Picard group *Pie* (0) via lhe commutative diagram

$$C_K \xrightarrow{\mathfrak{N}} \mathbb{R}^*_{+}$$

$$Pic(\bar{\mathcal{O}}) \xrightarrow{\mathfrak{N}} \mathbb{R}^*_{+}$$

Here the arrow

CK------+ Pic(8)

i� induced by the continuous surjective homomorphi<sm

IK------+ ./(O). (ap)i--------+ TTP"pic>pl,
p

with kernel

tZ = | (ap) Eh | lap Ip = I for all p}.

A,; to the kernel *C�* ofl)'t: *CK--+* IR+, we obtain, in analogy with chap. III, (1.14), the following important theorem. It reflects the finiteness of the unit rank of *K* as well as the finitcncs" of the cla�,; number.

(1.6) Theorem. *The group* Ct = {la] *ECK* | IJ1([a]) = I) *is compact.*

Proof: The claim concerning the commutative exact diagram

I ---+ C·i -------+ *CK* ----------;- ------+ I

I → Pic(0)^0 -------+ *Pic(O)* -------+ R: ------+ I

will be reduced to the compactness of the group Pic(8)^0, which wa� proved in chap. III, (1.14). The kernel of the vertical arrow in the middle i� the group *l�K*/K* = tfj!f* n *K**, where we have /� = TIP *1;1*, *1i*^{1} = {a11E *Kp* | = I}, and *If* n *K** = μ(K) by chap.III. (1.9). This kernel is compact. We obtain an exact �equence

I-----+ *tfK*/K**-----+ C¼-----+ *Pic(i5)*^{0}------------+I

of continuom homomorphi5m:-.. Since *Pie* (0)^0 is compact, and the same i� true for the fibres of the mapping ----+ Pic(0)^0 (they arc cosets, all homeomorphic to *tfK*/K�).* hence so ::J

The idele clas5 group *CK* plays a 5imilar r61c for the algebraic number field K as the multiplicative group $K;$ does for a p-adic number field Kp. It comes equipped with a collection of canonical subgroups which are to be viewed as analogues of the higher unit groups *uinJ* = I + pn of a p-adic number field Kp. Instead of pn, we take any integral ideal m = TTP ,.,,_,p""· We may also write it as a replete ideal

with llp = 0 for ploc, and we treat it in what follow5 a� a **module** of K. For every place p of K we put *U�Ol* = Up, and

$$\text{uinpJ} := \begin{cases} 1+\mu''e, & \text{ifpjcc}, \\ \mathrm{IR}: C\ K;, & \text{if p is real}, \\ 1 = K;, & \text{if p is complex}, \end{cases}$$

for np > 0. Given ap $\in$ $K;$ we write

$$\alpha_{\mathfrak p} \equiv 1 \bmod \mathfrak p^{n_{\mathfrak p}} \iff \alpha_{\mathfrak p} \in U_{\mathfrak p}^{(n_{\mathfrak p})}$$

For a finite prime p and np > 0 thi� means the usual congruence; for a real place. it symbolize� positivity. and for a complex place it i� the empty condition.

(I,7) Definition. *The* group

$$C_K^{\mathfrak m} = I_K^{\mathfrak m} K^*/K^*,$$

fonncd from *the idC/c group*

$$tK'=TT_{\mu}\ uinvi,$$

i.� *called the* **congruence subgroup** mod m, *and the quotient* group *CK* ;er; *i� called the* ray class **group** mod m.

Remark: This definition of the ray class group doe� correspond to the classical one, as given (in the ideal-theoretic ver�ion) for instance in Hasse\ ·'Zahlhericht" [53]. It differs from those found in modern textbooks, and also from that given in [I07] by the author: in the present hook, the components ap of ideles *a* in *!JP* are al\\-ays positive at all real places p, so we have here fewer congruence subgroups than in the other text�. Thi� choice does not only �implify maucr�. Mo�t of all, it wa� made �ub�lantially bccau�c of the choice of the canonical metric (,) on the Minkowski :-pace K_1r.. (see chap. I, §5). In fact. we saw in chap. Ill, §3, that thi:- choice force:- the extem.ion ICIIR. to be unramificd. We will explain in § 6 below how tu interpret this situation, and how to reconcile it with the definition of ray classes in other texts.

The significance of the congruence rnbgroup1> lie:- in that they provide an overview over all clo�cd ,;,ubgroup1> of llnite index in *CK.* More precisely, we have the

(1.8) Proposition. *The closed* subgroups of *finite index* of *CK* arc *precisely those subgroups that contain* ;:1 *congruence subgroup CK_.*

Proof: *CK_* i:- open in *CK* because *If,;'* = npuillp) is open in *IK, II('* i� contained in the group *();_'''--* = Tiplcx. *K;* x Tipt-x, *Up,* and since *(CK: !J''"''K*/K*) =#CfK = h* <cc.the index

$$(CK: Cf()= h(li;''-'K�: l'/;'K^*) :S\ h(lt''': l'J.:')$$
$$= h \prod_{pf,-x,} (Up: u;''P^1) \prod_{p'Xl} (K;: U�''v^1)$$

i:- finite. Being the complement of the nontrivial open cosets, which are finite in number, *Cl(* is closed of finite index. Consequently, every group containing is also closed of finite index. for it i5 the union of finitely many co�ets

Conversely, let }/ be an arbitrary closed subgroup of finite index. Then .A/ i� also open. being the complement of a finite number of clo�ed co1>ch. Thu� the preimage *.l* of.Vin *h* is also open. and it thus contains a �ub:-ct of the form

$$W � \prod_{p<c5} wp \times \prod_{piS} U,.$$

where *S* is a finite 5et of places of *K* containing the inlinite one�. and *Wp* i1, an open neighbourhood of I E *K;*. If p E finite, we are liable tu choose *Wp* = u;''P^1, because the group� <;; χ; form a ba�ic system of neighbourhood� of I E *K;.* If p E i5 real, we may choose *Wp* <;; IR.:. The open �ct *WP* will then generate the group IR.:. resp. *K;* in the ca5e of a complex place p. The �ubgroup of *.I* generated by *W* is therefore of the form */I(',* <,o ./1./ contain'> the congruence subgroup C/t [J

The ray cla5s groups can be given the following purely ideal-theoretic dc5cription. Let *Jf(* be the group of all fractional ideals relatively prime tom, and let *Pf(* be the group of all principal ideals (a) E *PK* such that

$$a = 1 \text{ mod m} \quad \text{and} \quad a \text{ totally positive.}$$

The latter condition means thal. for every real embedding *K* � R, *a* tum� out to be positive. The congruence *a* = I mod m means that *a* is the 4uoticnt *h/c* of two *intcw'n,* relatively prime to m such that *h* = (mod m. This i� tantamount to saying that *a* = I mod p"P in *Kp,* i.e., *a* E ui"P^1 for all plm = npt-x,P""· We put

$$Cl_K^{\mathfrak{m}} = J_K^{\mathfrak{m}} / P_K^{\mathfrak{m}}.$$

We then have the

(1.9) Proposition. *The /10momorphi.�m*

(*):IK--------)'JK,* *ctf--------+(a)=* TTP"P(""^{1}-
*

induces an isomorphism

$$C_K / C_K^{\mathfrak{m}} \cong Cl_K^{\mathfrak{m}}$$

Proof: Let m = np p"P' and let

,im) = la Eh I O'p E uillp) forplmoc).

Then *IK* = *l};")K*.* because for every *a* E */K,* by the approximation theorem, there exists an *a* E *K** such that *ctpa* = **1** mod pnp for Pim, and *apa* > 0 for p real. Thus *f3* = *(apa)* E *1km),* so that *a* = *fJa-^{1}* E ***lj;"^{1}****K*.* The element� *a* E !}^{011} n *K** arc precisely those generating principal ideals in *PK,* Therefore the correspondence *a* I-+ *(a)* = npj-x, p^1'μ(t>:μ) defines a surjective homomorphi�m

CK = *!km)K*/K** = *Ii")*//km) n *K*--------)'* *J{(JP{(•*

Since (a) = I for *a* E *If(.* the group('�' = *l;'K*J K** is certainly contained in the kernel. Conver�ely, if the class [al repre�entcd by *a* E *1km)* belongs to the kernel, then there is an *(a)* E *Pf(,* with *a* E !}^{011} n *K*,* such that *(a)* = (a). The componenl� of the idele *fJ* = *cw* -I sati�fy /Jp E *Up* for p 1 moo, and /3p E ut"^{1} for Plmrxi, in other words, *f3* E *1;',* and hence [al= 1,8] E *1;'K*/K"* = *Cl(.* Therefore *Cf!* i� the kernel of the above mapping, and the proposition is proved. D

The ray class groups in the ideal-theoretic version $Cl_K^{\mathfrak m} = J_K^{\mathfrak m}/P_K^{\mathfrak m}$ were introduced by HEINRICH WEBER (1842–1913) as a common generalization of ideal class groups on the one hand, and the groups $(\mathbb Z/m\mathbb Z)^*$ on the other. These latter groups may be viewed as the ray class groups of the field $\mathbb Q$:

(1.10) Proposition. *For any module $\mathfrak m = (m)$ of the field $\mathbb Q$, one has*

$$C_{\mathbb Q}/C_{\mathbb Q}^{\mathfrak m} \cong Cl_{\mathbb Q}^{\mathfrak m} \cong (\mathbb Z/m\mathbb Z)^*.$$

Proof: Every ideal $(a) \in J_{\mathbb Q}^{\mathfrak m}$ has two generators, a and $-a$. Mapping the *positive* generator onto the residue class mod m, we get a surjective homomorphism $J_{\mathbb Q}^{\mathfrak m} \to (\mathbb Z/m\mathbb Z)^*$ whose kernel consists of all ideals (a) which have a positive generator $\equiv 1 \bmod m$. But these are precisely the ideals (a) such that $a \equiv 1 \bmod \mathfrak p^{n_{\mathfrak p}}$ for $\mathfrak p | \mathfrak m\infty$, i.e., the kernel of $P_{\mathbb Q}^{\mathfrak m}$. □

The group is canonically isomorphic to the Galois group $G(\mathbb Q(\mu_m)|\mathbb Q)$ of the m-th cyclotomic field $\mathbb Q(\mu_m)$. We therefore obtain a canonical isomorphism

$$G(\mathbb Q(\mu_m)|\mathbb Q) \cong C_{\mathbb Q}/C_{\mathbb Q}^{\mathfrak m}.$$

It is class field theory, which provides a far-reaching generalization of this important fact. For all modules $\mathfrak m$ of an arbitrary number field K, there will be Galois extensions $K^{\mathfrak m}|K$ generalizing the cyclotomic fields: the so-called ray class fields, which satisfy canonically

$$G(K^{\mathfrak m}|K) \cong C_K/C_K^{\mathfrak m}$$

(see §6). The ray class group mod 1 is of particular interest here. It is related to the ideal class group Cl_K — which according to our definition here, is in general not a ray class group — as follows.

(1.11) Proposition. *There is an exact sequence*

$$1 \longrightarrow \mathcal O^*/\mathcal O^*_+ \longrightarrow \prod_{\mathfrak p \text{ real}} \mathbb R^*/\mathbb R^*_+ \longrightarrow Cl_K^1 \longrightarrow Cl_K \longrightarrow 1,$$

where $\mathcal O^*_+$ is the group of totally positive units of K.

Proof: One has $Cl_K^1 \cong C_K/C_K^1 = I_K/I_K^1 K^*$ and, by (1.3), $Cl_K \cong I_K/I_K^{S_\infty}K^*$, where $I_K^1 = \prod_{\mathfrak p} U_{\mathfrak p}$ and $I_K^{S_\infty} = \prod_{\mathfrak p \nmid \infty} U_{\mathfrak p} \times \prod_{\mathfrak p | \infty} K_{\mathfrak p}^*$. We therefore obtain an exact sequence

$$1 \longrightarrow I_K^{S_\infty}K^*/I_K^1 K^* \longrightarrow C_K/C_K^1 \longrightarrow Cl_K \longrightarrow 1.$$

f-lor lhc group on the left we have the exact !',Cquence

1- !f""nK*/tk nK⁴ - 1;""/tk- t%""K*/tkK* - I.

But ti""- nK* = o*, lk nK* = 0�, and 1Jx'/lk = nPl'X,K;/up = TT,,eo,ll'/ll:. □

Exercise 1. (1) A::i:, = (Z @"J, Qi) x IR.

(1i) The quotient group A::,,/Z is compact and rnnncctcd.

(i11) A::,,/Z i� arb1tranly and uniquely divi•1hle, i.e., the e4uat1on ,u = y has a uni4ue �olul1on, for every n EN and y E A(;/Z.

Exercise 2. Lei K be a number field, m = 2' m' (m' odd), and let S be a fimtc \cl of prime�. Let a EK* and a EK;"', forall p ¢ S. Show:

(i) If K((2, JIK h cyclic. where(,_, i� a primitive 2' -th root of unity. then a EK*"'.

(i1) Olherwi�c one has at least that a E K*"'/2_

Hint: U�e the following fact, proved rn (:UI): if LIK i� a linitc cxtcn�ion in which almo�t all prime ideal� split comple!ely. then L = K.

Exercise 3. Write /J = Ji x 1},_,, with 1/ = npt,,_ U,. I},_,= nplc,. Up. Show that takmg integer power� of 1deles a E: ii' extend� by continuity to exponentiation u' with x E Z.

Exercise 4. Let 1:1, ... ,t·, E o� he independem units. The image� i:1, ...• f, in Ji are then independent units with respect to the exponentiation with clements of Z, i.e., any relation

= 1. r, EZ,

imphe� t, = 0, 1 = I,

1<:xercise 5. Let 1:· E o� be totally po�11ive, i.e.,< E Ii:. Extend the cxponcntiat1on z → !i: II f--,- e", by continuity to an exponentiation Z IR---+ n= Jr' X !},_. 1: f--+ 1,·, m such a way that 91(1:l) = 1

Exercise 6. Let p1•....ph,e the complex prime� of K. For y ER, let ef;1(y) he the idele havint component e2'm at p1, and components I at all other place•. Let ....F1 be a Z-ha�1� ot the group of totally po�llivc units of K.

(i) The 1dele\ of 1he fonn

u=fi' ¢1(}'1)· ¢,()\), ;,, EZ°xlR., y, ElR,

form a group, and have ab�olutc nonn 91(a) = I.

(11) ct I\ a principdl ideal if and only it A.1 E :Z s:;; r_, x IR. ,md y, E Z <;; R.

Exercise 7. Sending

$$(\lambda_1, \dots, \lambda_t, y_1, \quad y_s) \mapsto \varepsilon_1^{\lambda_1} \cdots \varepsilon_t^{\lambda_t} \phi_1(y_1) \cdots \phi_s(y_s)$$

define� a continuou\ homomorphi�m

/ (:f:: x 1Rl x R' -----+ C�

into the group C� = (la) ECK | 91(1111) = 1), with kernel Z^1 x Z'.

Exercise 8. (1) The image *LJ*� of f is compact. connected and arbitrarily divi\ihle
(ii) f yield� a topological isomorph1�m

/ : ((Z x R)/Z)' x CiR/Z)' __:::_,. *[)*�

Exercise 9. The group *[)*�. is the mtcr�1.x:tion of all suhgroups or finite mdcx in ***Cl,*** and it is the connected component of I in

Exercise 10. The connected component *Dx* or l III the 1dclc r.:la\\ *CK* i\ the dm:ct product or *t* cop1e� of the "\olenoid" (Z x *s* circle� and a real hnc.

Exercise 11, Every idectl clas� of the cla..,.., group *Cl*�' can be repre�entcd by an integral idcal which i� prime to an fixed ideal.

Exercise 12. Let ,, = *uK.* Every cla�� in can be represented by a totally po�itive numher in *o* which is prnne 10 an fixed ideal.

Exercise 13. For every module m, one has an cxac1 �equence

I → o:/d.!..'----;. (o/mf----;. *Cl*�'----;. Cl� ..-,. I,

,�here re\p, 1s the group of totally po,.1tive umh of *o,* rc�p. of totally po�1tive = I

Exercise 14. Compute the kemeh of Cit--+ Cl;. and C/�¹ → *C'!t* tor rn'lm

§ 2. ldeles in Field Extensions

We �hall now study the behaviour of idClc'i and idC!c cla..,ses when we pa'>� from a field *K* to an extension *L*. So let LI *K* be a finite extcn..,ion of algebraic number fields. We embed the idele group *IK* of *K* into the idele group *ft.* of *L* by sending an ide!e *a*= (ap) E / *K* to the idele *a'*= (a::pl E *ft* whose components *a:l-l* are given by

a�= *ap* EK;<; L\1 for �lp.

In this way we obtain an injective homomorphi�m

,K--→h.

which will alway� be tacitly used to consider *h* a� a subgroup of *IL*. An element *a* = (aq:;) E *IL* therefore belongs to the group *I K* if and only if its components $a_{\mathfrak{P}}$ belong to $K_{\mathfrak{p}}$ ($\mathfrak{P}|\mathfrak{p}$), and if one has, furthermore $a_{\mathfrak{P}} = a_{\mathfrak{P}'}$, whenever $\mathfrak{P}$ and $\mathfrak{P}'$ lie above the same place $\mathfrak{p}$ of K.

Every isomorphism $\sigma : L \to \sigma L$ induces an isomorphism

$$\sigma : \mathbb{I}_L \longrightarrow \mathbb{I}_{\sigma L}$$

like this. For each place $\mathfrak{P}$ of L, σ induces an isomorphism

$$\sigma: L_{\mathfrak{P}} \to (\sigma L)_{\sigma\mathfrak{P}}.$$

For if we have $a = \mathfrak{P}\text{-}\lim a_i$ for some sequence $a_i \in L$, then the sequence $\sigma a_i \in \sigma L$ converges with respect to $|\;|_{\sigma\mathfrak{P}}$ in $(\sigma L)_{\sigma\mathfrak{P}}$, and the isomorphism is given by

$$a = \mathfrak{P}\text{-}\lim a_i \mapsto \sigma a = \sigma\mathfrak{P}\text{-}\lim \sigma a_i.$$

For an idele $\alpha \in I_L$, we then define $\sigma\alpha \in I_{\sigma L}$ to be the idele with components

$$(\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} \in (\sigma L)_{\sigma\mathfrak{P}}.$$

If $L|K$ is a Galois extension with Galois group $G = G(L|K)$, then every $\sigma \in G$ yields an automorphism $\sigma: I_L \to I_L$, i.e., I_L is turned into a G-module. As to the fixed module $I_L^G = \{\alpha \in I_L \mid \sigma\alpha = \alpha$ for all $\sigma \in G\}$, we have the

(2.1) Proposition. *If $L|K$ is a Galois extension with Galois group G, then*

$$I_L^G = I_K.$$

Proof: Let $\alpha \in I_K \subseteq I_L$. For $\sigma \in G$, the induced map $\sigma: L_{\mathfrak{P}} \to L_{\sigma\mathfrak{P}}$ is a $K_{\mathfrak{p}}$-isomorphism, if $\mathfrak{P}|\mathfrak{p}$. Therefore

$$(\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}} = \alpha_{\sigma\mathfrak{P}},$$

so that $\sigma\alpha = \alpha$, and therefore $\alpha \in I_L^G$. If conversely $\alpha = (\alpha_{\mathfrak{P}}) \in I_L^G$, then

$$(\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} = \alpha_{\sigma\mathfrak{P}}$$

for all $\sigma \in G$. In particular, if σ belongs to the decomposition group $G_{\mathfrak{P}} = G(L_{\mathfrak{P}}|K_{\mathfrak{p}})$, then $\sigma\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}}$, so that $\alpha_{\mathfrak{P}} \in K_{\mathfrak{p}}^*$. If $\sigma \in G$ is arbitrary, then $\sigma: L_{\mathfrak{P}} \to L_{\sigma\mathfrak{P}}$ induces the identity on $K_{\mathfrak{p}}$, and we get $\alpha_{\sigma\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}}$ for any two places $\mathfrak{P}$ and $\sigma\mathfrak{P}$ above $\mathfrak{p}$. This shows that $\alpha \in I_K$. $\square$

The idele group I_L is the unit group of the ring of adeles $\mathbb{A}_L$ of L. It is convenient to write this ring as

where

$$L_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}.$$

The restricted product $\prod_{\mathfrak p} L_{\mathfrak p}$ consists of all families $(\alpha_{\mathfrak p})$ of elements $\alpha_{\mathfrak p} \in L_{\mathfrak p}$ such that $\alpha_{\mathfrak p} \in \mathcal O_{\mathfrak p} = \prod_{\mathfrak P|\mathfrak p} \mathcal O_{\mathfrak P}$ for almost all $\mathfrak p$. Via the diagonal embedding

$$K_{\mathfrak p} \longrightarrow L_{\mathfrak p},$$

the factor $L_{\mathfrak p}$ is a commutative $K_{\mathfrak p}$-algebra of degree $\sum_{\mathfrak P|\mathfrak p}[L_{\mathfrak P}:K_{\mathfrak p}] = [L:K]$. These embeddings yield the embedding

$$\mathbb A_K \longrightarrow \mathbb A_L,$$

whose restriction

$$I_K = \mathbb A_K^* \hookrightarrow \mathbb A_L^* = I_L$$

turns out to be the inclusion considered above.

Every $\alpha_{\mathfrak p} \in L_{\mathfrak p}^*$ defines an automorphism

$$\alpha_{\mathfrak p}: L_{\mathfrak p} \longrightarrow L_{\mathfrak p}, \quad x \mapsto \alpha_{\mathfrak p} x,$$

of the $K_{\mathfrak p}$-vector space $L_{\mathfrak p}$, and as in the case of a field extension, we define the norm of $\alpha_{\mathfrak p}$ by

$$N_{L_{\mathfrak p}|K_{\mathfrak p}}(\alpha_{\mathfrak p}) = \det(\alpha_{\mathfrak p}).$$

In this way we obtain a homomorphism

$$N_{L_{\mathfrak p}|K_{\mathfrak p}}: L_{\mathfrak p}^* \longrightarrow K_{\mathfrak p}^*.$$

It induces a norm homomorphism

$$N_{L|K}: I_L \longrightarrow I_K$$

between the idele groups $I_L = \prod_{\mathfrak p} L_{\mathfrak p}^*$ and $I_K = \prod_{\mathfrak p} K_{\mathfrak p}^*$. Explicitly the norm of an idele is given by the following proposition.

(2.2) **Proposition.** *If $L|K$ is a finite extension and $\alpha = (\alpha_{\mathfrak P}) \in I_L$, the local components of the idele $N_{L|K}(\alpha)$ are given by*

$$N_{L|K}(\alpha)_{\mathfrak p} = \prod_{\mathfrak P|\mathfrak p} N_{L_{\mathfrak P}|K_{\mathfrak p}}(\alpha_{\mathfrak P}).$$

Proof: Putting $\alpha_{\mathfrak p} = (\alpha_{\mathfrak P})_{\mathfrak P|\mathfrak p} \in L_{\mathfrak p}$, the $K_{\mathfrak p}$-automorphism $\alpha_{\mathfrak p}: L_{\mathfrak p} \to L_{\mathfrak p}$ is the direct product of the $K_{\mathfrak p}$-automorphisms $\alpha_{\mathfrak P}: L_{\mathfrak P} \to L_{\mathfrak P}$. Therefore

$$N_{L_{\mathfrak p}|K_{\mathfrak p}}(\alpha_{\mathfrak p}) = \det(\alpha_{\mathfrak p}) = \prod_{\mathfrak P|\mathfrak p} \det(\alpha_{\mathfrak P}) = \prod_{\mathfrak P|\mathfrak p} N_{L_{\mathfrak P}|K_{\mathfrak p}}(\alpha_{\mathfrak P}). \qquad \square$$

The idele norm enjoys the following properties.

(2.3) Proposition. (i) *For a tower of fields $K \subseteq L \subseteq M$ we have $N_{M|K} = N_{L|K} \circ N_{M|L}$.*

(ii) *If $L|K$ is embedded into the Galois extension $M|K$ and if $G = G(M|K)$ and $H = G(M|L)$, then one has for $\alpha \in I_L$: $N_{L|K}(\alpha) = \prod_{\sigma \in G/H} \sigma\alpha$.*

(iii) *$N_{L|K}(\alpha) = \alpha^{[L:K]}$ for $\alpha \in I_K$.*

(iv) *The norm of the principal idèle $x \in L^*$ is the principal idèle of K defined by the usual norm $N_{L|K}(x)$.*

The proofs of (i), (ii), (iii) are literally the same as for the norm in a field extension (see chap. I, §2), (iv) follows from the fact that, once we identify $L_\mathfrak{p} = L \otimes_K K_\mathfrak{p}$ (see chap. II, (8.3)), the $K_\mathfrak{p}$-automorphism $f_{x_\mathfrak{p}} : L_\mathfrak{p} \to L_\mathfrak{p}$, $y \mapsto xy$ arises from the K-automorphism $f_x : L \to L$ by tensoring with $K_\mathfrak{p}$. Hence $N_{L|K}(x) = \det(f_x)$.

Remark: For fundamental as well as practical reasons, it is convenient to adopt a formal point of view for the above considerations which allows us to avoid the constant back and forth between idèles and their components. This point of view is based on identifying the ring of adèles $\mathbb{A}_L$ of L as

$$\mathbb{A}_L = \mathbb{A}_K \otimes_K L$$

which results from the canonical isomorphisms (see chap. II, (8.3))

$$K_\mathfrak{p} \otimes_K L \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}, \quad a \otimes \alpha \longmapsto \prod a(\tau_\mathfrak{P}\alpha).$$

Here $\tau_\mathfrak{P}$ denotes the canonical embedding $\tau_\mathfrak{P} : L \to L_\mathfrak{P}$.

In this interpretation the inclusion by components $\mathbb{A}_K \subseteq \mathbb{A}_L$ is simply given by the embedding $\mathbb{A}_K \to \mathbb{A}_L$, $a \mapsto a \otimes 1$, induced by $K \subseteq L$. An isomorphism $\sigma : L \to \sigma L$ then yields the isomorphism

$$\sigma : \mathbb{A}_L = \mathbb{A}_K \otimes_K L \longrightarrow \mathbb{A}_K \otimes_K \sigma L = \mathbb{A}_{\sigma L}$$

via $\sigma(a \otimes \alpha) = a \otimes \sigma\alpha$, and the norm of an L-idèle $\alpha \in I_L$ is simply the determinant

$$N_{L|K}(\alpha) = \det_{\mathbb{A}_K}(\alpha)$$

of the endomorphism $\alpha : \mathbb{A}_L \to \mathbb{A}_L$ which α induces on the finite $\mathbb{A}_K$-algebra $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$.

Here are consequences of the preceding investigations for the **idèle** class **groups.**

(2.4) Proposition. *If $L|K$ is a finite extension, then the homomorphism $I_K \to I_L$ induces an injection of idele class groups*

$$C_K \to C_L, \quad \alpha K^* \mapsto \alpha L^*.$$

Proof: The injection $I_K \to I_L$ clearly maps K^* into L^*. For the injectivity, we have to show that $I_K \cap L^* = K^*$. Let $M|K$ be a finite Galois extension with Galois group G containing L. Then we have $I_K \subseteq I_L \subseteq I_M$ and

$$I_K \cap L^* \subseteq I_K \cap M^* \subseteq (I_M \cap M^*)^G = I_K \cap M^{*G} = I_K \cap K^* = K^*. \quad \square$$

Via the embedding $C_K \to C_L$, the idele class group C_K becomes a subgroup of C_L: an element $\alpha L^* \in C_L$ ($\alpha \in I_L$) lies in C_K if and only if the class αL^* has a representative α' in I_K. It is important to know that we have **Galois descent** for the idele class group:

(2.5) Proposition. *If $L|K$ is a Galois extension and $G = G(L|K)$, then C_L is canonically a G-module and $C_L^G = C_K$.*

Proof: The G-module I_L contains L^* as a G-submodule. Hence every $\sigma \in G$ induces an automorphism

$$C_L \to C_L, \quad \alpha L^* \mapsto (\sigma\alpha)L^*.$$

This gives us an exact sequence of G-modules

$$1 \to L^* \to I_L \to C_L \to 1.$$

We claim that the sequence

$$1 \to L^{*G} \to I_L^G \to C_L^G \to 1$$

deduced from the first is still exact. The injectivity of $L^{*G} \to I_L^G$ is trivial. The kernel of $I_L^G \to C_L^G$ is $I_L^G \cap L^* = I_K \cap L^* = K^* = L^{*G}$. The surjectivity of $I_L^G \to C_L^G$ is not altogether straightforward. To prove it, let $\alpha L^* \in C_L^G$. For every $\sigma \in G$, one then has $\sigma(\alpha L^*) = \alpha L^*$, i.e., $\sigma\alpha = \alpha x_\sigma$ for some $x_\sigma \in L^*$. This x_σ is a "crossed homomorphism", i.e., we have

$$x_{\sigma\tau} = x_\sigma \cdot \sigma x_\tau.$$

Indeed, $x_{\sigma\tau} = \frac{\sigma\tau\alpha}{\alpha} = \frac{\sigma\alpha}{\alpha}\,\sigma\left(\frac{\tau\alpha}{\alpha}\right) = x_\sigma\,\sigma x_\tau$. By Hilbert 90 in Noether's version (see chap. IV, (3.8)), such a crossed homomorphism is of the form $x_\sigma = \sigma y/y$ for some $y \in L^*$. Putting $\alpha' = \alpha y^{-1}$ yields $\alpha' L^* = \alpha L^*$ and $\sigma\alpha' = \sigma\alpha\,\sigma y^{-1} = \alpha x_\sigma\,\sigma y^{-1} = \alpha y^{-1} = \alpha'$, hence $\alpha' \in I_L^G$. This proves surjectivity.

The norm map *Ni* IK : *h* _,. *IK* sends principal idele� lo principal ideb by (2.3). Hence we get a norm map also for the idclc cla'>� group *CL,*

NLIK : *CL*-----+ *CK.*

It enjoys the same properties (2.3), (i), (ii). (iii), a� the norm map on the ide!e group.

Exercise I, Let w_1. be a ba�1s of Then the 1�omorphi\m *I,tFhKμ;;,* n'J'.llPLp for almo�t all prime p of *K,* an i\omorphi\m

l01(Jpffi ··EBw,,np � $\prod$ 0,:i.,,

'VP

where op, resp. O\Jl, i� the valuation ring of KP· re�p. L_{73}.

Exercise 2. Let LI *K* he a finite exten\ion. The ab�olutc norm '.Tl of idele\ of *K,* resp.!,, hehave\ a\ follows under the inelu�ion $i_{1|}$K *!K* ---,. *l1.* re\p. under the nom1 N1.1K: *li,-,.!;,-:*

'.'11(11.1K(a)) = '.Tl(a)$^{|}$L Kl for *a* E *IK,*

'.Tl(N11do-)) = '.Tl(a) for *a* E */i.*

Exercise 3. The corre�pondem:c between idClc� and ideal�. *a* f---l- (a), \ati\fie� the follov.ing rule. in the Ca\c of a Galoi� cxtcn�mn *LIK,*

(N1.:K(a)) = *N1 K·((a)).*

(For the norm on ideals.. \ee chap. III, §1.)

Exercise 4. unlike the idClc class group, doe\ not have (ialo1� a Galoi� extensmn *l.* I*K,* the homomorphism *CIK*---,. i\ in general neither inJcctivc nor suqect1ve

Exercise 5. Define the trace $Tr_{L|K} : \mathbb{A}_L \to \mathbb{A}_K$ hy *Tr1,K(LY)* = trace or the endomorphi�m *A* f---l- *a,1* of the $\mathbb{A}_K$-algebra $\mathbb{A}_L$, and �how:

(i) *Tr1.1K(a)p* = L\JllP Tr1,,,1Kp(a,:p).

(ii) Fora tov.er of field� *K* <;::: *L* ,;; *M,* one ha¾ Trw_{1K} = "fr1. A" *"1)-M* 1.

(iii) If *LIK* is emhedded into the Gal01s cxtcn�ion and if G = *G(MIK)* and *H* = G{MIL). then one ha� for *a* E A1, *Tr1 da)* =

(iv)"fr11da)=IL:K]LY foraEAK.

(v) The trace of a principal adCle _\ E *L* I\ the principal addc in *A.K* dctincd hy the usual trace $Tr_{L|K}(x)$.

§ 3. The Herbrand Quotient of the ldele Class Group

Our goal now is to show that the idClc cla�s group !-.atisties the etas� field axiom of chap. IV, (6.1). To do thi� we v.ill llN compute its Herbrand quotient ll is constituted on the one hand by the Herbrand quotient of the idClc group, and by that of the unit group on the other. We study the idele group first.

Let LI K be a finite Galois extension with Galois group C. The G-module h may be described in the following simple manner, which immediately reduces us to local field:,. For every place p of K we put

$$L;= \underset{',J\}lp}{nL\$} \quad \text{and} \quad UL\_p= \underset{'Pip}{nu13.}$$

Since the automorphisms a E G permute the place� of L above p, the groups L� and $VL.p$ are G-modules, and we have for the G-modulc h the decomposition

$$h \quad �IJL;, \\ p$$

where the restricted product is taken with re:,pcct *to* the �ubgroups $U_{1.}$ p � $L;$. Choose a place ¹,P of L above p. and let G-i₁ = *G(L,vlKp)* � G be its decomposition group. As a varic<; over a system of representatives of *GjG,;,₃, aqJ* runs through the various places of Labove p, and we get

$$L; = i{:}iL�'+l = ga(L\$), \quad UL.p = gu'''+l = ga(U,-JJ).$$

In terms of the notion of *indur ed module* introduced in chap. IV *, 7, we thu:, get the following

(3.1) Proposition. /,; and *Ut.. p* are *the induced* G-modu/es

$$L� = \text{Ind}�;\text{-v}(l.\$), \quad U_1,p = \text{Ind}�/(U,:p).$$

Now let S be a finite :,ct of places of K containing the infinite places. We then define *I{= 1},* ½here S denotes the set of all place:, of L which lie above the place� of *S*. For *Jl_'* we have the G-module decompo:,ition

$$if= \prod_{pd} L; \times \prod_{piS} UL.p,$$

and (3.1) give,:, the

(3.2) **Proposition.** *If* LI K is ,1 *cyclic extemion, and* if S contains a// *prime:,* rnmified *in L, then we* /Jave for i = 0, - I *th:.it*

$$H'(G,I\}) � \underset{p<c.',}{ffiH^1(G,;13.L'.ii)} \quad and \quad H^1(G,l1.) � \underset{p}{ffi//'(G,:p,/,;\_,).}$$

where for *each* p, 1} is a *chosen* prime of *L a/Jove* p.

Proof: The decomposition *lf=* <EBp<c.\ *L;)* ffi *V.* *V* = np\i"S *u,*.p, gives m, an i:-.omorphism

ll¹(G,l}) = ffi *llli(G,L;)* ffi *H'(C.* V),
pE:S

and an injeclion *H'(G,* V) → np,t'i" *H'(G,* UL.p). By ('.U) and chap. IV, (7.4), we have the isomorphisms *H¹(C,L;)* ::::::; H'(C,-.p.L;_1) and *H'(G.lh.p)* ::::::; /-l'(G'J.l,U,+1). For p *<t S,* L'J.llKp is unramified. Hence *H'(C,v,ll;;p)* = I, by chap.V, (1.2). This shows the llr�t claim of the proposition. The second is an immediate consequence:

Hi(C,ft.)= � *H'(C.lfJ* - � ffiH'(Gq:i,L;p)=ffiH'(G'J.l,Lii),
"i" *S* *pcS* P

□

The proposition says that one has //-¹(G,*IL)*= /I}, because */-l* ¹(Gti, L1J) = {I} by Hilbert 90. Further it says that

$$IK/NL!Kh = \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}} L_{\mathfrak{P}}^*$$

where ,:P is a chosen place above p. In other words:

An idele *a* E *IK* b a norm of an idC!e of *L* if and only if it is *u norm everywhere,* i.e.. if every component ap is the nonn of an element

As for the Herbrand quotient *h(G, ii)* we obtain the rc�ult:

(3.J) **Propo�ition.** *If* LI *K h, a cyclic extension and* if *S contains all* rnmified *primes, then*

h(G,lj�) = ∩ *np,*
p<cS

where llp = /Lti: Kpl-

Proof: We have 1-1-¹(G, *ii)* = npES 1-1-¹(G,v,Lii) = I and

H⁰(G,if)= ∩ H⁰(G,v,ClJ).
pd"

By local cla�s field theory. we find #/-1°(G'J.l, L;) = *(K;* : *NL,JJIK,,L�)* = *np.* Hence

$$h(G, I_L^S) = \frac{\#H^0(G, I_L^S)}{\#H^{-1}(G, I_L^S)} = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}.$$

[J

Next we determine the Hcrbrand quotient of the G-module *Ls=* *L* n *12',* For this we need the following general

(3.4) Lemma. *Let \I he an s -dimen.�ional �-vector .�p.:1ce,* and *let G be a finite group* of automorphism� of\/ *which* operates *as* a permutation *group on the* clement.� of a *basi�* v_1. *. v.,: ov,* =

I[I' is :I *G -invariant complele lattice* in \/, *a r* S; *r* for all *a, then /here exists* a *complete sublatticc in I',*

$$r'=Z:w_1 + \quad -+Z:w,,$$

such tlwtaw, = w,,.(,I *fora/la* E G.

Proof: Lel I I be the sup-nom1 with respect to the coordinates of lhe basis v1, ... , *v., ·•* Since *I'* is a lattice, there exists a number *h* such that for every *x* E *\I,* there is a *y* E *r* satisfying

$$|x-y| < h.$$

Choose a large positive number *t* ER, and a *y* E *r* such that

$$|tv1 - y| < h,$$

and define

$$w,= \sum_{,-,.(I|=i} ay, \quad i=l,$$

i.e., the wmmation is over all *a* E *G* wch that a(I) = i. For every r E *G* \\-'e then have

$$TW1 = \sum_{a(I)=I} ray= \sum_{p(I)--r(1)} PY=w_{r(,)}.$$

It i), therefore enough to check the linear independence of thew,. To do this, let

$$\sum_{1=1} c,w,=0, \quad c;EIR.$$

If not all of the *c,* = 0, then we may assume |e,I :Sc I and c_1 = I for some *j.* Let

$$y = tv1 -y,$$

for some vector *y* of absolule value |*y*| < *h.* Then

$$IL',= \quad ay = t \quad v_{\sigma(1)} - y_i = tn_i v_i - y_i .$$

where IY,I .:S *gh,* for *R* = #G, and *n,* = #[a E GI a(I) = i}. We therefore get

$$0 = \sum_{I=I} c,w, = l \sum_{1=1} c,n,v, - z.$$

with |zI .:S *sih,* i.e.,

$$z=tn_1vJ+\sum_{i-f1} tc,n,v,.$$

If *t* was chosen �ufllciently large, then : cannot be written in thi), way. This contradiction proves the lemma. $\square$

Now let LI K be a cyclic extemion of degree II with Galois group $G = G(LIK)$, let 5 be a finite set of place? containing the infinite places, and let S be lhe set of places of L that lie above the places of S. We denote the group L.? of.?-units 5imply by L^5.

(3.5) **Proposition,** *The* Herbnmd *qt1otienl* of *the G -module L"" sati8fies*

$$h(G,I,?) = \_!\_TI \; !Ip, \quad n \; pc\backslash$$

wheren$_{11}$= [L'+l: K$_{11}$1.

Proof: Lel {c,,p | 'l} E SJ be the standard basis of the vector space V = fl'+Jc? IR. By (1.1), the homomorphism

$$A: L^8 \longrightarrow V, \quad A(a) = L\_ \log |al'+lc,p,$$

ha? kernel $\mu(L)$ and its image is an (.I' - I)-dimensional lattice. .S =#I.We make G operate on V via

$$ac,:p = c,-,-,:\mu.$$

Then A i? a G-homomorphism because we have, for a E G.

$$A(au) = L_{\mathfrak{P}} \log |aaj'-+lc,;p = L_{\mathfrak{P}} \log |ala\ 1'+\_1ac,,.\ 1,,p$$

$$= a(Llog\ |al,,.\ 1,.pC,-,--1'+l) = aA(a).$$

Therefore $e_0 = \sum_{\mathfrak{P}\in\bar{S}} e_{\mathfrak{P}}$ and A(Ls) generate a G-invariant complete lactice$r$ in \'. Since $\mathbb{Z}e_0$ is G-isomorphic lo Z, the exact sequence

$$0 \longrightarrow 7\text{-}c_0 \longrightarrow r \longrightarrow I'/Zc_0 \longrightarrow 0,$$

together with the fact that $I'/Zc_0 = A(L^5)$, yield5 the identities

$$h(G, Ls)= h(G.),(L'')) = h(G. Z:)^{-1}/z(G, I')= f\ /,(G, I').$$

We now choose in I' a sublattice r', in accordance with lemma (3.4). Then we have

$$I''= \bigoplus_{'+I} Zw'+I = \bigoplus_{pcS'I\text{-}IIP} \bigoplus Zw'+I = \bigoplus_{P'=S} r?$$

and $aw'+\text{-}1 = w,\text{-},\text{-}':JJ\cdot$ This idenlilie? $r;$ as the induced G-module

$$r; = \quad = \bigoplus_{oEG/(,'p} a(7::w'+\backslash i) = \operatorname{Ind}??(Zw'+Jo)\cdot$$

where $\mathfrak{P}$ is a chosen place above $\mathfrak{p}$, and $G_{\mathfrak{P}}$ is its decomposition group. The lattice Γ' has the same rank as Γ, so is therefore of finite index in Γ. From chap. IV, (7.4), we conclude that

$$h(G, L^S) = \frac{1}{n} h(G, \Gamma') = \frac{1}{n} \prod_{\mathfrak{p} \in S} h(G, \Gamma_{\mathfrak{p}}) = \frac{1}{n} \prod_{\mathfrak{p} \in S} h(G_{\mathfrak{P}}, \mathbb{Z} w_{\mathfrak{P}})$$
$$= \frac{1}{n} \prod_{\mathfrak{p} \in S} h(G_{\mathfrak{P}}, \mathbb{Z}).$$

Thus we do find that $h(G, L^S) = \frac{1}{n} \prod_{\mathfrak{p} \in S} n_{\mathfrak{p}}$, where $n_{\mathfrak{p}} = \# G_{\mathfrak{P}} = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. □

From the Herbrand quotient of I_L^S and L^S we immediately get the Herbrand quotient of the idele class group C_L. To do it choose a finite set of places S containing all infinite ones and all primes ramified in L, such that $I_L = I_L^S L^*$. Such a set exists by (1.4). From the exact sequence

$$1 \longrightarrow L^S \longrightarrow I_L^S \longrightarrow I_L^S L^*/L^* \longrightarrow 1$$

arises the identity

$$h(G, C_L) = h(G, I_L^S)\, h(G, L^S)^{-1}$$

and from (3.3) and (3.5) we obtain the

(3.6) Theorem. *If $L|K$ is a cyclic extension of degree n with Galois group $G = G(L|K)$, then*

$$h(G, C_L) = \frac{\# H^0(G, C_L)}{\# H^{-1}(G, C_L)} = n.$$

In particular $(C_K : N_{L|K} C_L) \geq n$.

From this result we deduce the following interesting consequence.

(3.7) Corollary. *If $L|K$ is cyclic of prime power degree $n = p^{\nu}$ ($\nu > 0$), then there are infinitely many places of K which do not split in L.*

Proof: Assume that the set S of nonsplit primes were finite. Let $M|K$ be the subextension of $L|K$ of degree p. For every $\mathfrak{p} \notin S$, the decomposition group $G_{\mathfrak{p}}$ of $L|K$ is different from $G(L|K)$. Hence $G_{\mathfrak{p}} \subseteq G(L|M)$. Therefore every $\mathfrak{p} \notin S$ splits completely in M. We deduce from this that $N_{M|K} C_M = C_K$, thus, contradicting (3.6).

Indeed, let a E /K. By the approximation theorem of chap. II, (3.4). there exi�ts an a E K^* such that is contained in the open subgroup $N_{M_{\mathfrak{P}}|K_{\mathfrak{p}}}M_{\mathfrak{P}}^*$, for all p E S. If p ,f_ then $a_{11}a^{-1}$ is automatically contained in $N_{M_{\mathfrak{P}}|K_{\mathfrak{p}}}M_{\mathfrak{P}}^*$ because $M<:p = K$p. Since

$$I_K/N_{M|K}I_M = \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/N_{M_{\mathfrak{P}}|K_{\mathfrak{p}}}M_{\mathfrak{P}}^*$$

the idele IHI-^{1} is a nonn of some idele fl of IM, i.e., a= (NMwfl)a E NMIK/lvfK*. This shows that the class of a belongs to NM,KC1vt, so that CK= NM1KC'Af. □

(3.8) Corollary. *Let LIK be* a *finite extension* of *algebraic nwnber fields. 1f* almost all *primes* of K split *completely* in L, *then* $L = K$.

Proof: We may a&sumc without loss of generality that LI K b. Galois. In fact, let MIK be the nonnal clo:;.ure of LIK, and write G = G(MIK) and H = G(MIL). Also]cl p be a place of K, q3 a place of M above p, and let Ci-:µ be it� decomposition group. Then the number of places of L above p equals the number #$H\backslash G$ /G'J3 of double cosets Ha Ge;µ in G (�ee chap. I, *9). Hence p �plit� completely in L if #$H\backslash G$ /G'J3 = [L : K J = #$H\backslash G$. But this is tantamount to = I, and hence to the fact that p splits completely in M.

So w,umc LIK Galoi<,, L #- K, and let a E G(LIK) be an clement of prime order, with fixed Held K'. If almo&t all prime� p of K were completely split in L, then the <,amc would hold for the primes p' of K'. Tiiis comrndict& (3.7). □

Exerci:;.e 1. If the Galoi� cxtcmion LI K is not cyclic. then there arc at most finitely many prime� of K which do not \plit m /..

1<:xercise 2, If /,IK i\ a finite Galoi\ then the Cialois group G(LIK) 1� generated by the Frobcniu� automorphi�m� if"l-1 prime idcab ,P of L which arc unramitied over K.

Exercise 3. Let be a finite abelian exten�ion, and let D be d subgroup of I;. �uch that Kx/J is in/Kand D s::; $N_{1\_1}KL'$. Then $L = K$.

Exercise 4. Let ....L,I K he cyclic extension� of prime degree p such that L,nL, =K for1 Then there arc infinitely prime� p or K whJCh \p!it completely in L_1, _.,. 1, hut which are non�plit m

§ 4. The Class Field Axiom

Having determined the Herbrand quotient *h(G,CL)* to be the degree 11 = [L: Kl of the cyclic extension *LIK*, it will now be enough to show either H-¹(G,CL) = I or H⁰(G.CL) = *(CK : NLIKCL)* = 11. The first identity is curiously inaccessible by ½ay of direct attack. We are thus stuck with the <,econd. We will reduce the problem to the case of a *Kumrne1 cxtemion.* For such an extension the norm group NL_1KCL can be written do'.¼n explicitly, and this allows us to compute lhe index $(CK : NL_1KCL)$.

So let *K* be a number field that contain;, the 11-th roots of unity, where *n* is a fixed *prime pmrer,* and let Ll *K* be a Galois extension with a Galois group of the forrn

G(l,IKJ "' (Z/nZ)',

We choose a finite set of places *S* containing the ramified place'>, tho;,e that divide *n,* and the infinite ones, and which is wch that / *κ* = *I J:: K* •. We ½rite again *Ks= Ii:* n *K** for the group of S-units. and we puts= *#S.*

(4.1) Proposition. One *has* 1 ?. *r,* and *there exist.� a* set *T* of *s - r primes* of *K that* do *not he/ong to S such that*

$$L = K(\sqrt[n]{\Delta}),$$

where L1 *is the J...cmc/ 0{1hc map Ks----+* npcT *K�/K;".*

Proof: We show first that *L* = K(n) if L1 = f,*"nKs,and then that L1 is the ;,aid kernel, By chap, IV, (3.6), we certainly have that *L* = *K* (':JD), with *D* = *L*"nK.* lfx E /J. then Kp(,v't)IKp isunramifiedforall p *(j. S* because *S* contains the ramified in *L.* By chap. V, (3.3), we may therefore write *x* = with 11µ EUµ. Yµ EK;. Putting Jp = I for p ES. we get an idele *y* = (yµ) which can be written as a product _r = a: with *a* EI{, *z* EK*. Then *x:::-/1* � llpO'� E Up for all p *(j_ S,* i.e., .t: 11 E ,ℤ ,*f*� = *K⁵,* ;,o that *xz-¹¹* E Ll. Thi;, �how<, that *fJ* = *L1K*",* and thu� *L* = *K(n*).

The field *N* = *K*(W) contaim the field t because L1 = *L*,,* n *K·*� <; *K·".* By Kummer theory. chap, IV, (3.6), we have

G(NIK) � *Hom(Ks/(Ks)'1,Z/11Z)*

Hy (I.I), *Ks* is the product of a free group of rank .1 - 1 and of the cyclic group *11(K)* whose order is d1vi;,ibk by *n.* Therefore *Ks/(Ks)"* is a free $(\mathbb{Z}/n\mathbb{Z})$-module of rank s, and so is $G(N|K)$. Moreover, $G(N|K)/G(N|L) \cong G(L|K) \cong (\mathbb{Z}/n\mathbb{Z})^r$ is a free $(\mathbb{Z}/n\mathbb{Z})$-module of rank r so that $r \le s$, and $G(N|L)$ is a free $(\mathbb{Z}/n\mathbb{Z})$-module of rank $s-r$. Let $\sigma_1, \dots, \sigma_{s-r}$ be a basis of $G(N|L)$, and let N_i be the fixed field of σ_i, $i = 1, \dots, s-r$. Then $L = \bigcap_{i=1}^{s-r} N_i$. For every $i = 1, \dots, s-r$ we choose a prime $\mathfrak{P}_i$ of N_i which is nonsplit in N such that the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_{s-r}$ of K lying below $\mathfrak{P}_1, \dots, \mathfrak{P}_{s-r}$ are all distinct and do not belong to S. This is possible by (3.7). We now show that the set $T = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{s-r}\}$ realizes the group $\Delta = L^{*n} \cap K^S$ as the kernel of $K^S \to \prod_{\mathfrak{p}\in T} K_\mathfrak{p}^*/K_\mathfrak{p}^{*n}$.

N_i is the decomposition field of $N|K$ at the unique prime $\mathfrak{P}_i'$ above $\mathfrak{P}_i$, for $i = 1, \dots, s-r$. Indeed, this decomposition field Z_i is contained in N_i because $\mathfrak{P}_i$ is nonsplit in N. On the other hand, the prime $\mathfrak{p}_i$ is unramified in N, because by chap. V, (3.3), it is unramified in every extension $K(\sqrt[n]{u})|K$, $u \in K^S$. The decomposition group $G(N|Z_i) \supseteq G(N|N_i)$ is therefore cyclic, and necessarily of order n since each element of $G(N|K)$ has order dividing n. This shows that $N_i = Z_i$.

From $L = \bigcap_{i=1}^{s-r} N_i$ it follows that $L|K$ is the maximal subextension of $N|K$ in which the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_{s-r}$ split completely. For $x \in K^S$ we therefore have

$$x \in \Delta \iff K(\sqrt[n]{x}) \subseteq L \iff K_{\mathfrak{p}_i}(\sqrt[n]{x}) = K_{\mathfrak{p}_i},\ i = 1, \dots, s-r,$$
$$\iff x \in K_{\mathfrak{p}_i}^{*n},\ i = 1, \dots, s-r.$$

This shows that Δ is the kernel of the map $K^S \to \prod_{\mathfrak{p}\in T} K_\mathfrak{p}^*/K_\mathfrak{p}^{*n}$. $\square$

(4.2) Theorem. *Let T be a set of places as in* (4.1), *and let*

$$C_K(S,T) = I_K(S,T)K^*/K^*,$$

$$I_K(S,T) = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^{*n} \times \prod_{\mathfrak{p}\in T} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p}.$$

Then one has

$$N_{L|K} C_L \supseteq C_K(S,T) \quad \text{and} \quad \big(C_K : C_K(S,T)\big) = [L:K].$$

In particular, if $L|K$ is cyclic, then $N_{L|K}C_L = C_K(S,T)$.

Remark: It will follow from (5.5) that $N_{L|K}C_L = C_K(S,T)$ also holds in general.

For the proof of the theorem we need the following

(4.3) Lemma. $I_K(S,T)\cap K^* = (K^{S\cup T})^n$.

Proof: The inclusion $(K^{S\cup T})^n\subseteq I_K(S,T)\cap K^*$ is trivial. Let $y\in I_K(S,T)\cap K^*$, and $M=K(\sqrt[n]{y})$. It suffices to show that $C_K = N_{M|K}C_M$, for then (3.6) implies $M=K$, hence $y\in K^{*n}\cap I_K(S,T)\subseteq (K^{S\cup T})^n$. Let $[\alpha]\in C_K = I_K/K^*$, and let $\alpha\in I_K$ be a representative of the class $[\alpha]$. The map

$$K^S\longrightarrow \prod_{\mathfrak p\in T} U_{\mathfrak p}/U_{\mathfrak p}^n$$

is surjective. For if Δ denotes its kernel, then obviously $K^{*n}\cap\Delta = (K^S)^n$, and $\Delta K^{*n}/K^{*n} = \Delta/(K^S)^n$. From (1.1) and Kummer theory, we therefore get

$$\#(K^S/\Delta) = \frac{\#K^S/(K^S)^n}{\#\Delta/(K^S)^n} = \frac{n^s}{\#G(L|K)} = n^{s-r}.$$

This is also the order of the product because by chap. II, (5.8), we have $\#U_{\mathfrak p}/U_{\mathfrak p}^n = n$ since $\mathfrak p\nmid n$. We thus find an element $x\in K^S$ such that $\alpha_{\mathfrak p} = xu_{\mathfrak p}^n$, $u_{\mathfrak p}\in U_{\mathfrak p}$, for $\mathfrak p\in T$. The idele $\alpha' = \alpha x^{-1}$ belongs to the same class as α, and we show that $\alpha'\in N_{M|K}I_M$. By (3.2), this amounts to checking that every component $\alpha'_{\mathfrak p}$ is a norm from $M_{\mathfrak P}|K_{\mathfrak p}$. For $\mathfrak p\in S$ this holds because $y\in K_{\mathfrak p}^{*n}$. Hence we have $M_{\mathfrak P}=K_{\mathfrak p}$. For $\mathfrak p\in T$ since $\alpha'_{\mathfrak p}=u_{\mathfrak p}^n$ is an n-th power. For $\mathfrak p\notin S\cup T$ it holds because $\alpha'_{\mathfrak p}$ is a unit and $M_{\mathfrak P}|K_{\mathfrak p}$ is unramified (see chap. V, (3.3)). This is why $[\alpha]\in N_{M|K}C_M$. q.e.d. □

Proof of theorem (4.2): The identity $(C_K : C_K(S,T)) = [L:K]$ follows from the exact sequence

$$1\longrightarrow I^{S\cup T}\cap K^*/I_K(S,T)\cap K^*\longrightarrow I^{S\cup T}/I_K(S,T)$$
$$\longrightarrow I_K/I_K(S,T)K^*\longrightarrow 1.$$

Since $I^{S\cup T}K^* = I_K$, the order of the group on the right is

$$(I_K : I_K(S,T)K^*) = (I_K/K^* : I_K(S,T)K^*/K^*)$$
$$= (C_K : C_K(S,T)).$$

The order of the group on the left is

$$(I^{S\cup T}\cap K^* : I_K(S,T)\cap K^*) = (K^{S\cup T} : (K^{S\cup T})^n) = n^{2s-r},$$

because $\#(S\cup T) = 2s-r$, and $\mu_n\subseteq K^{S\cup T}$. In view of chap. II, (5.8), the order of the group in the middle is

$$(I^{S\cup T} : I_K(S,T)) = \prod_{\mathfrak p\in S}(K_{\mathfrak p}^* : K_{\mathfrak p}^{*n}) = \prod_{\mathfrak p\in S}\frac{n^2}{|n|_{\mathfrak p}} = \frac{n^{2s}}{\prod_{\mathfrak p}|n|_{\mathfrak p}} = n^{2s}.$$

Altogether this gives

$$(C_K : C_K(S,T)) = \frac{n^{2s}}{n^{2s-r}} = n^r = [L:K].$$

We now show the inclusion $C_K(S,T) \subseteq N_{L|K}C_L$. Let $\alpha \in I_K(S,T)$. In order to show that $\alpha \in N_{L|K}I_L$ all we have to check, by (3.2), is again that every component $\alpha_\mathfrak{p}$ is a norm from $L_\mathfrak{P}|K_\mathfrak{p}$. For $\mathfrak{p} \in S$ this is true because $\alpha_\mathfrak{p} \in K_\mathfrak{p}^{*n}$ is an n-th power, hence a norm from $K_\mathfrak{p}(\sqrt[n]{K_\mathfrak{p}^*})$ (see chap. V, (1.5)), so in particular also from $L_\mathfrak{P}|K_\mathfrak{p}$. For $\mathfrak{p} \in T$ it holds because (4.1) gives $\Delta \subseteq K_\mathfrak{p}^{*n}$, and thus $L_\mathfrak{P} = K_\mathfrak{p}$. Finally, it holds for $\mathfrak{p} \notin S \cup T$ since $\alpha_\mathfrak{p}$ is a unit and $L_\mathfrak{P}|K_\mathfrak{p}$ is unramified (see chap. V, (3.3)). We therefore have $I_K(S,T) \subseteq N_{L|K}I_L$, i.e., $C_K(S,T) \subseteq N_{L|K}C_L$.

Now if $L|K$ is cyclic, i.e., if $r = 1$, then from (3.6),

$$|L:K| \le (C_K : N_{L|K}C_L) \le (C_K : C_K(S,T)) = [L:K],$$

hence $N_{L|K}C_L = C_K(S,T)$. □

Now that we have an explicit picture in the case of a Kummer field, the result we want follows also in complete generality:

(4.4) Theorem (Global Class Field Axiom). *If $L|K$ is a cyclic extension of algebraic number fields, then*

$$\#H^i(G(L|K), C_L) = \begin{cases} [L:K] & \text{for } i = 0, \\ 1 & \text{for } i = -1. \end{cases}$$

Proof: Since $h(G(L|K), C_L) = [L:K]$, it is clearly enough to show that $\#H^0(G(L|K), C_L) \mid [L:K]$. We will prove this by induction on the degree $n = [L:K]$. We write for short $H^0(L|K)$ instead of $H^0(G(L|K), C_L)$. Let $M|K$ be a subextension of prime degree p. We consider the exact sequence

$$C_M/N_{L|M}C_L \xrightarrow{N_{M|K}} C_K/N_{L|K}C_L \longrightarrow C_K/N_{M|K}C_M \longrightarrow 1,$$

i.e., the exact sequence

$$H^0(L|M) \xrightarrow{N} H^0(L|K) \longrightarrow H^0(M|K) \longrightarrow 1.$$

If $p < n$, then $\#H^0(L|M) \mid [L:M]$, $\#H^0(M|K) \mid [M:K]$ by the induction hypothesis, hence $\#H^0(L|K) \mid [L:M][M:K] = [L:K]$.

Now let $p = n$. We put $K' = K(\mu_p)$ and $L' = L(\mu_p)$. Since $d = [K':K] \mid p-1$, we have $G(L|K) \cong G(L'|K')$. $L'|K'$ is a cyclic

Kummer extension, so by (4.2), $\#H^0(L'|K') = [L':K'] = p$. It therefore suffices to show that the homomorphism

$$H^0(L|K) \longrightarrow H^0(L'|K') \quad (*)$$

induced by the inclusion $C_L \to C_{L'}$ is injective. $H^0(L|K)$ has exponent p, because for $a \in C_K$ we always have $a^p = N_{L|K}(a)$. Taking $d = [K':K]$-th powers on $H^0(L|K)$ is therefore an isomorphism. Now let $x = a \bmod N_{L|K}C_L$ belong to the kernel of $(*)$. We write $x = y^d$, for some $y = b \bmod N_{L|K}C_L$. Then y also is in the kernel of $(*)$, i.e., $b = N_{L'|K'}(c')$, $c' \in C_{L'}$, and we find:

$$y^d = N_{K'|K}(b) = N_{K'|K}(N_{L'|K'}(c')) = N_{L|K}(N_{L'|L}(c')) \in N_{L|K}C_L.$$

Hence $x = y^d = 1$.

An immediate consequence of the theorem we have just proved is the famous Hasse **Norm Theorem**:

(4.5) Corollary. *Let $L|K$ be a cyclic extension. An element $x \in K^*$ is a norm if and only if it is a norm locally everywhere, i.e., a norm in every completion $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ $(\mathfrak{P}|\mathfrak{p})$.*

Proof: Let $G = G(L|K)$ and $G_{\mathfrak{p}} = G(L_{\mathfrak{P}}|K_{\mathfrak{p}})$. The exact sequence

$$1 \longrightarrow L^* \longrightarrow I_L \longrightarrow C_L \longrightarrow 1$$

of G-modules gives, by chap. IV, (7.1), an exact sequence

$$H^{-1}(G, C_L) \longrightarrow H^0(G, L^*) \longrightarrow H^0(G, I_L).$$

By (4.4), we have $H^{-1}(G, C_L) = 1$, and from (3.2) it follows that $H^0(G, I_L) = \bigoplus_{\mathfrak{p}} H^0(G_{\mathfrak{p}}, L_{\mathfrak{P}}^*)$. Therefore the homomorphism

$$K^*/N_{L|K}L^* \longrightarrow \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}L_{\mathfrak{P}}^*$$

is injective. But this is the claim of the corollary. □

It should be noted that cyclicity is crucial for Hasse's norm theorem. In fact, whereas it is true by (3.2) that an element $x \in K^*$ which is everywhere locally a norm, is always the norm of some idele α of L, this need not be by any means a principal idele, not even in the case of arbitrary abelian extensions.

Exercise 1. l)ctermme the norm group $_{L}$ for an arbitrary Kummer cxtcn�1on m a way analogou, to the ca�e treated in where $G(L|K) \cong$ (Z/p"Zl'.

Exercise 2. Let be a primitive m-th root of unity. Show that the norm group *N,z;li:l J]Cr,* the ray da�, group mod m $= (m)$ in $C_{\mathbb{Q}}$.

Exerci1>e 3. An e4uation .1 ^{2} $= h$, *a. h* ec *K*'. has a solution in *K* if and on!} il it 1, ,olvable everywhere i.e., 111 each completion *K* p.

Hint: ,1^2 - U\$^2$ = NKl-.;<1)IK(,1 - *-Jay)* 1t *ll* rf_ K^{*2}.

Exercise 4. If a quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$ repre,ent, ..:ero over a field *K* with more than five elements (i.e., $a_1x_1^2 + \cdots + a_nx_n^2 = 0$ has a nontrivial �olut1on in *K*). then there is a representation of zero in which all.1.,f=O.

Hint: It *a/;*^{2} = *}*, *f*= 0, *h f*= 0, then there arc non-7ero elements *a* and *fi* �uch that *aa*^{2} +*hji*^{2} = *}*,. To prove th1,. multiply the identity

(I - 1)2 *4t*

(t+ 1)2 ±(l± ll2= I

hy *a/;*^{2} = A and msert *1* $= b\gamma^2/a$, for some element $\gamma \neq 0$ such that $t \neq \pm 1$. Use thi� to prove the claim by induction.

Exercise 5. A 4um.!ratic form ,u:^{2} + c:^{2} *,a, h,c* E *K".* rcprc�cnt, 7ero if and only irit represents 7eroeverywhcrc

Remark: In complete generality, one ha, the followmg "local-to-glohal prme1ple'":

Theorem of Minkowski-Hasse: A 4uadratic form over J number held *K* repre,ent� 7ero 1!" and only 1f II repre,enL, zero over every completion *KP*

The proof follow� rrorn the rc�ult stated m exercise .5 hy pure Jlgebra (�cc 11131).

§ 5. The Global Reciprocity Law

Now that we know that the ide!e cla�s group satisfies the cla% field axiom, we proceed to determine a pair of homomorphi\m1>

$$(G_{\mathbb{Q}} \xrightarrow{d} \widehat{\mathbb{Z}},\ C_{\mathbb{Q}} \xrightarrow{v} \widehat{\mathbb{Z}})$$

obeying the rules of abstract cla1>s field theory a� developed in chap. IV, *4. For the Z-extension of given by *d,* we have only one choice. It i1> described in the following:

(5.1) Proposition. *Lei Q* l(Q *be the field obtained by adjoining all root.�* of *unity, <md let T be the torsion subgroup* of $G(DIK)$ (i.e., *the group* of *all* element.� of *fiuite order). Then the fixed field* ij l(Q of T *is a Z-extension.*

Proof: Since Q = Un .1::](1111), we llnd

Gi!?l(!l �� G(l!(1,,,JIG) � � (:Z/n:Z)' � Z·

But Z = TT" ZI', and Z;, � Zp x Z/(p - l)Z for p -=I- 2 and Z; � Z2 x Z/2Z. Consequently,

G(QIQ) � Z* �ix f, where f = TT Z/(p- 1)ZxZ/2Z.
/Jci-2

Thi1> shows that the tor5ion 5ubgroup T of $G(Q$ IQ) i� iwmorphic to the tor�ion subgroup of f Since the latter contains the group ffip_t-2Z/(p - I)� ffi Z/2Z, we see that the closure T of Tis iso_'.?lorphic to T. Now, if Q is the fixed field of T, this implies that C(Qll!Ql) = GWIQJ/T c, Z. LJ

Another description of the Z-extension QIQl is obtained in the following manner. For every prime number p, let !11, IQ he the field obtained by adjoining all roots of unity of p-power order, Then

G(S?plQl) = l!!!! G(Q(p1,,)IQ) = l!!!! (7,/p''Y..)* = Z;,.

and Z;, � ZI' x Z/(p - l)Z for p -=I- 2 and Z; � Z2 x Z/2Z. The torsion subgroup of Z;, is isomorphic to Zj(p - l)Z, resp. Z/2Z, and taking its fixed field gives an extemion ij(pJIQ with Galois group

G(ij'"1(!l c, :Z,,.

The 2-extension Q1:QJ i1, then the composite fj_, = TTI' ij<1,1.

We fix an isomorphism G(IQ IQ) � :5:. There j.., no canonical choice a5 in the case of local fields. However, the reciprocity law will not depend on the choice. Via G(QIQ) � Z, we obtain a continuous surjective homomorphism

d: G:"t----+ Q

of the absolute Galois group Gru: = G(QIQl). With this we continue a� in chap. IV, §4, choosing $k = $ Q as our base field. If KIQ is a finite extension. then we put fr = rKn Q : Ql and get a suijective homomorphism

dK = 1 y;d:GK -----+ Z,

which defines the Z-extension $K = Kij$ of K. $i<IK$ is called the cyclotomic Z-extension of K. We denote again by 'PK the elemenl of G(K IK) which i�

mapped to 1 by the isomorphism $G(\tilde{K}|K) \cong \hat{\mathbb{Z}}$, and by $\varphi_{L|K}$ the restriction $\varphi_K|_L$ if $L|K$ is a subextension of $\tilde{K}|K$. The automorphism $\varphi_{L|K}$ must not be confused with the Frobenius automorphism corresponding to a prime ideal of L (see §7).

For the $G_{\mathbb{Q}}$-module A, we choose the union of the idele class groups C_K of all finite extensions $K|\mathbb{Q}$. Thus $A_K = C_K$. The henselian valuation $v : C_{\mathbb{Q}} \to \hat{\mathbb{Z}}$ will be obtained as the composite

$$C_{\mathbb{Q}} \xrightarrow{(\ ,\tilde{\mathbb{Q}}|\mathbb{Q})} G(\tilde{\mathbb{Q}}|\mathbb{Q}) \xrightarrow{d} \hat{\mathbb{Z}},$$

where the mapping $(\ ,\tilde{\mathbb{Q}}|\mathbb{Q})$ will later turn out to be the norm residue symbol $(\ ,\tilde{\mathbb{Q}}|\mathbb{Q})$ of global class field theory (see (5.7)). For the moment we merely define it as follows.

For an arbitrary finite abelian extension $L|K$, we define the homomorphism

$$(\ ,L|K) : I_K \to G(L|K)$$

by

$$(\alpha, L|K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}|K_{\mathfrak{p}}),$$

where $L_{\mathfrak{p}}$ denotes the completion of L with respect to a place $\mathfrak{P}|\mathfrak{p}$, and $(\ ,L_{\mathfrak{p}}|K_{\mathfrak{p}})$ is the norm residue symbol of local class field theory. Note that almost all factors in the product are 1 because almost all extensions $L_{\mathfrak{p}}|K_{\mathfrak{p}}$ are unramified and almost all $\alpha_{\mathfrak{p}}$ are units.

(5.2) **Proposition.** *If $L|K$ and $L'|K'$ are two abelian extensions of finite algebraic number fields such that $K \subseteq K'$ and $L \subseteq L'$, then we have the commutative diagram*

$$\begin{tikzcd}
I_{K'} \arrow[r, "(\ ,L'|K')"] \arrow[d] & G(L'|K') \arrow[d] \\
I_K \arrow[r, "(\ ,L|K)"] & G(L|K).
\end{tikzcd}$$

Proof: For an idele $\alpha = (\alpha_{\mathfrak{P}}) \in I_{K'}$ of K', we find by chap. IV, (6.4), that

$$(\alpha_{\mathfrak{P}}, L'_{\mathfrak{P}}|K'_{\mathfrak{P}})|_{L_{\mathfrak{p}}} = \big(N_{K'_{\mathfrak{P}}|K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}), L_{\mathfrak{p}}|K_{\mathfrak{p}}\big), \quad (\mathfrak{P}|\mathfrak{p}),$$

and (2.2) implies

[NK'1da). LI Kl= Q(NK'1da)p. LplKp) = Q,IJP(NK:+iKP(m_p), LplKp)

� TT(a�,L:,,IK�)IL � [a,L'IK'IIL D
�

If LI K is an abelian extension of infinite degree. then we define the homomorphism

I ,LIKI 'IK - G(LIK)

by its restriction5 [,LIK]IL' := [.L'IK] to the finite subextensions L' of LIK. In other words, ifa Eh. then the elements fa,L'IK] define, by (5.2). an element of the projective limit � L' G(L'IK), and la.LI KI is precisely this element, once we identify G(LIK) = � G(L'IK). Again one has the equation

[a,LIK] � TT(a,,L,IK,J.

where Lp does not denote the completion of L ½ith respect to a place above p, but rather the *localization,* i.e., the union of the completions L�IKp of all linite subextem,iom, (sec chap. II, §8). Then /.plKp is Galois, G(LplKp) � G(LIK), and the product nP(ap,LplKp) converge5 in the prollnitc group to the element [a,LIKJ. Indeed, if L'IK varies over the llnitc subextensiom of /.IK, then the 5ets SL'= {p I (ap,L�IKp) -=I- I) are all finite, �o that we may write down the finite products

al,= n(lip.LplKp)EC(LIK>.
p<c.'1'1·

TI1ey converge to [a, L IK J, for if [a, L IKlG(L IN) is one of the fundamental neighbourhoods (i.e., NIK is one of the finite subextensions of LIK), then

$$\sigma_{L'} \in [\alpha, L|K]G(L|N)$$

for all L' 2 N because

aL' IN� TT(a,,N,IKμ) � Ja,NIK] � Ja,LJKI l,v.

Thi5 shows that [a, L IK] is the only accumulation point of the family {a,_}.

It is clear that proposition (5.2) remains true for infinite extemions L and L' of finite algebraic number fields Kand K'.

(5.3) Proposition. *For every root of unity* ζ *and every principal idele* $a \in K^*$ *one has*

$$[a, K(\zeta)|K] = 1.$$

Proof: By (5.2), we have $[N_{K|\mathbb{Q}}(a), \mathbb{Q}(\zeta)|\mathbb{Q}] = [a, K(\zeta)|K]|_{\mathbb{Q}(\zeta)}$. Hence we may assume that $K = \mathbb{Q}$. Likewise we may assume that ζ has prime power order $l^m \neq 2$. Now let $a \in \mathbb{Q}^*$, let v_p be the normalized exponential valuation of $\mathbb{Q}_p$ for $p \neq \infty$ and write $a = u_p p^{v_p(a)}$. For $p \neq l, \infty$, $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ is unramified and $(p, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p)$ is the Frobenius automorphism $\varphi_p : \zeta \mapsto \zeta^p$. From chap. V, (2.4), we thus get

$$\big(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p\big)\zeta = \zeta^{n_p} \quad \text{with} \quad n_p = \begin{cases} p^{v_p(a)} & \text{for } p \neq l, \infty, \\ u_p^{-1} & \text{for } p = l, \\ \operatorname{sgn}(a) & \text{for } p = \infty. \end{cases}$$

Hence

$$\big(a, \mathbb{Q}(\zeta)|\mathbb{Q}\big)\zeta = \prod_p \big(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p\big)\zeta = \zeta^{\alpha},$$

where $\alpha = \prod_p n_p = \operatorname{sgn}(a) \prod_{p \neq l, \infty} p^{v_p(a)} u_l^{-1} = \operatorname{sgn}(a) \prod_{p \neq \infty} p^{v_p(a)} a^{-1} = 1.$ □

Since the extension $\tilde{K}|K$ is contained in the field of all roots of unity over K, the proposition implies

$$[a, \tilde{K}|K] = 1$$

for all $a \in K^*$. The homomorphism $[\ , \tilde{K}|K] : I_K \to G(\tilde{K}|K)$ therefore induces a homomorphism

$$[\ , \tilde{K}|K] : C_K \longrightarrow G(\tilde{K}|K),$$

and we consider its composite

$$v_K : C_K \longrightarrow \hat{\mathbb{Z}}$$

with $d_K : G(\tilde{K}|K) \to \hat{\mathbb{Z}}$. The pair (d_K, v_K) is then a class field theory, for we have the

(5.4) Proposition. *The map* $v_K : C_K \to \hat{\mathbb{Z}}$ *is surjective and is a henselian* *valuation with* respect *to dK.*

Proof: We first show surjectivity. If *l.lK* is a tinite subextension of *K1K.* then the map

[,LIKI � n< .L,[K,): lK----+ G(L[K)
p

i� surjective. Indeed, since (,l.plKp) : *K;* ----+ G(LplKp) i� �urjective, *[lK,LIK]* comains all decompo�ition groups G(LplKp)· Thm all p �plit completely in the !hcd tield *M* of [/ *K, I.* | *K*]. By (3.8), this implie" that *M* = *K,* and so *[/K,l,IKI* = G(LIK), This yield� furthermore that f/ *K, K* lK l =[CK, ii Kl is dense in *G(K* | *K*). In the exact sequence

l ------+ C¼ ------+ *CK* � -----+ l

(see * I) the group C¼ is compact by (1.6), and we obtain a splitting, if we identify R.: with the group of positive real number� in any infinite completion *Kp,* Thus *CK* = *Ci* x *f!t�.* Now, fR:.KlKJ = I, for if *x* E then [x,K.IKJIL = [x.LIKl = I for every !inite �ubextemion *LIK KiK,* because we may alway� write *x* = with *y* ER: and *n* = fL: K]. Therefore [CK,ilK] = [C¼,R'IK) is a closed, dense subgroup of *G(KlK)* and therefore equal to C(ilK). This prove� the surjectivity *ofvK =dK* c [,KIK].

In the definition of a hensclian va!.!!ation given in chap. IV, (4.6), condition (i) i� sati5tlcd because *vK(CK)* = ?., and condition (ii) follows from (5.2) because for every finite extension LI *K* we have the identity

vK(NL1KCLI = vK(N, ,Kfi) = ddNL1Kh,ilK]

=fL1KddtL,LILI= tfwv1.(C1.)=.hwi. CJ

In view of the fact that the idelc cla�� group *CK* satisfies the class field axiom, the pair

(dQ: G.:;_,----+ 2, :C:;;:, ---- +i)

comtitutcs a clas� field theory, the "global field theory". The above homomorphism *t'K* = *th* 8 f, R'IK]: *CK* ----+ for finite extensiom *K* lQ, sati�fies the formula

1'K = 0 ! ,QIQ]0 *NK11:,,* = *y;v-:.:_,* o *NK1,:;_*

and is therefore preci�ely the induced homomorphism in the �cmc of the abstract theory in ch:tp. IV, (4.7).

As the main result of global class field theory we now obtain the Artin reciprocity law:

(5.5) Theorem. *For every Galois extension $L|K$ of finite algebraic number fields we have a canonical isomorphism*

$$r_{L|K} : G(L|K)^{ab} \xrightarrow{\ \sim\ } C_K/N_{L|K}C_L.$$

The inverse map of $r_{L|K}$ yields a surjective homomorphism

$$(\ ,L|K) : C_K \to G(L|K)^{ab}$$

with kernel $N_{L|K}C_L$. The map $(\ ,L|K)$ is called the **global norm residue symbol.** We view it also as a homomorphism $I_K \to G(L|K)^{ab}$.

For every place $\mathfrak{p}$ of K, we have on the one hand the embedding $G(L_\mathfrak{P}|K_\mathfrak{p}) \hookrightarrow G(L|K)$, and on the other the canonical injection

$$[\ ] : K_\mathfrak{p}^* \to C_K,$$

which sends $a_\mathfrak{p} \in K_\mathfrak{p}^*$ to the class of the idele

$$(a_\mathfrak{p}) = (\dots, 1, 1, 1, a_\mathfrak{p}, 1, 1, \dots).$$

These homomorphisms express the compatibility of local and global class field theory as follows.

(5.6) Proposition. *If $L|K$ is an abelian extension and $\mathfrak{p}$ is a place of K, then the diagram*

$$\begin{tikzcd} K_\mathfrak{p}^* \arrow[r, "(\ ,L_\mathfrak{P}|K_\mathfrak{p})"] \arrow[d, "{[\ ]}"'] & G(L_\mathfrak{P}|K_\mathfrak{p}) \arrow[d] \\ C_K \arrow[r, "(\ ,L|K)"] & G(L|K) \end{tikzcd}$$

is commutative.

Proof: We first show that the proposition holds if $L|K$ is a subextension of $\tilde{K}|K$, or if $L = K(i)$, $i = \sqrt{-1}$, and $\mathfrak{p}|\infty$. Indeed, the two maps $[\ ,\tilde{K}|K]$, $(\ ,\tilde{K}|K) : I_K \to G(\tilde{K}|K)$ agree because from chap. IV, (6.5), we have

$$d_K \circ (\ ,\tilde{K}|K) = v_K = d_K \circ [\ ,\tilde{K}|K].$$

Thus, if $L|K$ is a subextension of $\tilde{K}|K$ and $\alpha = (\alpha_\mathfrak{p}) \in I_K$, then

$$(\alpha, L|K) = [\alpha, L|K] = \prod_\mathfrak{p} (\alpha_\mathfrak{p}, L_\mathfrak{P}|K_\mathfrak{p}).$$

In particular, for $a_\mathfrak{p} \in K_\mathfrak{p}^*$ we have the identity

$$([a_\mathfrak{p}], L|K) = (a_\mathfrak{p}, L_\mathfrak{P}|K_\mathfrak{p}),$$

which shows that the diagram is commutative when restricted to the finite subextensions of $\tilde{K}|K$.

On the other hand, let $L = K(i)$, $\mathfrak{p}|\infty$, and $L_\mathfrak{p} \neq K_\mathfrak{p}$. Then $K_\mathfrak{p} = \mathbb{R}$, $\mathbb{R}_+^*$ is the kernel of $(\ ,L_\mathfrak{p}|K_\mathfrak{p})$ and $(-1, L_\mathfrak{p}|K_\mathfrak{p})$ is complex conjugation in $G(L_\mathfrak{p}|K_\mathfrak{p}) = G(\mathbb{C}|\mathbb{R})$. Thus, all we have to show is that $((-1), L|K) \neq 1$. If we had $((-1), L|K) = 1$, then the class of (-1) would be the norm of a class of C_L, i.e., $(-1)a = N_{L|K}(\mathfrak{a})$ for some $a \in K^*$ and an idèle $\mathfrak{a} \in I_L$. This would mean that $a = N_{L_\mathfrak{q}|K_\mathfrak{q}}(\mathfrak{a}_\mathfrak{q})$ for $\mathfrak{q} \neq \mathfrak{p}$ and $-a = N_{L_\mathfrak{p}|K_\mathfrak{p}}(\mathfrak{a}_\mathfrak{p})$, i.e., $(a, L_\mathfrak{q}|K_\mathfrak{q}) = 1$ for $\mathfrak{q} \neq \mathfrak{p}$ and $(-a, L_\mathfrak{p}|K_\mathfrak{p}) = 1$. By (5.3), we have $1 = [a, L|K] = \prod_\mathfrak{q}(a, L_\mathfrak{q}|K_\mathfrak{q}) = (a, L_\mathfrak{p}|K_\mathfrak{p})$, so that $(-1, L_\mathfrak{p}|K_\mathfrak{p}) = 1$, and therefore $-1 \in N_{L_\mathfrak{p}|K_\mathfrak{p}}(L_\mathfrak{p}^*) = \mathbb{R}_+^*$, a contradiction.

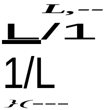
We now reduce the general case to these special cases as follows. Let $L'|K'$ be an abelian extension, so that $K \subseteq K'$, $L \subseteq L'$. We then consider the diagram

$$\begin{tikzcd}[row sep=small, column sep=small]
& G(L'_\mathfrak{p}|K'_\mathfrak{p}) \arrow[dl] \arrow[dd] & & K'^*_\mathfrak{p}/N_{L'_\mathfrak{p}|K'_\mathfrak{p}}L'^*_\mathfrak{p} \arrow[ll] \arrow[dl] \arrow[dd] \\
G(L_\mathfrak{p}|K_\mathfrak{p}) \arrow[dd] & & K^*_\mathfrak{p}/N_{L_\mathfrak{p}|K_\mathfrak{p}}L^*_\mathfrak{p} \arrow[ll, crossing over] & \\
& G(L'|K') \arrow[dl] & & C_{K'}/N_{L'|K'}C_{L'} \arrow[ll] \arrow[dl] \\
G(L|K) & & C_K/N_{L|K}C_L \arrow[ll] \arrow[from=uu, crossing over] &
\end{tikzcd}$$

where $L_\mathfrak{p} = K_\mathfrak{p}L$, $K'_\mathfrak{p} = K_\mathfrak{p}K'$, $L'_\mathfrak{p} = K_\mathfrak{p}L'$. In this diagram, the top and bottom are commutative by chap. IV, (6.4), and the sides are commutative for trivial reasons. If now $L'|K'$ is one of the special extensions for which the proposition is already established, then the back diagram is commutative, and hence also the front one, for all elements of $G(L_\mathfrak{p}|K_\mathfrak{p})$ in the image of $G(L'_\mathfrak{p}|K'_\mathfrak{p}) \to G(L_\mathfrak{p}|K_\mathfrak{p})$. This makes it clear that it is enough to find, for every $\sigma \in G(L_\mathfrak{p}|K_\mathfrak{p})$, some special extension $L'|K'$ such that σ lies in the image of $G(L'_\mathfrak{p}|K'_\mathfrak{p})$. It is even sufficient to do this only for all σ of prime power order, because they generate the group. Passing to the fixed field of σ we may assume moreover that $G(L_\mathfrak{p}|K_\mathfrak{p})$ is generated by σ.

When $\mathfrak{p}|\infty$ and $L_\mathfrak{p} \neq K_\mathfrak{p}$, i.e., $K_\mathfrak{p} = \mathbb{R}$, $L_\mathfrak{p} = \mathbb{C}$, we put $L' = L(i) \subseteq \mathbb{C}$, and choose for K' the fixed field of the restriction of complex conjugation to L'. Then $L' = K'(i)$ and $K'_\mathfrak{p} = \mathbb{R}$, $L'_\mathfrak{p} = \mathbb{C}$, so the mapping $G(L'_\mathfrak{p}|K'_\mathfrak{p}) \to G(L_\mathfrak{p}|K_\mathfrak{p})$ is surjective.

When $\mathfrak{p} \nmid \infty$, we find the extension $L'|K'$ as follows. Let σ be of p-power order. We denote by $\tilde{K}|K$, resp. $\tilde{L}|L$, the $\mathbb{Z}_p$-extension contained in $\tilde{K}|K$, resp. $\tilde{L}|L$, and consider the field diagram



with localintiom .RP= Kpf, LP= Lpf� (all field� arc considered to lie in a common bigger field). We mily now lift *o* E G(LplKp) = G(LIK) to an automorphism *Cl* of *LP* such that

(I) *Cl* E G(LplKp),

(2)6-IR =*rpR* $_{1}$ *K* forsomen EN.

Indeed, '>im:e RP= *Ki)(* -*I*- Kp, the group G(RplKµ) -*I*- I, and thus i� of finite index if viewed as subgroup of G(flK) ;;::: *'LI'*. It is ,!_herefore generated by a natural power *ifr* = <*pf* IK of Frohenius <*"PiiK* E *G(K* IK). A� in the proof of chap. IV. (4.4). we may lift *o* to a CT E G([p IKµ) such that CTIRP = *vrm. m* EN. so that CTIK =

We now take lhe tixed field *K'* of CT I *[,* and the extension *L'* = *K'L.* As in chap. IV. (4.5), conditiom (ii) and (iii), it then follows that [K' : KI < oc and *R'* = *L. L'IK'* is therefore a �ubexten�ion of f'IK'. and *o* is the image of 6-lcp under *G(L�lK�)*----+ G(LµIKp)- This finishes the proof. □

(5.7) Corollary. *ffLIK is an abeli.m extension* and *a*= (aµ) E *IK, then*

(a,LIK) � TT(apJ,IK,).
p

In particular. for a *principal* ide/e *a* E *K*� we *have the* produc/ formula

TT(a,LplK,J�l.
p

Proof: Since *I K* is topologically generated by the idelcs or the form *a* = (oµ), op E *K;,* it is enough to prove the fir�! formula for the�e idele�. But thi� i� exactly the statement of (5.h):

(a.LIK) = *(\ap),LIK)* = (oµ.LplKp) = *n* *<aq,LqlKq).*
,,

The product formula i� a consequence of the fact that *(a.LI K)* depends only on the idele cla�s *a* mod *K*.* □

Identifying $K_\mathfrak{p}^*$ with its image in C_K under the map $a_\mathfrak{p} \mapsto (a_\mathfrak{p})$, we obtain the following further corollary, where we use the abbreviations $N = N_{L|K}$ and $N_\mathfrak{p} = N_{L_\mathfrak{P}|K_\mathfrak{p}}$.

(5.8) Corollary. *For every finite abelian extension one has*

$$N C_L \cap K_\mathfrak{p}^* = N_\mathfrak{p} L_\mathfrak{P}^*.$$

Proof: For $x_\mathfrak{p} \in N_\mathfrak{p} L_\mathfrak{P}^*$ we see from (5.6) that $((x_\mathfrak{p}), L|K) = (x_\mathfrak{p}, L_\mathfrak{P}|K_\mathfrak{p}) = 1$. Thus the class $\bar{a}$ is contained in NC_L. Therefore $N_\mathfrak{p}L_\mathfrak{P}^* \subseteq NC_L$. Conversely, let $\bar{a} \in NC_L \cap K_\mathfrak{p}^*$. Then $\bar{a}$ is represented on the one hand by a norm idele $\alpha = N\beta$, $\beta \in I_L$, and on the other hand by an idele $(x_\mathfrak{p})$, $x_\mathfrak{p} \in K_\mathfrak{p}^*$. Thus $(x_\mathfrak{p})a = N\beta$ with $a \in K^*$. Passing to components shows that a is a norm from $L_\mathfrak{Q}|K_\mathfrak{q}$ for every $\mathfrak{q} \neq \mathfrak{p}$, and the product formula (5.7) shows that a is also a norm from $L_\mathfrak{P}|K_\mathfrak{p}$. Therefore $x_\mathfrak{p} \in N_\mathfrak{p}L_\mathfrak{P}^*$, and this proves the inclusion $NC_L \cap K_\mathfrak{p}^* \subseteq N_\mathfrak{p}L_\mathfrak{P}^*$. □

Exercise 1. If D_K is the connected component of the unit element and $K^{ab}|K$ is the maximal abelian extension of K, then $C_K/D_K \cong$ ...

Exercise 2. For every place $\mathfrak{p}$ of K one has $K_\mathfrak{p}^{ab} = K^{ab}K_\mathfrak{p}$.

Hint: Use (5.6) and (5.8).

Exercise 3. Let p be a prime number, and let $M_p|K$ be the maximal abelian p-extension unramified outside of (p). Further, let $H|K$ be the maximal unramified subextension of $M_p|K$ in which the infinite places split completely. Then there is an exact sequence

$$1 \to G(M_p|H) \to G(M_p|K) \to Cl_K(p) \to 1,$$

where $Cl_K(p)$ is the p-Sylow subgroup of the ideal class group Cl_K, and there is a canonical isomorphism

$$G(M_p|H) \cong \prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)} / \Big(\prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)} \cap \bar{E}\Big).$$

where $\bar{E}$ is the closure of the (diagonally embedded) unit group $E = \dots$ in $\prod_{\mathfrak{p}|p} U_\mathfrak{p}$.

Exercise 4. The group $\bar{E}(p) := \bar{E} \cap \prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)}$ is a $\mathbb{Z}_p$-module of rank $r_p(K) := \operatorname{rank}_{\mathbb{Z}_p}(\bar{E}(p)) = |K:\mathbb{Q}| - \operatorname{rank}_{\mathbb{Z}_p} G(M_p|K)$. $r_p(K)$ is called the *p-adic unit rank.*

Problem: For the p-adic unit rank, one has the famous Leopoldt conjecture:

$$r_p(K) = r + s - 1$$

where r, resp. s, is the number of all real, resp. complex, places; in other words,

$$\operatorname{rank}_{\mathbb{Z}_p} G(M_p|K) = s + 1$$

The Leopoldt conjecture was proved for abelian number fields $K|\mathbb{Q}$ by the American mathematician ARMAND BRUMER [22]. The general case is still open to date.

§ 6. Global Class Fields

A:,, in local class field theory, the reciprocity law provide" al�o in global cla�5 llcl<l lheory a complete classification of all abelian extensions of a finite algebraic number field K. For this it is nccc��ary lo view the idele cla�s group CK as a topological group, equipped with it5 natural topology which the valuations of the various completions KP impre% upon it (:,,ee § I).

(6.1) Theorem. *The map*

$$LI----+ JV/.= N1.1KCt.$$

is a I *-1-corre.\pondence between the* finite *abelii:W extemion.�* LI*K and the closed subgroup,* of *finite index* in *CK.* *Moreover* one *lws:*

$$L1 S; L2 \{:::::::\}.VL1\ 2\ \}\backslash(Le'\ A�.,1.2 = .V1,\ n.VLc,\cdot\ )l,/L1nL2 = ,,vl1\cdot''^1 i.2-$$

The field LI*K corre.�ponding to the .�*ubgroup *JV* of *CK is called the* class **field** of.V. *Il satisfies*

$$G(L|K) \cong C_K/\mathcal{N}\,\blacksquare$$

Proof: By chap. IV. (6.7), all we have to show is that the subgroup:,, JV ofC K which are open in the nonn topology are precisely the closed :,,ubgroup:,, of !inite index for the natural topology.

If the :,,ubgroup JV is open in the norm topology, then it contain:,, <1 norm group $N_{1\_1}KCi.$ and i� therefore of tlnite index. because from (5.5), $(CK : NL_1KCL) = \#G(LIK)ah\_$ To show that ;Vi:,, closed it is enough to show that $NLIKCL$ i:,,. For this. we choo"e an infinite place p of K and denote hy $I'K$ the image of the subgroup of po�itive real numbers in K_p under the mapping ( ) : $K;\ \rightarrow\ CK.$ Then $I'K$ is a group of repre-;entative:,, for the homomorphism 91 : CK -----+ �� with kernel ci (see � I), i.e., $CK = ci \times rK.$ By lhe same token. $I'K$ i:,, a group of repre:,,entatives for the homomorphi�m 91: CL -----+ JR:. We therefore get

$$N1,KCL = NL1KCr \times NL,K\,I'K = N1.1KCj^{i}_{-} \times l'f: = NLIKC2 \times I'K.$$

The norm map is continuom, and CZ i� compact by (1.6). Hence $NLIKC2$ i:,, clo�ed. Since rK is clearly also clo:,,ed in $CK,$ we get that $N1._1KCL$ i� closed.

Conversely let _t,,/ be a closed subgroup of CK of finite index. We have to <,how that JV i:,, open in the norm topology, i.e., contains a nonn group For thi-; we may assume that the index 11 b a prime power. For if $p/''$. and J'v·: S; CK is the group containing .V of index then .V = $_1$.\1�. and if the J\·� arc open in the norm topology, then \O

Now let J be the preimage of $\mathcal{N}$ with respect to the projection $I_K \to C_K$. Then J is open in I_K because $\mathcal{N}$ is open in C_K (with respect to the natural topology). Therefore J contains a group

$$U_S = \prod_{\mathfrak{p}\in S} \{1\} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}},$$

where S is a sufficiently big finite set of places of K containing the infinite ones and those primes that divide n, such that $I_K = JK^*$. Since $(I_K : J) = n$, J also contains the group $\prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\notin S} \{1\}$, and hence the group

$$I_K(S) = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}.$$

Thus it is enough to show that $C_K(S) = I_K(S)K^*/K^* \subseteq \mathcal{N}$ contains a norm group. If the n-th roots of unity belong to K, then $C_K(S) = N_{L|K}C_L$ with $L = K(\sqrt[n]{K_S^*})$, because of the remark following (4.2). If they do not belong to K, then we adjoin them and obtain an extension $K'|K$. Let S' be the set of primes of K' lying above primes in S. If S was chosen sufficiently large, then $I_{K'} = I_{K'}^{S'}K'^*$ and $C_{K'}(S') = N_{L'|K'}C_{L'}$ with $L' = K'(\sqrt[n]{K'^*_{S'}})$, by the above argument. Using chap. V, (3.5), this gives on the other hand that $N_{K'|K}(C_{K'}(S')) \subseteq C_K(S)$, so that

$$N_{L'|K}C_{L'} = N_{K'|K}(N_{L'|K'}C_{L'}) = N_{K'|K}(C_{K'}(S')) \subseteq C_K(S).$$

This finishes the proof. $\square$

The above theorem is called the "existence theorem" of global class field theory because its main assertion is the existence, for any given closed subgroup $\mathcal{N}$ of finite index in C_K, of an abelian extension $L|K$ such that $N_{L|K}C_L = \mathcal{N}$. This extension L is the class field for $\mathcal{N}$. The existence theorem gives a clear overview of all the abelian extensions of K once we bring in the ray class groups $C_K^{\mathfrak{m}}$ of C_K corresponding to the modules $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$. These are closed of finite index by (1.8), and they prompt the following definition.

(6.2) Definition. *The class field $K^{\mathfrak{m}}|K$ for the congruence subgroup $C_K^{\mathfrak{m}}$ is called the* **ray class field** mod $\mathfrak{m}$.

The Galois group of the ray class field is canonically isomorphic to the ray class group mod $\mathfrak{m}$:

$$G(K^{\mathfrak{m}}|K) \cong C_K/C_K^{\mathfrak{m}}.$$

One has

$$\mathfrak m \mid \mathfrak m' \implies K^{\mathfrak m} \subseteq K^{\mathfrak m'},$$

because clearly $C_K^{\mathfrak m'} \subseteq C_K^{\mathfrak m}$. Since the closed subgroups of finite index in C_K are by (1.8) precisely those subgroups containing a congruence subgroup $C_K^{\mathfrak m}$, we get from (6.1) the

(6.3) **Corollary.** *Every finite abelian extension $L|K$ is contained in a ray class field $K^{\mathfrak m}|K$.*

(6.4) Definition. Let *$L|K$ be a finite abelian extension, and let $\mathcal N_L = N_{L|K}C_L$. The* **conductor** $\mathfrak f$ of $L|K$ (or of $\mathcal N_L$) *is the gcd* of all *modules* $\mathfrak m$ *such that $L \subseteq K^{\mathfrak m}$ (i.e., $C_K^{\mathfrak m} \subseteq \mathcal N_L$).*

$K^{\mathfrak f}|K$ is therefore the smallest ray class field containing $L|K$. But it is not true in general that $\mathfrak m$ is the conductor of $K^{\mathfrak m}|K$. In chap. V, (1.6), we defined the conductor $\mathfrak f_{\mathfrak p}$ of a $\mathfrak p$-adic extension $L_{\mathfrak p}|K_{\mathfrak p}$ for a finite place $\mathfrak p$, to be the smallest power $\mathfrak f_{\mathfrak p} = \mathfrak p^n$ such that $U_{\mathfrak p}^{(n)} \subseteq N_{L_{\mathfrak P}|K_{\mathfrak p}}L_{\mathfrak P}^*$. For an infinite place $\mathfrak p$ we define $\mathfrak f_{\mathfrak p} = 1$. Then we view $\mathfrak f$ as the replete ideal $\mathfrak f \prod_{\mathfrak p|\infty} \mathfrak p^0$ and obtain the

(6.5) Proposition. *If $\mathfrak f$ is the conductor* of *the abelian* extension $L|K$, *and* $\mathfrak f_{\mathfrak p}$ *is the conductor* of *the local extension* $L_{\mathfrak P}|K_{\mathfrak p}$, *then*

Proof: Let $\mathcal N_L = N_{L|K}C_L$, and let $\mathfrak m = \prod \mathfrak p^{n_{\mathfrak p}}$ be a module ($n_{\mathfrak p} = 0$ for $\mathfrak p \nmid \infty$). One then has

$$C_K^{\mathfrak m} \subseteq \mathcal N_L \iff \mathfrak f \mid \mathfrak m \quad\text{and}\quad \prod_{\mathfrak p} \mathfrak f_{\mathfrak p} \mid \mathfrak m \iff \mathfrak f_{\mathfrak p} \mid \mathfrak p^{n_{\mathfrak p}} \quad \text{for all } \mathfrak p.$$

So to prove $\mathfrak f = \prod \mathfrak f_{\mathfrak p}$, we have to show the equivalence

$$C_K^{\mathfrak m} \subseteq \mathcal N_L \iff \mathfrak f_{\mathfrak p} \mid \mathfrak p^{n_{\mathfrak p}} \quad \text{for all } \mathfrak p.$$

It follows from the identity $\mathcal N_L \cap K_{\mathfrak p}^* = N_{\mathfrak p}L_{\mathfrak P}^*$ (see (5.8)):

$$C_K^{\mathfrak m} \subseteq \mathcal N_L \iff (\alpha \in I_K^{\mathfrak m} \Rightarrow \bar\alpha \in \mathcal N_L)$$

$$\iff (\alpha_{\mathfrak p} \equiv 1 \bmod \mathfrak p^{n_{\mathfrak p}} \Rightarrow (\alpha_{\mathfrak p}) \in \mathcal N_L \cap K_{\mathfrak p}^* = N_{\mathfrak p}L_{\mathfrak P}^*) \quad \text{for all } \mathfrak p$$

$$\iff (\alpha_{\mathfrak p} \in U_{\mathfrak p}^{(n_{\mathfrak p})} \Rightarrow \alpha_{\mathfrak p} \in N_{\mathfrak p}L_{\mathfrak P}^*) \iff U_{\mathfrak p}^{(n_{\mathfrak p})} \subseteq N_{\mathfrak p}L_{\mathfrak P}^* \iff \mathfrak f_{\mathfrak p} \mid \mathfrak p^{n_{\mathfrak p}}.$$

□

By chap. V, (1.7). the local extension LplKp, for a finite prime p, i:-. ramified if and only if its conductor fp is -1- I. This continue� to hold al�o for an infinite place p. provided we call the extension LplKμ *unramified* in this case, m, we did in chap. III. Then (6.5) yield� the

(6.6) Corollary. Lei *LIK be a finite ;.ibelian extension and* f *its conductor. Then:*

pisramitiedinl {=::::} Plf-

In the case of the base field Q, the ray class fields are nothing but the familiar cydotomic fields:

(6.7) **Proposition.** *Let m be a natural number* and m = (m). *Then /he ray* c/as.� *field* mod m of (fJ *is 1hc field*

$$\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\mu_m)$$

of *m -th* roots of *unity.*

Proof: Let *m* = nf't/h.. *Pn''*. Then (8' = nl'rl'..,__, *U?*1') x IR�. Let *m* = *m'p*11 1 1_ Then *U* 11 1 1; 'is contained in the norm group of the unramitied extension but also in the norm group according to This means, * 3, that every is a norm of 5ome idele of Q(/L111). Thu� *C*� £; On the *C:;,;c;'* ;::: (Z/mZ)* by (1.10). and therefore

(Co, cO)� [ll(M,,,), G] �(Co, NC0"""1)-

so that C1) = NCo_,(1,,,,), and thi5 proves the claim. n

According lo thi� proposition. one may view the general ray clas� fields *KmlK* as analogues of the cyclotomic fields Q(μ111)1:{]. Nonetheless, they arc not made to take over the important r61e of the latter because all we know about them i� that they exist. but not how to generate them. In the case of local fields things were different. There the analogues of the ray das� field� were the Lubin-Tate extensiom, which could be generated by the division points of formal group� - a fact that can-ies a long way (�ee chap. V, *5). This local discovery docs, however, originate from the problem of generating global cla�s fields, which will be discussed at the end of this section.

Note in pas�ing that the above propo�ition give� another proof of the theorem of Kronecker and Weber (sec chap. V. (1.10)) to the effect that every finite abelian extension $L|\mathbb{Q}$ is contained in a field $\mathbb{Q}(\mu_m)|\mathbb{Q}$, because by (1.8) the norm group $\mathcal{N}_L$ lies in some congruence subgroup $C_{\mathbb{Q}}^{\mathfrak{m}}$, $\mathfrak{m} = (m)$, so that $L \subseteq \mathbb{Q}(\mu_m)$.

Among all abelian extensions of K, the ray class field mod 1 occupies a special place. It is called the big Hilbert class field and has Galois group

$$G(K^1|K) \cong Cl_K^1 .$$

By (1.11), the group Cl_K^1 is linked to the ordinary ideal class group by the exact sequence

$$1 \longrightarrow \mathcal{O}^*/\mathcal{O}^*_+ \longrightarrow \prod_{\mathfrak{p}\ \mathrm{real}} \mathbb{R}^*/\mathbb{R}^*_+ \longrightarrow Cl_K^1 \longrightarrow Cl_K \longrightarrow 1 .$$

The big Hilbert class field has conductor $\mathfrak{f} = 1$ and may therefore be characterized by (6.6) in the following way.

(6.8) Proposition. *The big Hilbert class field is the maximal unramified abelian extension of K.*

Since the infinite places are always unramified, this means that all prime ideals are unramified. The Hilbert class field, or more precisely, the "small Hilbert class field", is defined to be the maximal unramified abelian extension $H|K$ in which all infinite places split completely, i.e., the real places stay real. It satisfies the

(6.9) Proposition. *The Galois group of the small Hilbert class field $H|K$ is canonically isomorphic to the ideal class group:*

$$G(H|K) \cong Cl_K .$$

In particular, the degree $[H:K]$ is the class number h_K of K.

Proof: We consider the big Hilbert class field $K^1|K$ and, for every infinite place $\mathfrak{p}$, the commutative diagram (see (5.6))

$$\begin{tikzcd} K_{\mathfrak{p}}^* \arrow[r, "(\,,K_{\mathfrak{p}}^1|K_{\mathfrak{p}})"] \arrow[d] & G(K_{\mathfrak{p}}^1|K_{\mathfrak{p}}) \arrow[d] \\ I_K/K^* \arrow[r, "(\,,K^1|K)"] & G(K^1|K). \end{tikzcd}$$

The &mall Hilbert cla�s held HI K is the fixed field of the subgroup G_{XJ} generated hy all $G(K$�IKp), PIXJ, Under (. K^{I} IK) lhi5 i5 the image of

$$(n_{p�}\ K;)t\}K'/I\}K'�Ii;�K'/t\}K',$$

where /;,,., = $TTp_{1,-,.K,;}$ x TTPt= Up· Therefore by (1.3),

$$G(H|K) = G(K^{\mathrm{I}}|K)/G_{\infty} \cong I_K/I_K^{S_\infty}K^* \cong Cl_K$$

Remark: The small Hilbert class field is in general not a ray da�� field in tenns of the theory developed here. But il i& in many other textbooks where ray class group� and ray class field:,, arc defined differently (�cc for imtance [1071). Thi:,, other theory is obtained by equipping all number liclds with the Minkow:,,ki metric

$$(X,Y)K = \qquad (r \text{ E Hom}(K,C)),$$

$a,=$ I if $r = T$, $a,$ = { if $r \# T$. A ray cla:,,:,, group can then be attached to any *replete* module �

$$m�\prod_{p} np''\bullet\cdot,$$

where np E Z. np 2: 0, and $n\mu = 0$ or= 1 ifploo. The groups utpJ attached to the metrized number field $(K,\ (\ ,\ )K)$ .ire defined by

$$U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} = \begin{cases} 1+\mathfrak{p}^{n_{\mathfrak{p}}}, & \text{for lip} > 0, \text{and } Up \text{ for } n\mu = 0. \text{ if p } 1\text{Xl}, \\ \mathbb{R}^*, & \text{if p is real and l!p} = 0, \\ \mathbb{R}_+^*. & \text{ifp j., real and llp} = 1, \\ \mathbb{C}^* = K_{\mathfrak{p}}^*, & \text{if p is complex.} \end{cases}$$

The *congruence suhgroup* mod m of $(K.\ (,\ )K)$ b then the subgroup $C_K^{\mathfrak{m}} = I_K^{\mathfrak{m}}K^*/K^*$ of CK fom1cd with the group

$$r; = \prod_{p} u,;^{11}_{p}{}^{1}.$$

and the factor group is the *ray ı fas.1 group* mod rn. The *rav (los,1 {tcfd* mod m of (K. (, again the clas5 field of K corresponding to the group $C;$ s;;; $C«$. As explained in chap. Ill, QJ. the infinite plilcC� p have to be comidcrcd as *ram!fied* in an extension LI K if $Lp \# K_{p}$. Likewi�e.

the *conductor* of an abclian extension *LIK,* i.e., the gcd of all module� m = np))¹¹P such that *Cl(* 5:;:; *NL1KCL,* is the replete ideal

f� flfp.
p

where now for an intinite place p, we have fp = *pn�* with *np* = 0 if *Lp* = *Kp,* and np = I if *Lp #- Kp,* Corollary (6.6) then continues to hold: a place pis ramified in *L* if and only if p occurs in the conductor f.

This entails the following modifications of the above theory, as far as ray cla1,s field:-. arc concerned. The ray cla5� field mod I is the *.1mafl* Hilbert class field. It is now the maximal abelian extension of *K* which is unramitied at *all* places. The big Hilbert class field is the ray clas� field for the module m = nPI"'' p. In the case of the base field Q, the field IQ(t) of m-th roots of unity i1, the ray class field mod *mpcx,,* where *pc,c* is the infinite place. The ray cla�5 field for the module *m* become� the maximal real subextcn�ion IQ((+ (-¹), which was not a ray class field before. This is the theory one find1, in the textbooks alluded to above. It corrc�pomb to the number field'> with the Minkowski metric. The theory of ray class llcld� according to the treatment of this book is forced upon u� already by the choice of the standard metric {x, *y)* = *Lr.*,r.Yr on *Ki,:* taken in chap. I. S 5. It is compatible �ith the Riemann-Roch theory of chap. III, and has the advantage of being simpler.

Over the field Q, the ray class field mod *(m)* can be generated, according to (6.7), them-th root� of unity, i.e., by special value1, of the exponential function The que�tion 5uggested by this observation is whether one may con�truct the abelian extensions of an arbitrary number tield in a similarly concrete way, via special values of analytic functiom. Thb was the historic origin of the notion of cla55 field. A completely sati�factory answer to thi� question has been given only in the ca�e of an imaginary tJUadratic tield *K,* The result<, for thi1, case are sub5utned under the name of Kronecker•� Jugendtraum (Kronecker'1, dream of hi� youth). We will briefly describe them here. For the proof�, which pre�uppose an in-depth knowledge of the theory of *elliptic curves,* we have to refer to [96] and [28].

An elliptic curve is given as the quotient *E* = *CJ I'* of C hy a complete lattice *I'* = :z(J)1 + *Zcv2* in This is a toru5 which receive1, the �tructure of an algebraic curve via the Weierstrass p-function

$$\wp(z) = \wp_{\Gamma}(z) = \frac{1}{z^2} + \sum_{\omega\in\Gamma'}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right].$$

where *I"*= *I'"*- {OJ. p(:::) i� a meromorphic doubly periodic function, i.e.,

1;,,(z+(J))=1;;i(z) for all wE /',

and it salisllcs, along with its derivalive p'(:), an identity

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 .$$

The constants $g_1, g1$ only depend on the lallicc $r,$ are given by $g2 = g2(I') =$ 60I\,c;eo �, $g3 = g,(I') = 140Lw\#O$ p and,;/ may thus be interpreted a� functions on C/ I'. If one takes the finite set S i; r:; I' of poles, one gets a bijection

$$\mathbb{C}/\Gamma \setminus S \xrightarrow{\sim} \left\{ (x, y) \in \mathbb{C}^2 \,\middle|\, y^2 = 4x^3 - g_2 x - g_3 \right\}, \quad z \longmapsto \big(\wp(z), \wp'(z)\big)$$

onto the affine algebraic curve in by the equation $y^1 =$ $4x^1$ - - g_1. This give" the torus the structure of an algebraic curve over of geom I. An important r61c is played by the **j-invariant**

$$j(E) = j(\Gamma) = \frac{2^6 3^3 g_2^3}{\Delta} \qquad \text{with} \quad LI = gi - 27g\{.$$

It determines the elliptic curve E up to isomorphism. Writing generator" $w_{1,w2}$ of I' in '-UCh an order that r $= o>_1/<o_1$ lies in the upper half-plane H, then)(£) becomes the value **j(r)** of a **modular function,** i.e., of a holomorphic function j on lHl which is invariant under the substitution

r i---+ :'::; for every matrix (; :) E $Sl,2(.?'.)$.

Now let K £: C be an imaginary quadratic number held. Then the ring OK of integers forms a lattice in C, and more generally, any ideal a of OK doe� as well. The tori *C/a* constructed in this way are elliptic curves with *cvmple.t multipllmtion*. Thbmeans the following. An endomorphism of an elliptic curve $E =$ IC/I' b given as multiplication by a complex number : such that Zr £: $r.$ Generically, one has End(£)= If this is not the case, then End(£) @ IQ i� necessarily an imaginary quadratic number lleld K, and one �ay� that this is an elliptic curve with complex multiplication. The curve� *IC/a* are obviously of thb kind.

The con�equences of these analytic investigations for cla-.� field theory are the following.

(6.10) Theorem. *Let K* be *an* imagimlfy *quadratic number* field and *a* an idea/ of $_o$ *K*. *Then* one *has:*

(i) *The 1-invariant* i(a) of IC/a i� an *algebraic integer which depends only* on *the ideal c/as.*� J'l of *a. 11nd will* therefore *be denoted by* j(ft).

(ii) *Every* j(a) *generate.� tile Hilben* cla'>'> *field over K.*

(iii) *If* $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ are representatives of *the ideal class group* Cl_K, *then the numbers* $j(\mathfrak{a}_i)$ *are conjugate to one another over* K.

(iv) *For almost all prime ideals* $\mathfrak{p}$ *of* K *one has*

$$\varphi_{\mathfrak{p}} j(\mathfrak{a}) = j(\mathfrak{p}^{-1}\mathfrak{a}),$$

where $\varphi_{\mathfrak{p}} \in G(K(j(\mathfrak{a}))|K)$ *is the* Frobenius *automorphism of a prime ideal* $\mathfrak{P}$ of $K(j(\mathfrak{a}))$ above $\mathfrak{p}$.

Note that for a totally imaginary field K there is no difference between big and small Hilbert class field. In order to go beyond the Hilbert class field, i.e., the ray class field mod 1, to the ray class fields for arbitrary modules $\mathfrak{m} \neq 1$, we form, for any lattice Γ, the Weber function

$$\tau_\Gamma(z) = \begin{cases} -2^7 3^5 \frac{g_2 g_3}{\Delta}\wp(z), & \text{if } g_2 g_3 \neq 0, \\ -2^9 3^6 \frac{g_3}{\Delta}\wp(z)^3, & \text{if } g_2 = 0, \\ 2^8 3^4 \frac{g_2^2}{\Delta}\wp(z)^2, & \text{if } g_3 = 0. \end{cases}$$

Let $\mathfrak{K} \in Cl_K$ be an ideal class chosen once and for all. We denote by $\mathfrak{K}^*$ the classes in the ray class group $Cl_K^{\mathfrak{m}} = J^{\mathfrak{m}}/P^{\mathfrak{m}}$ which under the homomorphism

$$Cl_K^{\mathfrak{m}} \longrightarrow Cl_K$$

are sent to the ideal class $(\mathfrak{m})\mathfrak{K}^{-1}$. Let $\mathfrak{a}$ be an ideal in $\mathfrak{K}$, and let $\mathfrak{b}$ be an integral ideal in $\mathfrak{K}^*$. Then $\mathfrak{a}\mathfrak{b}\mathfrak{m}^{-1} = (a)$ is a principal ideal. The value $\tau_{\mathfrak{a}}(a)$ only depends on the class $\mathfrak{K}^*$, not on the choice of $\mathfrak{a}$, $\mathfrak{b}$ and a. It will be denoted by

$$\tau(\mathfrak{K}^*) = \tau_{\mathfrak{a}}(a).$$

With these conventions we then have the

(6.11) Theorem. (i) *The invariants* $\tau(\mathfrak{K}^*)$, ..., *for a fixed ideal class* $\mathfrak{K}$, *are distinct numbers and are conjugate over the Hilbert class field* $K^1 =$

(ii) *For* $\mathfrak{m}$ *arbitrary* $\mathfrak{K}$, *the* field $K(j(\mathfrak{K}), \tau(\mathfrak{K}^*))$ *is the ray class field* mod $\mathfrak{m}$ *over* K.

K''' � K(iUO. r(Jl'J)

Exercise **J,** Let he the big, and $H|K$ the small Hilbert field. Then G(K1]11):;,: '. where r 1� the number of real place�. and : drl-

Exercise 2. Let $d > 0$ be s4uarefree, and $K =$ Let f he a totally fuml:tmental unit of K. Then one ha� [K 1 : = or = 2. according a� = -1 or=\.

Exercise]. The group (CK)" = $I_K)^n K^*/K^*$ is the intersection of the norm groups $N_{L|K} C_L$ of all abel1an exten�ion $L|K$ of exponent n.

Exercise **4.** For a number field K. local Tate dudiity ("cc chap. V, � I, exere1"c 2) yield� a ,o,-d,,<eo,cmc pairing

(*) $\prod H^1(K_{\mathfrak p}, \mathbb{Z}/n\mathbb{Z}) \times \prod H^1(K_{\mathfrak p}, \mu_n) \to \mathbb{Z}/n\mathbb{Z}$

of locally compact groups, where the restricted products arc taken with re�peet to he subgroups $H^1_{nr}(K_{\mathfrak p}, \mathbb{Z}/n\mathbb{Z})$, resp. $H^1_{nr}(K_{\mathfrak p}, \mu_n)$. For $X = (X_{\mathfrak p})$ in the fir�1 and $\alpha = (\alpha_{\mathfrak p})$ in the second product, it is given by

$$(x, a) = \sum_{\mathfrak p} X_{\mathfrak p}(L|'p, K_{\mathfrak p}|K_{\mathfrak p})$$

(i1) If $L|K$ ha linilc extension. then one ha� a commutative diagram

$$\prod_{\mathfrak P} H^1(L_{\mathfrak P}, \mathbb{Z}/n\mathbb{Z}) \times \prod H^1(L_{\mathfrak P}, \mu_n) \to \mathbb{Z}/n\mathbb{Z}$$

$$\prod_{\mathfrak p} H^1(K_{\mathfrak p}, \mathbb{Z}/n\mathbb{Z}) \times \prod H^1(K_{\mathfrak p}, \mu_n) \to \mathbb{Z}/n\mathbb{Z}.$$

(iii) The images o(

$$H^1(K, \mathbb{Z}/n\mathbb{Z}) \to \prod_{\mathfrak p} H^1(K_{\mathfrak p}, \mathbb{Z}/n\mathbb{Z})$$

and

$$H^1(K, \mu_n) \to \prod H^1(K_{\mathfrak p}, \mu_n)$$

are mutual orthogonal complement� with rc�pec1 to the pairing (*).

Hint for (iii): The cokernel of the �econd map 1� and one ha" $H^1(K, \mathbb{Z}/n\mathbb{Z}) = \operatorname{Hom}(G(L|K), \mathbb{Z}/n\mathbb{Z})$ where $L|K$ 1." maxima! abelian exten"ion of exponent n.

Exercise 5 **((ilobal Tate Dualit�').** Show that the statement" of exercise 4 extend to an arbitrary finite (;A•-module ;\ m�tead of $\mathbb{Z}/n\mathbb{Z}$. and $A' = \operatorname{Hom}(A, \bar{K}^*)$ instead of μ_n.

Hint: u�e exercise" 4-8 of chap. IV, *3, and exercise 4 of chap. V*, 1.

Exerci�e 6. It S is a linite "et of place� of K, then the mdp

$$H^1(K, \mathbb{Z}/n\mathbb{Z}) \to \bigoplus H^1(K_{\mathfrak p}, \mathbb{Z}/n\mathbb{Z})$$

is surjective if and only if the map

$$H^1(K,\mu_n) \to \prod H^1(K_p,\mu_n)$$

is injective. This is the case in ifc1thcr the exten"mn IIK i, cyclic, $n = 2^r m$, $(m, 2) = 1$, or if S not contain all place� pl2 arc nonspl1t in $K(\mu_{2^r})$ (see § 1, exercise 2).

1<:xercise 7 (Theorem of GRLNw111J). If the la�l condiuon of exercise 6 i\ \ati�lied for the triple then. extensions $l,\mu_{\mathfrak p}$ KP for p E S, there ex1\ts a has tplKμ a� a completion for p ES, whJCh satisfies the identity of degrees

$$[L : K] = \mathrm{scm}\{[L_{\mathfrak p} : K_{\mathfrak p}]\}$$

(�ee abo [!OJ. chap. X, *2)

Note: Let G be a finite group of order prime to $\#\mu(K)$, let She a finite \et or places, and let $L\mu_{\mathfrak p}$ $K_{\mathfrak p}$, p E S, be given Gal01s exten�1on, whose Galoi� groups c;P can he embedded into G. Then there exi�t\ a Galo1., cxlcmion LI K which on the one hand has Galois isomorphil· to G. and which on the other hand has the given extensions .i.., completion� ("ee 1109]).

§ 7. The Ideal-Theoretic Version of Class Field Theory

Class field theory has found its idele-theore1ic formulation only after it had been completed in the language of ideals. f-irom the very start, it was guided by the desire to clas"ify all abelian exten"ions of a number field K. But al first, instead of the ide!e class group C_K, there wa� only the ideal ela�:c. group Cl_K at hand to do thi�. along with its subgroups. In tenn� of the insights that we have gained in the preceding section, thil> means the restriction to the subfields of the Hilbert class field, i.e., to the *unramificd* abelian cxtcnsionl> of K. if the base llcld is Q, this restriction il> of course radical, for Q ha� no unramitied extension:c. at all by Minkow"ki\, theorem. But over :Q. we naturally encounter the cyclotomic fields Q(Jlmll:Ql with their familiar isomorphi�ms G(Q(11m)IIQ) ;,: Hut,'R1(·11 WF11n1 realized, a� was already mentioned, that the groups and (Z/111Z)* are - with a grain of salt - only different in�tances of a common concept, that of a ray c]a�., group, which he defined in an ideal-theoretic way a� the quotient group

$$Cl_K^{\mathfrak m} = J^{\mathfrak m}/P^{\mathfrak m}$$

of all ideals relatively prime lo a given module m, by the principal ideals (a) with $a \equiv 1 \bmod \mathfrak m$, and a totally positive. He conjectured that this group $Cl_K^{\mathfrak m}$, along with its ._ubgroup�. would do the same for the �ubextemions of a "ray class field" $K^{\mathfrak m}|K$ (which at first \¼a� only po<,tula!cd lo exist) al> the ideal dal>s group *CIK* and ih �ubgroups did for the wblield� of the Hilhert cla�., (icld. Moreover. he �tated the hypothesis that every abclian extension ought lo be captured by such a ray cla5s field, as wa� rngge�ted by the case where the ba�e field is Q, whose abelian extensions are all contained in cyclotomic fields by the Kronecker-Weber theorem. After the seminal work of the mathematician *P111ut'I' FcRnVANG!FR* 144], these conjecture� were confirmed the Japanese arithmetician *Tn.11 TAKA<a* (1875-1960), and cast by *EMIL* (1898-1962) into a definite, canonical form.

The idelc-theoretic language introduced by *Cm v.1LLH* brought the simplification that the idcle da�s group *CK* encapsulated all abelian extcn�ion� of LI *K* at once, avoiding choosing a module m every time such an extension was given, in order to accommodate it into the ray cla�f> field *KmiK,* and thereby make it amenable to class field theory. The classical point of view can be vindicated in term5 of the idele-theoretic version by looking at congruence �ubgroup5 *CK* in *CK,* which detlne the ray clasf> field5 *KmlK.* Their wbfields correspond, according to the new point of view, to the groups between *CK* and *CK,* and hence, in view of the isomorphism

CK/CK �Cl';_.

tothe subgroups of the ray class group *Cl!(.*

In what follows, we want to deduce the clas5ical, ideal-theoretic ver5ion of global class field theory from the idcle-theoretic one. Thi� i� not only an obligation towards history, but a factual necessity that If, forced upon ut, by the numerous applications of the more elementary and more immediately accessible ideal group�.

Let LI *K* be an abelian extension, and let p be an unramified prime ideal of *K* and 'l3 a prime ideal of *L* lying above p. The decompo�ition group G(L<+1IKp) £ *G(LIK)* i� then generated by the cla�5ical **Frobenius automorphism**

$$\varphi_{\mathfrak p} = (\pi_{\mathfrak p}, L_{\mathfrak P}|K_{\mathfrak p}),$$

where Jtp is a prime clement of Kp. As an automorphism of *L*, (,Op is obviou�ly characterized by the congruence

(,Opt.I = *c/f* mod 'l3 for all *a* E *OL*

where *q* is the number of element� in the re1>idue class field of p. We put

$$\varphi_{\mathfrak p} =: \left(\frac{L\,|\,K}{\mathfrak p}\right).$$

Now let $\mathfrak{m}$ be a module of K such that L lies in the ray class field mod $\mathfrak{m}$. Such a module is called a **module of definition** for L. Since by (6.6) each prime ideal $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in L, we get a canonical homomorphism

$$\left(\frac{L|K}{\ }\right) : J^{\mathfrak{m}} \to G(L|K)$$

from the group $J^{\mathfrak{m}}$ of all ideals of K which are relatively prime to $\mathfrak{m}$ by putting, for any ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$:

$$\left(\frac{L|K}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}} \left(\frac{L|K}{\mathfrak{p}}\right)^{\nu_{\mathfrak{p}}}.$$

$\left(\frac{L|K}{\ }\right)$ is called the **Artin symbol.** If $\mathfrak{p} \nmid \mathfrak{m}$ is a prime ideal and $\pi_{\mathfrak{p}}$ a prime element of $K_{\mathfrak{p}}$, then clearly

$$\left(\frac{L|K}{\mathfrak{p}}\right) = ((\pi_{\mathfrak{p}}), L|K),$$

if $(\pi_{\mathfrak{p}}) \in C_K$ denotes the class of the idèle $(\dots, 1, 1, \pi_{\mathfrak{p}}, 1, 1, \dots)$.

The relation between the idele-theoretic and the ideal-theoretic formulation of the Artin reciprocity law is now provided by the following theorem.

(7.1) Theorem. *Let $L|K$ be an abelian extension, and let $\mathfrak{m}$ be a module of definition for it. Then the Artin symbol induces a surjective homomorphism*

$$\left(\frac{L|K}{\ }\right) : J^{\mathfrak{m}}/P^{\mathfrak{m}} \to G(L|K)$$

with kernel $H^{\mathfrak{m}}/P^{\mathfrak{m}}$, where $H^{\mathfrak{m}} = (N_{L|K} J_L^{\mathfrak{m}}) P^{\mathfrak{m}}$, and we have an exact commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & N_{L|K}C_L \arrow[r] \arrow[d] & C_K \arrow[r] \arrow[d] & G(L|K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H^{\mathfrak{m}}/P^{\mathfrak{m}} \arrow[r] & J^{\mathfrak{m}}/P^{\mathfrak{m}} \arrow[r] & G(L|K) \arrow[r] & 1.
\end{tikzcd}$$

Proof: In § 1, we obtained the isomorphism $\phi: C_K/C_K^{\mathfrak{m}} \to Cl_K^{\mathfrak{m}} = J^{\mathfrak{m}}/P^{\mathfrak{m}}$ by sending an idele $\alpha = (\alpha_{\mathfrak{p}})$ to the ideal $(a) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$. This isomorphism yields a commutative diagram

$$\begin{tikzcd}
C_K/C_K^{\mathfrak{m}} \arrow[r] \arrow[d, "\phi"] & G(L|K) \arrow[d, "\mathrm{id}"] \\
Cl_K^{\mathfrak{m}} \arrow[r, "\psi"] & G(L|K),
\end{tikzcd}$$

and we show that ψ is given by the Artin symbol.

Let p be a prime ideal not dividing m. JTp a prime clement of Kp, and *c ECK/Cf.!* the cla�s of the idClc (rrp} = (. I, l.JTp, l, I, ...). Then *(c)* = p mod *Pt* and

i((cJ)�(c,LIKJ�((rr,).LIK)�(L p IK.)

Thi� shows that *f: JK/PJF--+ G(LIK)* is induced by the Artin symbol *(!c..lK) : Jf(--+* G(L IK), and that il is surjective.

It remain� to �how that the image of *NL KCr.* under the map ( ) *CK* ➔ *JK / Pf* is the group H'n/ *Pp.* We view the module m = Tiptc,., pnP m, a module of *L* by wbstituting for each prime ideal p of *K* the product p = n".1-llP 'P"•+<i". As in the proof of (1.9). we then get *CL= I{m)L*/L**, where t},m) = {a E *IL* I *U<,p* E for 'Plmcx:i}. The clements of

NLIKCL = Nr.1Kulm¹)K/K.,*

are the classes of norm idelcs *NLIK* (a). for *a* E t{ml. As

NL K(U)p = TI *NL,+,* K,,(a13)
':PIP

(see (2.2)), and since *vp(NL'll* Kµ(ai;p)) = (.�cc chap. III. (1.2)). the idele *Ni.iK* (a) is mapped by ( ) to the

(N11K(a))= =*NLK(* n -.µv,p(a,pl).
'+Jt,x.

Therefore the image of *N1.1KCL* under the homomorphism (: *CK* ---+ *J'f//Pr;,* is precisely the group *(NL1KlfJPR'JP;'*, q.e.d. D

(7.2) **Corollary.** *The A1ti11* symbol (***L∕).*** fi_1r a E *1;-, only* depends *on the* c/as� *a* mod *P'JF". It deJincs* an isomorphism

(IJ.".) *Jt/Hm* __::_, *G(LIK).*

The group Hm = *(N1.1KJt)P;'* is called the *"idea{ group defined* mod m" helonging to the extension tIK. From the existence theorem (6.1). we sec that the correspondence /, i---+ *Hm* is 1-1 between subcxtensions of the ray cla% field mod m and c.;uhgroups of *1;;'* containing *P;'.*

The most important consequence of theorem (7. l) is a precise ana[y5i5 of the kind of decomposition of any unramified prime ideal p in an abelian extension LI *K.* It can be immediately read off the ideal group *H*m s*r;* which determines the field *L* as class field.

(7.3) Theorem (Decomposition Law). *Let $L|K$ be an abelian extension of degree n, and let $\mathfrak{p}$ be an unramified prime ideal. Let $\mathfrak{m}$ be a module of definition for $L|K$ that is not divisible by $\mathfrak{p}$ (for instance the conductor), and let $H^{\mathfrak{m}}$ be the corresponding ideal group.*

If f is the order of $\mathfrak{p}$ mod $H^{\mathfrak{m}}$ in the class group $J^{\mathfrak{m}}/H^{\mathfrak{m}}$, i.e., the smallest positive integer such that

$$\mathfrak{p}^f \in H^{\mathfrak{m}},$$

then $\mathfrak{p}$ decomposes, in L, into a product

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

of $r = n/f$ distinct prime ideals of degree f over $\mathfrak{p}$.

Proof: Let $\mathfrak{p} = \mathfrak{P}_1 \cdots$, be the prime decomposition of $\mathfrak{p}$ in L. Since $\mathfrak{p}$ is unramified, the $\mathfrak{P}_i$ are all distinct and have the same degree f. This degree is the order of the decomposition group of $\mathfrak{P}_i$ over K, i.e., the order of the Frobenius automorphism $\varphi_{\mathfrak{p}} = (\frac{L|K}{\mathfrak{p}})$. In view of the isomorphism $J^{\mathfrak{m}}/H^{\mathfrak{m}} \cong G(L|K)$, this is also the order of $\mathfrak{p}$ mod $H^{\mathfrak{m}}$ in $J^{\mathfrak{m}}/H^{\mathfrak{m}}$. This finishes the proof. □

The theorem shows in particular that the prime ideals which split completely are precisely those contained in the ideal group $H^{\mathfrak{f}}$, if $\mathfrak{f}$ is the conductor of $L|K$.

Let us highlight two special cases. If the base field is $K = \mathbb{Q}$ and we look at the cyclotomic field the conductor is the module $\mathfrak{m} = (m)$, and the ideal group corresponding to $\mathbb{Q}(\mu_m)$ in $J_{\mathbb{Q}}^{\mathfrak{m}}$ is the group $P_{\mathbb{Q}}^{\mathfrak{m}}$. As $J_{\mathbb{Q}}^{\mathfrak{m}}/P_{\mathbb{Q}}^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^*$ (see we obtain for the decomposition of rational primes $p \nmid m$, the law which we had already deduced in chap. I, (10.4), and in particular the fact that the prime numbers which split completely are characterized by

$$p \equiv 1 \bmod m.$$

In the case of the Hilbert class field $L|K$, i.e., of the field inside the ray class field mod 1 in which the infinite places split completely, the corresponding ideal group $H \subseteq J_K = J_K$ is the group P_K of principal ideals (see (6.9)). This gives us the strikingly simple

(7.4) Corollary. *The prime ideals of K which split completely in the Hilbert class field are precisely the principal prime ideals.*

Another highly remarkable property of the Hilbert class field is expressed by the following theorem, known as the **principal ideal theorem.**

(7.5) Theorem. *In the Hilbert class field every ideal $\mathfrak{a}$ of K becomes a principal ideal.*

Proof: Let $K_1|K$ be the Hilbert class field of K and let $K_2|K_1$ be the Hilbert class field of K_1. We have to show that the canonical homomorphism

$$J_K/P_K \longrightarrow J_{K_1}/P_{K_1}$$

is trivial. By chap. IV, (5.9), we have a commutative diagram

$$\begin{tikzcd} C_{K_1}/N_{K_2|K_1}C_{K_2} \arrow[r] & G(K_2|K_1) \\ C_K/N_{K_1|K}C_{K_1} \arrow[r] \arrow[u, "i"] & G(K_1|K), \arrow[u, "\mathrm{Ver}"'] \end{tikzcd}$$

where i is induced by the inclusion $C_K \subseteq C_{K_1}$. It is therefore enough to show that the transfer

$$\mathrm{Ver} : G(K_1|K) \longrightarrow G(K_2|K_1)$$

is the trivial homomorphism. Since $K_1|K$ is the maximal unramified abelian extension of K in which the infinite places split completely, i.e., the maximal abelian subextension of $K_2|K$, we see that $G(K_2|K_1)$ is the commutator subgroup of $G(K_2|K)$. The proof of the principal ideal theorem is thus reduced to the following purely group-theoretic result. $\square$

(7.6) **Theorem.** *Let G be a finitely generated group, G' its commutator subgroup, and G'' the commutator subgroup of G'. If $(G : G') < \infty$, then the transfer*

$$\mathrm{Ver}: G/G' \longrightarrow G'/G''$$

is the trivial homomorphism.

We give a proof of this theorem which is due to ERNST WITT [141]. In the group ring $\mathbb{Z}[G] = \{\sum n_\sigma \sigma \mid n_\sigma \in \mathbb{Z}\}$, we consider the **augmentation ideal** I_G, which is by definition the kernel of the ring homomorphism

$$\mathbb{Z}[G] \longrightarrow \mathbb{Z}, \quad \sum n_\sigma \sigma \longmapsto \sum n_\sigma ,$$

For every subgroup H of G, we have $I_H \subseteq I_G$, and $\{\tau - 1 \mid \tau \in H,\ \tau \neq 1\}$ is a $\mathbb{Z}$-basis of I_H. We first establish the following lemma, which also has independent interest in that it gives an additive interpretation of the transfer.

(7.7) **Lemma.** *For every subgroup H of finite index in G, one has a commutative diagram*

$$\begin{tikzcd} G/G' \arrow[r, "\mathrm{Ver}"] \arrow[d, "\delta", "\wr"'] & H/H' \arrow[d, "\delta", "\wr"'] \\ I_G/I_G^2 \arrow[r, "S"] & (I_H + I_G I_H)/I_G I_H, \end{tikzcd}$$

where the homomorphisms δ are induced by $\sigma \mapsto \delta\sigma = \sigma - 1$, and the homomorphism S is given by

$$S(x \bmod I_G^2) = x \sum_{\rho \in R} \rho \bmod I_G I_H,$$

for a system of representatives of the left cosets $R \ni 1$ of G/H.

Proof: We first show that the homomorphism

$$H/H' \xrightarrow{\delta} (I_H + I_G I_H)/I_G I_H \tag{*}$$

induced by $\tau \mapsto \delta\tau = \tau - 1$ has an inverse. The elements $\rho\delta\tau$, $\tau \in H$, $\tau \neq 1$, $\rho \in R$, form a $\mathbb{Z}$-basis of $I_H + I_G I_H$. Indeed, it follows from

$$\rho\delta\tau = \delta\tau + \delta\rho\delta\tau$$

that they generate $I_H + I_G I_H$, and if

$$0 = \sum_{\rho,\tau} n_{\rho,\tau}\rho\delta\tau = \sum_{\rho,\tau} n_{\rho,\tau}\rho(\tau - 1) = \sum_{\rho,\tau} n_{\rho,\tau}\rho\tau - \sum_{\rho}\Big(\sum_{\tau} n_{\rho,\tau}\Big)\rho,$$

then we conclude that $n_{\rho,\tau} = 0$ because the $\rho\tau$, ρ are pairwise distinct. Mapping $\rho\delta\tau$ to $\tau \bmod H'$, we now have a surjective homomorphism

$$I_H + I_G I_H \longrightarrow H/H'.$$

It sends $\delta(\rho\tau')\delta\tau \in I_G I_H$ to $\tau'\tau\tau'^{-1}\tau^{-1} \equiv 1 \bmod H'$ because $\delta(\rho\tau')\delta\tau = \rho\delta(\tau'\tau) - \rho\delta\tau' - \delta\tau$. It thus induces a homomorphism which is inverse to (*). In particular, if $H = G$, we obtain the isomorphism $G/G' \cong I_G/I_G^2$.

The transfer is now obtained as

$$\mathrm{Ver}(\sigma \bmod G') = \prod_{\rho \in R} \sigma_\rho \bmod H',$$

where $\sigma_\rho \in H$ is defined by $\sigma\rho = \rho'\sigma_\rho$, $\rho' \in R$. Ver thus induces the homomorphism

$$S : I_G/I_G^2 \longrightarrow (I_H + I_G I_H)/I_G I_H$$

given by $S(\delta\sigma \bmod I_G^2) = \sum_{\rho\in R}\delta\sigma_\rho \bmod I_G I_H$. From $\sigma\rho = \rho'\sigma_\rho$ follows the identity

$$\delta\rho + (\delta\sigma)\rho = \delta\sigma_\rho + \delta\rho' + \delta\rho'\delta\sigma_\rho .$$

Since ρ' runs through the set R if ρ does, we get as claimed

$$S(\delta\rho \bmod I_G^2) = \sum_{\rho\in R}\delta\sigma_\rho = \sum_{\rho\in R}(\delta\sigma)\rho = \delta\sigma\sum_{\rho\in R}\rho \bmod I_G I_H . \qquad \square$$

Proof of theorem (7.6): Replacing G by G/G'', we may assume that $G'' = \{1\}$, i.e., that G' is abelian. Let $R \ni 1$ be a system of representatives of left cosets of G/G', and let $\sigma_1, \dots, \sigma_n$ be generators of G. Mapping $e_i = (0,\dots,0,1,0,\dots,0) \in \mathbb{Z}^n$ to σ_i, we get an exact sequence

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{\ f\ } \mathbb{Z}^n \longrightarrow G/G' \longrightarrow 1,$$

where f is given by an $n\times n$-matrix (m_{ik}) with $\det(m_{ik}) = (G:G')$. Consequently,

$$\prod_{i=1}^{n}\sigma_i^{m_{ik}}\tau_k = 1 \quad \text{with} \quad \tau_k \in G' .$$

The formulae $\delta(xy) = \delta x + \delta y + \delta x\,\delta y$, $\delta(x^{-1}) = -(\delta x)x^{-1}$ yield by iteration that

$$\delta\Big(\prod_{i=1}^{n}\sigma_i^{m_{ik}}\tau_k\Big) = \sum_{i=1}^{n}(\delta\sigma_i)\mu_{ik} = 0,$$

where $\mu_{ik} \equiv m_{ik} \bmod I_G$. In fact, the τ_k are products of commutators of the σ_i and σ_i^{-1}. We view (μ_{ik}) as a matrix over the commutative ring

$$\mathbb{Z}[G/G'] \cong \mathbb{Z}[G]/\mathbb{Z}[G]I_{G'},$$

which gives a meaning to the determinant $\mu = \det(\mu_{ik}) \in \mathbb{Z}[G/G']$. Let (λ_{kj}) be the adjoint matrix of (μ_{ik}). Then

$$(\delta\sigma_j)\mu = \sum_{i,k}(\delta\sigma_i)\mu_{ik}\lambda_{kj} \equiv 0 \bmod I_G\mathbb{Z}[G]I_{G'},$$

so that $(\delta\sigma)\mu \equiv 0 \bmod I_G\mathbb{Z}[G]I_{G'} = I_G I_{G'}$ for all σ. This yields

$$\mu \equiv \sum_{\rho\in R}\rho \bmod \mathbb{Z}[G]I_{G'} .$$

For if we put $\mu = \sum_{\rho\in R} n_\rho\bar\rho$, where $\bar\rho = \rho \bmod G'$, then for all $\bar\sigma \in G/G'$,

$$\bar\sigma\mu = \sum_\rho n_\rho\,\bar\sigma\bar\rho =$$

This implies that **all** *nf* are equal, hence */L* = *m L,P"R p* mod Z[GJ/c;, and

$$\mu, =\det(m;A\} = ((J: G^1) = m(G: C.;') \text{ mOO } le;,$$

we even have m = I. Applying now lemma (7.7). we sec that the transfer i� the trivial homomorphism since

$$S(8a \bmod !J) = Ocr_{L,\ pct/}\ p = (!ia)tL = 0 \bmod /GIG'\bullet \qquad D$$

A problem which i� closely related to the principal ideal theorem and which wa� first put forward by *P1111 II'!' FvRrnAi'H;U:R* is the **problem of the** class **field tower.** This i� the question whether the class field tower

$$K = Ko£" \ Ki£" \ K2 \ £" \ K, \ £".$$

where $Ki+i$ is the Hilbert class field of $K,$. stops after a finite number of sleps. A positive amwer would have the implication that the last field in the tower had cla�s number I *w* that in it not only the ideals of *K.* but in fact all its ideals become principal. Thi,; perspective naturally generated the greate�t intere�t. But the problem. after withstanding for a long time all attempts to �olve it, was finally decided in the negative by the Russian mathematicians *E.S.Gmon* and *I.R. S,11ARn1t* in 1964 (see [48).]241).

Exercise **1.** The deeompo.\ition Jaw for the prime ideals p which arc *1w11(fied* m an abelian *L* IK can be torrnulated like this. Let f be the conductor of LI *K,* Hr the ideal group for *L.* and //p the \Jnalle�t ideal group containing //f ot prime top.

It r = (Hp : // f) and p¹ i\ the smallc�t pov.-er or p which belong\ to *Hp,* then

p � ('!l, .. ·'!l,J"

where the �' are of deg-rec *f* over *K.* and 1 = 11 = IL : KI.

Hint: The etas� tield for *Hp* i� the inertia tield above p.

The rollowing exercbe� 2-6 concern a non-abdian example of *E. Au11.*�-

Exercise 2. The polynomial = *X'* *X* + ! i\ irreducible. The dt�criminant of a root *a* (1.e., the d1\cnmirnmt i\ *d* = 19 • 151.

Hint: The d1�criminant of ,1 root of *X'* + *aX* +hi\ *S'h⁴* + 2⁸u¹.

Exercise J. Let *k* ={):'(a). Then Z[a] i� the rmg *o,* of integer\ of/.:..

Hint: The d1�ernnin,m! of Zia I e4uab the di�crirnmant of because on the one hand, both differ only hy a and on the other 11 1., ,4u.1rel'rec. The tran�ition matrix trom 1.a, to an intcgrnl ba�i, w1, or c1, is therefore invertible over

Exercise **4.** The dccompo�ition field K 10' of {(X) ha� as G;;lois group the symmetric group 6_1, i.e.. it i� of degree 120.

Exercise 5. K has cla�� number I.

Hint: Show, using chap. exercise 3. that every ideal c!a�s of K contains an ideal a with \Jt(a) < 4. then a ha� to be a pnme ideal p such that 'Jt(p) $=$ 2 or 3. Hence or $=$ Z/3Z, so f ha� a root mod 2 or 3. which is not the case.

Exercise **6.** Show that K I Qi(v'197sf) i� a (non-abclian!) unramilied extension.

Exercise 7, For every Glllois cxten�ion LIK of finite numher field.�. there exist infinitely many finite exten�1on� K' �uch that $K' = K$. and �uch that LK^1IK' 1� unramified.

Hint: Let S be the �et of ramified in LIK. and let $=$ Kp(ap). By the approximation theorem, an algebraic number a every p E S, is clo�c to when embedded into Kr· Then ,;;; Kp(a) by Kra�ncr'� lemma, chap. **11,** exerci�e 2. Put $K' = K(a)$ and that $LK'IK'$ is unramified. Tu �how that a can be chmen �uch that L n $K' = K$ use CU). and the fact that G(LIK) i� generated by elements of prime power order.

§ 8. The Reciprocity Law of the Power Residues

In cla�s field theory Gaus:;.'s reciprocity law meets its mo�t general and definite formulation. Let n be a positive integer :::_ 2 and K a number field containing the group JL_{11} of 11-th roots of unity. In chap. V, �3, we introduced, for every place).J of K, then-th Hilbert �ymbol

$$(\text{�}) \quad : K; \times K; \to JL_{11} \cdot$$

It is given via the norm residue symbol by

$$(a, Kp(V'h) / Kp) \ 'v'h'' = p^{('' \cdot h)} \ 'v'h''.$$

Thc�e symbols all fit together in the following *productfonnula.*

(8.1) Theorem. *For* a, h E K^* one *has*

$$\prod_{\mathfrak{p}} \left(\frac{a, b}{\mathfrak{p}} \right) = 1$$

Proof: From (5.7), wc find

$$\Big[\prod_{\mathfrak p}\Big(\frac{a,b}{\mathfrak p}\Big)\Big]\sqrt[n]{b}=\Big[\prod_{\mathfrak p}(a,K_{\mathfrak p}(\sqrt[n]{b})|K_{\mathfrak p})\Big]\sqrt[n]{b}=\big(a,K(\sqrt[n]{b})|K\big)\sqrt[n]{b}=\sqrt[n]{b},$$

and hence the theorem. □

In chap. V, S3, we defined then-th power residue symbol in terms of the Hilbert symbol:

$$\Big(\frac{a}{\mathfrak p}\Big)=\Big(\frac{\pi,a}{\mathfrak p}\Big),$$

where *p* is a prime ideal of *K* not dividing *n, a* E Up, and rr is a prime element of *K11*. We have seen that this definition does not depend on the choice of the prime element *n* and that one has

$$\Big(\frac{a}{\mathfrak p}\Big)=1\iff a\equiv\alpha^n \bmod \mathfrak p,$$

and more generally

(�)=a(q-l)/nmodμ, q=lJl(μ).

(8.2) Definition. *For eve1y ideal* b = npfn μ¹ₚ *prime* to *n, 1111d every* number *a prime* to b, we *define then-th* power residue symbol *by*

$$\Big(\frac{a}{\mathfrak b}\Big)=\prod_{\mathfrak p\nmid n}\Big(\frac{a}{\mathfrak p}\Big)^{\nu_{\mathfrak p}}$$

Here (;)vp = I *when* l!p = 0.

The power residue symbol (*) is obviously multiplicative in both argument�. If bis a principal ideal *(h),* we write for �hurt(*) = (Ti). We now prove the general reciprocity law for then-th power residues.

(8.3) Theorem. *If a, h* E *K** are *prime to each other and* to *n. then*

$$\Big(\frac{a}{b}\Big)\Big(\frac{b}{a}\Big)^{-1}=\prod_{\mathfrak p|n\infty}\Big(\frac{a,b}{\mathfrak p}\Big)$$

Proof: If p is prime to /moo, then we have

$$\left(\frac{b}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)} = \left(\frac{\pi, b}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)} = \left(\frac{a, b}{\mathfrak{p}}\right),$$

where JT i'> a prime element of *Kμ*. Fur if we p_ut *a* $=$ *un"μia*, then (¥) $=$ I because *u.h* E *Up*. For the same reason, we find

p("·") = I .!or p prime to *a/moo.*

(8.1) then gives

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|(b)} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \prod_{\mathfrak{p}|(a)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_{\mathfrak{p}}(a)} = \prod_{\mathfrak{p}|(b)} \left(\frac{b, a}{\mathfrak{p}}\right) \prod_{\mathfrak{p}|(a)} \left(\frac{a, b}{\mathfrak{p}}\right)^{-1}$$
$$= \prod_{\mathfrak{p}|(ab)} \left(\frac{b, a}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}\nmid n\infty} \left(\frac{b, a}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}|n\infty} \left(\frac{a, b}{\mathfrak{p}}\right).$$

Here t:il(h) mcam that p occurs in the prime decomposition of *(h).* n

Gauss's reciprocity law, for which we gave an elementary proof using the theory of Gau�s sums in chap. I, (8.6), in the case of two odd prime number� *p, l,* is contained in the general reciprocity law (8.3) as a case. For if we substitute, in the case K $=$ ::]), $n = 2$, into formula the explicit description (chap. V, (3.6)) of the Hilbert symbol(¥) for$p = 2$ and $p =$ oo, we obtain the following theorem, which is more general than chap. **I,** (8.6).

(8.4) Gauss's **Reciprocity Law.** Let K $=$ Ql, $n = 2$, and *let a* ;md *h be odd, relatively prime integers. Then* one ha�

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}(-1)^{\frac{\operatorname{sgn} a-1}{2}\frac{\operatorname{sgn} b-1}{2}},$$

and for *positive odd integer.� h,* we *have the* two *·\uppleme11t:1ry thcorem8"*

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) =$$

For the last equalion we need again the product fommla:

$$\left(\frac{2}{b}\right) = \prod_{p \neq 2, \infty} \left(\frac{p, 2}{p}\right)^{v_p(b)} = \prod_{p \neq 2, \infty} \left(\frac{b, 2}{p}\right) = \left(\frac{2, b}{2}\right)\left(\frac{2, b}{\infty}\right) = (-1)^{\frac{b^2-1}{2}}$$

The symbol $(*)$ is called the **Jacobi symbol,** or abo the **quadratic residue symbol** (although, for h not a prime number, the condition that the symbol $(*) =$ I is no longer equivalent to the condition that a i� a quadratic re�idue modulo h).

In the above formulation, the reciprocity law allows us to compute simply by iteration the quadratic residue symbol $(*)$, as is shown in the following example:

$$\left(\frac{40077}{65537}\right) = \left(\frac{65537}{40077}\right) = \left(\frac{25460}{40077}\right) = \left(\frac{2''}{40077}\right)\left(\frac{6365}{40077}\right) = \left(\frac{40077}{6365}\right) =$$

$$\left(\frac{1887}{6365}\right) = \left(\frac{6365}{1887}\right) = \left(\frac{704}{1887}\right) = \left(\frac{4'}{1887}\right)\left(\frac{II}{1887}\right) = -\left(\frac{1887}{II}\right) =$$

-(�)�-(�)(M �(M�-(*)�-w� 1

Clas� tield theory originated from Gauss's reciprocity law. The quest for a similar law for the n-th power residues dominated number theory for a long time, and the all-embracing an�wcr wa� finally found in Artin\, reciprocity law. The above reciprocity law (8.3) of the power residues now appears as a simple and special comequence of Artin 's reciprocity law. But to really settle the original problem, class tield theory was still lacking the explicit computation of the Hilbert �ymbols (¥) for plnoc. Thi� was tinally completed in the I 960s by the mathematician *Hi 1.Aw1 B1u CK,\•JoR,* chap. V, (3.7).

Chapter VII

Zeta Functions and L-series

§ 1. The Riemann Zeta Function

One of the most astounding phenomena in number theory consists in the fact that a great number of deep arithmetic properties of a number field are hidden within a single analytic function, its zeta function. This function has a simple shape, but it is unwilling to yield its mysteries. Each time, however, that we succeed in stealing one of these well-guarded truths, we may expect to be rewarded by the revelation of some surprising and significant relationship. This is why zeta functions, as well as their generalizations, the L-series, have increasingly moved to the foreground of the arithmetic scene, and today are more than ever the focus of number-theoretic research. The fundamental prototype of such a function is Riemann's zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where s is a complex variable. It is to this important function that we turn first.

(1.1) Proposition. *The series* $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ *is absolutely and uniformly convergent in the domain* $\mathrm{Re}(s) \geq 1 + \delta$, *for every* $\delta > 0$. *It therefore represents an analytic function in the half-plane* $\mathrm{Re}(s) > 1$. *One has Euler's identity*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

where p runs through the prime numbers.

Proof: For $\mathrm{Re}(s) = \sigma \geq 1+\delta$, the series $\sum_{n=1}^{\infty} |1/n^s| = \sum_{n=1}^{\infty} 1/n^\sigma$ admits the convergent majorant $\sum_{n=1}^{\infty} 1/n^{1+\delta}$, i.e., $\zeta(s)$ is absolutely and uniformly convergent in this domain. In order to prove Euler's identity, we remind ourselves that an infinite product $\prod_{n=1}^{\infty} a_n$ of complex numbers a_n is said to converge if the sequence of partial products $P_n = a_1 \cdots a_n$ has a nonzero limit. This is the case if and only if the series $\sum_{n=1}^{\infty} \log a_n$ converges, where $\log$ denotes the principal branch of the logarithm (see [2], chap. V, 2.2). The product is called absolutely convergent if the series converges absolutely. In this case the product converges to the same limit even after a reordering of its terms a_ν.

Let us now formally take the logarithm of the product

$$E(s) = \prod_p \frac{1}{1-p^{-s}}.$$

We obtain the series

$$\log \prod_p \frac{1}{1-p^{-s}} = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}}.$$

It converges absolutely for $\mathrm{Re}(s) = \sigma \geq 1+\delta$. In fact, since $|p^{ns}| = p^{n\sigma} \geq p^{n(1+\delta)}$, one has the convergent majorant

$$\sum_p \sum_n \Big(\frac{1}{p^{1+\delta}}\Big)^n = \sum_p \frac{1}{p^{1+\delta}-1} \leq 2 \sum_p \frac{1}{p^{1+\delta}}.$$

This implies the absolute convergence of the product

$$E(s) = \prod_p \frac{1}{1-p^{-s}} = \exp\Big(\sum_p \Big(\sum_{n=1}^{\infty} \frac{1}{np^{ns}}\Big)\Big).$$

In this product we now expand the product of the factors

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots$$

for all prime numbers $p_1, \dots, p_r \leq N$ and obtain the equality

$$(*) \qquad \prod_{p \leq N} \frac{1}{1-p^{-s}} = \sum_{\nu_1,\dots,\nu_r=0}^{\infty} \frac{1}{(p_1^{\nu_1} \cdots p_r^{\nu_r})^s} = \sum_n{}' \frac{1}{n^s},$$

where $\sum'$ denotes the sum over all natural numbers which are divisible only by prime numbers $p \leq N$. Since the sum $\sum'$ contains in particular the terms corresponding to all $n \leq N$, we may also write

$$\prod_{p \leq N} \frac{1}{1-p^{-s}} = \sum_{n \leq N} \frac{1}{n^s} + \sum_{n>N}{}' \frac{1}{n^s}.$$

Comparing now in $(*)$ the sum $\sum'$ with the series $\zeta(s)$, we get

$$\Big| \prod_{p \leq N} \frac{1}{1-p^{-s}} - \zeta(s) \Big| \leq \Big| \sum_{n>N} \frac{1}{n^s} \Big| \leq \sum_{n>N} \frac{1}{n^{1+\delta}},$$

where the right hand side goes to zero as $N \to \infty$ because it is the remainder of a convergent series. This proves Euler's identity. $\square$

Euler's identity expresses the law of unique prime factorization of natural number1, in a 1,inglc equation. Thi1, already demonstrates the number-theoretic &ignificance of the zeta function. It challenge,; us to study its propertie" more clo5ely. By its definition. the function is only given on the half-plane Re(s) > I. It does, however, admit an analytic continuation to the whole complex plane, with the point $s = 1$ removed, and it satisfies a functional equation which relate1, the arguments to the argument I - *s.* The1,e crucial fact<, will be proved next. The proof hinge<s on an integral formula for the zeta function ((s) which arises from the well-known gamma function. This latter is defined for Re(s) > 0 by the absolutely convergent integral

$$\Gamma(s) = \int_0^{\infty} e^{-y} y^s \frac{dy}{y}$$

and obcy1, the follo\\--ing rules (,;cc [341, vol. I, chap. I).

(1.2) Proposition. (i) *The gamma* function *is analytic* and admits *a merommphic continuation to all* ofC.

(ii) *II is nowhere :-ero and has 1,imp/c poles al s = -n, n =* 0, I, 2, .. , *with* residues (-1)"/*n*!. *There are no* poles *anywhere* else.

(iii) *11 sati1,fies the fonclional equations*

I) r(-1 + 1) =*-1I'(s),*

2) *I'(s)I'(I* - s) = �i��"ri-,

3) *I'(s)I'(s* + ½) = -2*f* *I'(2s)* (Legendre's duplication formula).

(iv) *JI ha1, the special values* I'(l/2) = *fa,* I'(I) = I, *I'(k* + 1) = k!, *k* � 0, 1.2,

To relate the gamma function to the Leta function. start with the 1,ubstitution *y* f—;- rr11^2*y,* which gives the equation

$$\pi^{-s}\Gamma(s)\frac{1}{n^{2s}} = \int_0^{\infty} e^{-\pi n^2 y} y^s \frac{dy}{y}$$

Now sum over all *II* E N and get

$$\pi^{-s}\Gamma(s)\zeta(2s) = \int_0^{\infty} \sum_{n=1}^{\infty} e^{-\pi n^2 y} y^s \frac{dy}{y}$$

Observe that it is legal to interchange the sum and the integral because

$$\sum_{n=1}^{\infty} \int_0^{\infty} \left| e^{-\pi n^2 y} y^{s} \right| \frac{dy}{y} = \pi^{-\mathrm{Re}(s)} \Gamma(\mathrm{Re}(s)) \zeta(2\mathrm{Re}(s)) < \infty .$$

Now the series under the integral,

$$g(y) = \sum_{n=1}^{\infty} e^{-\pi n^2 y},$$

arises from Jacobi's classical theta series

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z} = 1 + 2 \sum_{n=1}^{\infty} e^{\pi i n^2 z},$$

i.e., we have $g(y) = \frac{1}{2}(\theta(iy) - 1)$. The function

$$Z(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$$

is called the completed zeta function. We obtain the

(1.3) Proposition. *The completed zeta function* $Z(s)$ *admits the integral representation*

$$Z(s) = \frac{1}{2} \int_0^{\infty} \big(\theta(iy) -$$

The proof of the functional equation for the function $Z(s)$ is based on the following general principle. For a continuous function $f : \mathbb{R}_+^* \to \mathbb{C}$ on the group $\mathbb{R}_+^*$ of positive real numbers, we define the Mellin transform to be the improper integral

$$L(f, s) = \int_0^{\infty} \big(f(y) - f(\infty) \big) y^{s} \frac{dy}{y}$$

provided the limit $f(\infty) = \lim_{y \to \infty} f(y)$ and the integral exist. The following theorem is of pivotal importance, also for later applications. We will often refer to it as the Mellin principle.

(1.4) Theorem. Let *.f,g:* 11:J;.�--+ C *be* continuous *functions such that*

f(y) = ao + O(<,-n"), g(_v) =ho+ O(e-cy"),

for y --+ oo, *with positive com.rant.� c,a.* ff *these* functions *1,atisfy the equation*

r({:J�chcvl,

for some real number k > 0 *and* some *complex number(' #-* 0, *then* one *has:*

(i) *The integrafa L(f,s) and L(f:,s) converge absolutely and uniformly ifs* varies *in an :irbitnuy compact domain contained in* {s E CI Re(s) > *k). They are lhercfore holomorphic functions on* {s EC l Re(.l) > A). *They admit holomorphic continuations to* , {0,k).

(ii) *They have .�imple poles at s* = 0 *ands* = *k with residues*

Rcs.,=ol(.f,s)=-a_0, Res,=1-L(j,s)=Ch_0, resp.

Res,-=nL(i,s) = *-ho,* Rc1,_,=� *L(g,s)* = $C^{-1}a_0$.

(iii) *They satisfy the functional equation*

L(f,.,)�CL(g,*k* - .,) .

Remark l: The 1,ymbol ,p(y) = O(1/!(y)) means, *a�* usual, that one has *,p(y) = r(y)ijr(y),* for ,;ome function c(_v) which stays hounded under 1he limit in question, so in our case, a1, *y*--+ oo.

Remark 2: Condition (ii) is to be understood to say that there is no pole if a_0 = 0, resp. *ho* = 0. But there i5 a pole, which b simple, if a_0 #- 0, re,p. *ho*#- 0.

Proof: If., varie5 over a compact 1,ubset of C, then the function
a = Re(s), is bounded for *y* 2:: I by a constant which is independent *a.*
Therefore the condition *f(y)* = ao + *O(e-cv")* the following upper bound for the integrand of the Mellin integral

!(f(y)-ao))"" ll::': *Be-,v"ya+ly-'.'* ::': *B'�,*)'

forall *y* 2:. 1. with comtanb *B.8'*. The integral *fi•..,U(y)* - ao)y'- *dy* therefore admit1, the convergent majorant *Ji"• �dy* which i1, independent of *s.* It therefore converge,; absolutely and unifofmly, for all .1 in the compact 1,ubset. The same holds for *fi'*^{0}*(g(y)* - b_0)y 1 *dy*.

Now let $\operatorname{Re}(s) > k$. We cut the interval of integration $(0,\infty)$ into $(0,1]$ and $[1,\infty)$ and write

$$L(f,s) = \int_1^\infty (f(y)-a_0)y^s \frac{dy}{y} + \int_0^1 (f(y)-a_0)y^s \frac{dy}{y}.$$

For the second integral, the substitution $y \mapsto 1/y$ and the equation $f(1/y) = Cy^k g(y)$ give:

$$\int_0^1 (f(y)-a_0)y^s \frac{dy}{y} = -\frac{a_0}{s} + C\int_1^\infty (g(y)-b_0)y^{k-s}\frac{dy}{y} - \frac{Cb_0}{k-s}.$$

By the above, it also converges absolutely and uniformly for $\operatorname{Re}(s) > k$. We therefore obtain

$$L(f,s) = -\frac{a_0}{s} + \frac{Cb_0}{s-k} + F(s),$$

where

$$F(s) = \int_1^\infty \left[(f(y)-a_0)y^s + C(g(y)-b_0)y^{k-s}\right]\frac{dy}{y}.$$

Swapping f and g, we see from $g(1/y) = C^{-1}y^k f(y)$ that:

$$L(g,s) = -\frac{b_0}{s} + \frac{C^{-1}a_0}{s-k} + G(s)$$

where

$$G(s) = \int_1^\infty \left[(g(y)-b_0)y^s + C^{-1}(f(y)-a_0)y^{k-s}\right]\frac{dy}{y}.$$

The integrals $F(s)$ and $G(s)$ converge absolutely and locally uniformly on the whole complex plane, as we saw above. So they represent holomorphic functions, and one obviously has $F(s) = CG(k-s)$. Thus $L(f,s)$ and $L(g,s)$ have been continued to all of $\mathbb{C} \setminus \{0,k\}$ and we have $L(f,s) = C\,L(g,k-s)$. This finishes the proof of the theorem.

The result can now be applied to the integral (1.3) representing the function $Z(s)$. In fact, Jacobi's theta function $\theta(z)$ is characterized by the following property.

(1.5) Proposition. *The series*

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$$

converges absolutely and uniformly in the domain $\{z \in \mathbb{C} \mid \mathrm{Im}(z) \geq \delta\}$, *for every* $\delta > 0$. *It therefore represents an analytic function on the upper half-plane* $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$, *and satisfies the transformation formula*

$$\theta(-1/z) = \sqrt{z/i}\,\theta(z).$$

We will prove this proposition in much greater generality in §3 (see (3.6)), so we take it for granted here. Observe that if z lies in $\mathbb{H}$ then so does $-1/z$. The square root $\sqrt{z/i}$ is understood to be the holomorphic function

$$h(z) = e^{\frac{1}{2}\log z/i},$$

where log indicates the principal branch of the logarithm. It is determined uniquely by the conditions

$$h(z)^2 = z/i \quad \text{and} \quad h(iy) = \sqrt{y} > 0 \ \text{ for } y \in \mathbb{R}_+^*.$$

(1.6) Theorem. *The completed zeta function*

$$Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$$

admits an analytic continuation to $\mathbb{C} \smallsetminus \{0, 1\}$, *has simple poles at* $s = 0$ *and* $s = 1$ *with residues* -1 *and* 1, *respectively, and satisfies the functional equation*

$$Z(s) = Z(1-s).$$

Proof: By (1.3), we have

$$Z(2s) = \frac{1}{2}\int_0^\infty \big(\theta(iy) -$$

i.e., $Z(2s)$ is the Mellin transform

$$Z(2s) = L(f, s)$$

of the function $f(y) = \frac{1}{2}\theta(iy)$. Since

$$\theta(iy) = 1 + 2e^{-\pi y}(1 + \sum_{n=2}^\infty e^{-\pi(n^2-1)y}),$$

one has $f(y) = \frac{1}{2} + O(e^{-\pi y})$. From (1.5), we get the transformation formula

$$f(1/y) = \frac{1}{2}\theta(-1/iy) = \frac{1}{2}y^{1/2}\theta(iy) = y^{1/2}f(y).$$

By (1.4), $L(f,s)$ has a holomorphic continuation to $\mathbb{C} \setminus \{0, 1/2\}$ and simple poles at $s = 0, 1/2$ with residues $-1/2$ and $1/2$, respectively, and it satisfies the functional equation

$$L(f,s) = L(f, \tfrac{1}{2} - s).$$

Accordingly, $Z(s) = L(f, s/2)$ has a holomorphic continuation to $\mathbb{C} \setminus \{0, 1\}$ and simple poles at $s = 0, 1$ with residues -1 and 1, respectively, and satisfies the functional equation

$$Z(s) = L(f, \tfrac{s}{2}) = L(f, \tfrac{1}{2} - \tfrac{s}{2}) = Z(1-s). \qquad \square$$

For the Riemann zeta function itself, the theorem gives the

(1.7) Corollary. *The Riemann zeta function $\zeta(s)$ admits an analytic continuation to $\mathbb{C} \setminus \{1\}$, has a simple pole at $s = 1$ with residue 1 and satisfies the functional equation*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

Proof: $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ has a simple pole at $s = 0$, but so does $\Gamma(s/2)$. Hence $\zeta(s)$ has no pole. At $s = 1$, however, $Z(s)$ has a simple pole, and so does $\zeta(s)$, as $\Gamma(1/2) = \sqrt{\pi}$. The residue comes out to be

$$\operatorname{Res}_{s=1}\zeta(s) = \pi^{1/2}\Gamma(1/2)^{-1}\operatorname{Res}_{s=1}Z(s) = 1.$$

The equation $Z(1-s) = Z(s)$ translates into

$$\zeta(1-s) = \pi^{-s+\frac{1}{2}}\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\zeta(s).$$

Substituting $(1-s)/2$, resp. $s/2$, into the formulae (1.2), (iii), 2) and 3) gives

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) = \frac{2\sqrt{\pi}}{2^s}\Gamma(s),$$

$$\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) = \frac{\pi}{\cos(\pi s/2)},$$

and after taking the quotient,

$$r\left(\frac{\cdot}{2}\right)/r\left(\frac{!-\cdot\cdot,}{2}\right) = \frac{2}{2} \ldots m \cos \frac{\pi \cdot}{2} r(s).$$

Inserting this into(*) now yields the functional equation claimed. n

At �ome point during the first month5 of studies every mathematics student has the supri�e to discover the remarkahle fonnula

$$\ldots = \frac{1}{n}\pi^2.$$

It is only the beginning of a sequence:

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{1}{90}\pi^4, \quad \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{1}{945}\pi^6 \quad \text{etc.}$$

The�e are explicit evaluations of the special value� of the Riemann Leta function at the points .1· = 2k, k EN. The phenomenon j., explained via the functional equation by the fact that the values of the Riemann .t:eta function at the *nexative* odd integer5 are given by **Bernoulli numbers.** The�e arise from the function

$$F(r) = \frac{tc'}{e^{t} - 1}$$

and are defined by the series expansion

$$F(f) = E/'O' \; r'$$

Their relation to the t:eta function give� them a special arithmetic significance. The lir�t Bernoulli numbers are

$$B_0 = 1,\quad B_1 = \frac{1}{2},\quad B_2 = \frac{1}{6},\quad H, = 0,\quad 84 = -\frac{1}{30},\quad B� = 0,\quad 81:, = \frac{1}{42}.$$

In general one has $8_{2..+1} = 0$ for $I!$ 2'.:: I. because $F(-f) = F(f)$ - !. In the cla�sical lite�ature, it i, u\ually the fu�ction �, which '>erves for defin'.ng the Bernoulli numbers. As $F(t) = 7$--=--i- + t, this docs not change anythmg except for B_1. where one flmb - � instead of *j.* But the above definition **i�** more natural and better �uitcd for the further development of the theory. We now prove the remarkable

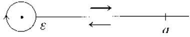
(1.8) Theorem. For cvc1y integed > 0 *oneha.,*

((I -kI�

We prepare the proof proper by a function-theoretic lemma. For f > 0 and a E [E, ocl, we com,idcr the path

$$C_{\varepsilon, a} = (a, \varepsilon] + K_\varepsilon + [\varepsilon, a),$$

which first follows the half-line from a to F:, then the circumference K, = /z I 1:1 = e} in the negative direction. and finally the half-line from f toa:



(1.9) Lemma. *Let U be an open* subset of C rlwt *contains the path C'i-.a and afao the interior* of *K,. Lee* G(z) *be a holomorphic* fonc1ion on *U*, /0) *with* a *pole* of *order m al* 0, *and* let *G(t)r''·'* 1 *(n* EN), forRc(s) > �- be *integrable on* (0. a). *Then one ha�*

$$\int_{(} G(::)z'''^{-1}dz = (e^{2,rrn.i} - 1) \int_0 G(t)t'''^{-1}dt.$$

Proof: The integration doc� not actually take place in the complex plane but on the universal covering of:::::�,

X={(x.a)EC*x iargx==amod2;r)

z and ::'-¹ arc holomorphic functions on X, namely

$$z(x, \alpha) = x, \quad z^{s-1}(x, \alpha) = e^{(s-1)(\log x + i\alpha)}$$

and C,." i::, the path

$$C_{\varepsilon, a} = I^-_{\varepsilon, a} + K_\varepsilon + I^+_{\varepsilon, a}$$

where *le�''*= (a.Pj x {O), K, = {n,-¹¹ It E [0.2;rl}, !,\, = [F,a) x (2;r) in X. We now have

$$\int_{11-,i} G(z)::',, \, dz = -\int_I G(t)t111\text{-}1 \, dt.$$

$$\int_{/,+,,} G(z)::n'^{-1}dz = e^{2'u^{11}} \cdot \int_I G(l)tu'^{\,1}dt,$$

$$\int_{K_\varepsilon} G(z) z^{ns-1}\, dz = -i \int_0^{2\pi} G(\varepsilon e^{-it}) \varepsilon^{ns-1} e^{-it(ns-1)} \varepsilon e^{-it}\, dt = -i \int_0^{2\pi} \varepsilon^{ns} G(\varepsilon e^{-it}) e^{-itns}\, dt\,.$$

Since $\mathrm{Re}(s) > \frac{m}{n}$, i.e., $\mathrm{Re}(ns - m) > 0$, the last integral $I(\varepsilon)$ tends to zero as $\varepsilon \to 0$. In fact, one has $\lim_{\varepsilon\to 0} \varepsilon^{ns} G(\varepsilon e^{-it}) = 0$. This gives

$$\int_{L_\varepsilon} G(z) z^{ns-1}\, dz = (e^{2\pi i ns} - 1) \int_\varepsilon^\infty G(t) t^{ns-1}\, dt + I(\varepsilon),$$

and since the integral on the left is independent of ε, the lemma follows by passing to the limit as $\varepsilon \to 0$. □

Proof of (1.8): The function

$$F(z) = \frac{z}{e^z - 1} = \sum_{k=0}^\infty B_k \frac{z^k}{k!}$$

is a meromorphic function of the complex variable z, with poles only at $z = 2\pi i\nu$, $\nu \in \mathbb{Z}$, $\nu \neq 0$. B_k/k is the residue of $(k-1)!\, F(z) z^{-k-1}$ at 0, and the claim reduces to the identity

$$\mathrm{Res}_{z=0} F(z) z^{-k-1} = \frac{1}{2\pi i} \int_{|z|=\varepsilon} F(z) z^{-k-1}\, dz = -\frac{\zeta(1-k)}{(k-1)!},$$

for $0 < \varepsilon < 2\pi$, where the circle $|z| = \varepsilon$ is taken in the positive orientation. We may replace it with the path $L_\varepsilon = (-\infty, -\varepsilon] + K_\varepsilon + [-\varepsilon, -\infty)$, which traces the half-line from $-\infty$ to $-\varepsilon$, followed by the circumference $K_\varepsilon = \{|z| = \varepsilon\}$ in the positive direction, from $-\varepsilon$ to $-\varepsilon$, and finally the half-line from $-\varepsilon$ to $-\infty$. In fact, the integrals over $(-\infty, -\varepsilon]$ and $[-\varepsilon, -\infty)$ cancel each other. We now consider on L_ε the function

$$H(s) = \int_{L_\varepsilon} F(z) z^{s-1} \frac{dz}{z}\,.$$

Here the integrals over $(-\infty, -\varepsilon]$ and $[-\varepsilon, -\infty)$ do not cancel each other any longer because the function z^{s-1} is multivalued. The integration takes place on the universal covering $X = \{(z, \alpha) \in \mathbb{C}^\times \times \mathbb{R} \mid \arg z = \alpha \bmod 2\pi\}$

of X as in (1.9), and z, z^{s-1} are the holomorphic functions $z(x,\alpha) = x$, $z^{s-1}(x,\alpha) = e^{(s-1)(\log|x|+i\alpha)}$. The integral converges absolutely and locally uniformly for all $s \in \mathbb{C}$. It thus defines a holomorphic function on $\mathbb{C}$, and we find that

$$\mathrm{Res}_{z=0} F(z)z^{-k-1} = \frac{1}{2\pi i}H(1-k).$$

Now substitute $z \mapsto -z$, or more precisely, apply the biholomorphic transformation

$$\varphi : X \longrightarrow X, \quad (x,\alpha) \longmapsto (-x, \alpha - \pi).$$

Since $z \circ \varphi = -z$ and

$$(z^{s-1} \circ \varphi)(x,\alpha) = z^{s-1}(-x, \alpha-\pi) = e^{(s-1)(\log|x|+i\alpha-i\pi)} = -e^{-i\pi s}z^{s-1}(x,\alpha),$$

we obtain

$$H(s) = -e^{-i\pi s}\int_{C'_\varepsilon} F(-z)z^{s-1}\frac{dz}{z},$$

where the path $C'_\varepsilon = \varphi^{-1} \circ (-C_\varepsilon)$ follows the half-line from ∞ to ε, then the circumference K_ε in *negative* direction from ε to ε, and finally the half-line from ε to ∞. The function

$$G(z) = F(-z)z^{-1} = \frac{1}{e^z - 1} = \frac{e^{-z}}{1-e^{-z}} = \sum_{n=1}^{\infty} e^{-nz}$$

has a simple pole at $z = 0$ so that, for $\mathrm{Re}(s) > 1$, (1.9) yields

$$\begin{aligned} H(s) &= -e^{-i\pi s}\int_{C'_\varepsilon} G(z)z^{s-1}dz \\ &= -(e^{i\pi s} - e^{-i\pi s})\int_0^\infty G(t)t^s\frac{dt}{t} = -2i\sin\pi s\int_0^\infty G(t)t^s\frac{dt}{t}. \end{aligned}$$

The integral on the right will now be related to the zeta function. In the gamma integral

$$\Gamma(s) = \int_0^\infty e^{-t}t^s\frac{dt}{t},$$

we substitute $t \mapsto nt$ and get

$$\Gamma(s)\frac{1}{n^s} = \int_0^\infty e^{-nt}t^s\frac{dt}{t}.$$

Summing this over all $n \in \mathbb{N}$ yields,

$$\Gamma(s)\zeta(s) = \int_0^\infty G(t)\, t^s \frac{dt}{t}.$$

The interchange of summation and integration is again justified because

$$\sum_n \int_0^\infty |e^{-nt} t^s| \frac{dt}{t} < \infty.$$

From this and (1.2), 2), we get

$$H(s) = -2i \sin \pi s\, \Gamma(s)\zeta(s) = -\frac{2\pi i}{\Gamma(1-s)}\zeta(s).$$

Since both sides are holomorphic on all of $\mathbb{C}$, this holds for all $s \in \mathbb{C}$. Putting $s = 1-k$ we obtain, since $\Gamma(k) = (k-1)!$,

$$\operatorname{Res}_{z=0} F(z) z^{-k-1} = \frac{1}{2\pi i} H(1-k) = -\frac{\zeta(1-k)}{(k-1)!}. \quad \text{q.e.d.} \quad \square$$

Applying the functional equation (1.7) for $\zeta(s)$ and observing that $\Gamma(2k) = (2k-1)!$, the preceding theorem gives the following corollary, which goes back to *Euler*.

(1.10) Corollary. *The values of $\zeta(s)$ at the positive even integers $s = 2k$, $k = 1,2,3,\ldots$, are given by*

$$\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}.$$

The values $\zeta(2k-1)$, $k > 1$, at the positive odd integers have been elucidated only recently. Surprisingly enough, it is the higher K-groups $K_n(\mathbb{Z})$ from algebraic K-theory, which take the lead. In fact, one has a mysterious canonical isomorphism

The image R_{2k} of a nonzero element in $K_{4k-1}(\mathbb{Z}) \otimes \mathbb{Q}$ is called the 2k-th regulator. It is well-determined up to a rational factor, i.e., it is an element of $\mathbb{R}^*/\mathbb{Q}^*$, and one has

$$\zeta(2k-1) \equiv R_{2k} \bmod \mathbb{Q}^*.$$

This discovery of the Swiss mathematician *ARM,1N!J BoRFJ.* has had a tremendous influence on further arithmetical ret-,earch, and hat-, opened up deep insight5 into the arithmetic nature of zeta function� and L-series of the most general kind. Thet-.e imight5 are �ummarized within the comprehemive **Beilinson conjecture** (t-.ee 1117J). In the meantime, the mathematiciam *SPENCCR Ht.OCH* and *K11LUY,1 K,i.ro* have found a complete description of the special 1eta values ((2/... - 1) (i.e.. not just a description mod O:;•i via a new theory of the *Tamagawa measure.*

The zeroes of the Riemann zeta function command special aucntion. Euler's identity (I.I) shows that one hat-. ((.1) -::f. 0 for Re(s) > **1.** The gamma function *I'(s)* is nowhere 0 and has simple poles at *s* = 0. - I. - 2, ... The functional equation Z(s) = Z(l - s*)*. i.e..

,,-,;, n.,/2J((.<J � ,,r,-1J1^2*r(* (1 - ,J/2) ((1 - .,) .

therefore showt-. that the only 7eroes of ((s) in the domain Re(s) < 0 arc the poles of *I'(s/2),* i.e., the arguments *s* = -2, - 4. - 6. The�e arc called the *trii·ial :croc.1* of *((s*). Other zeroes have to lie in the **critical strip** 0 _:s Re(s) _:s 1, :c.ince ((s) -::f. 0 for Rc(s) > I. They are the �ubject of the famout-., t-.till unproven

Riemann Hypothesis: The non-trivial zeroes of ((s) lie on the line Re(s) = �-

This conjecture has heen verified for 150 million zeroes. It hat-. immediate consequences for the problem of the di�tribution of prime numbers within all the natural number�. The distribution function

rr(x) = *#/p* prime number _:s *x)*

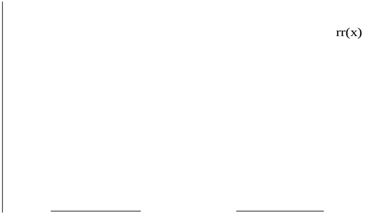
may be \'.fitten. according to *RIEMAAA·,* as the seriet-.

rr(_t) = R(x) - *L* *R(rP)_*
p

where *p* varies over all the LCroes of ((s). and *R(x)* it-. the function

R(x)� 1+ I ------------------------ I ([ogx)^{11}
n =t+((I1 + I) n!

On a microscopic scale, 1hc function rr(,-) is a �tcp-function with a highly irregular hehaviour. But on a large scale it i� its a�tounding smoothness which poses one of the biggest mysterie<, in mathematic�:



On thi� matter, we urge the reader to consult the essay I 142) by *Dm,' 7-1<,ltH*

Exercise **1.** Let a, h be positive real number�. Then the Mellin transform\ ur the function� / (y} ,md $g(y) = f(ay^h)$ satisty:

$$L(f \quad .1/h) = ha'i^1 'L(g,.1).$$

Exercise 2. f"hc **Bernoulli polynomials** $B,(.1.)$ arc defined by

1
t<'.; �':' =F(tlr"=I/1.C1)�,

so that $B_k = B_k(0)$. Show that

B.,,(r)=

Exercise J, R,(1)- B.(t - 1) = /.,_r• 1.

Exercise **4,** For the power sum

$$;.(n)=1'+2'+3'+ \quad +n'$$

one ha\

$$;_k(n) = \frac{1}{k+1}(B_{k+1}(n) - B_{k+1}(0)).$$

Exercise 5, Let 11(:-J $= H(2z) = L'''$ Then for all matnce\ $y = (:^1$;;) 111 the group

/i,(4) = {(:'. j) E SL,(ZJ j c '=O mud 4) one ha� the formula

$$\vartheta\Big(\frac{az+b}{cz+d}\Big) = j(\gamma, z)\vartheta(z), \quad z \in \mathbb{H}.$$

where

$$j(\gamma, z) = \Big(\frac{c}{d}\Big)\varepsilon_d^{-1}(cz+d)^{1/2}.$$

The Legendre �ymhol (�) and the con�tanl *id* are defined by

$$\Big(\frac{c}{d}\Big) = \begin{cases} -\Big(\frac{c}{|d|}\Big), & \text{ift<0.d<0,} \\ \Big(\frac{c}{|d|}\Big), & \text{otherwi�e.} \end{cases}$$

$$\varepsilon_d = \begin{cases} 1, & \text{ifd-= I mod 4,} \\ i, & \textit{ifd} = 3 \bmod 4. \end{cases}$$

Jacobi's theta function *i!(z)* is thu� an example of a **modular form of weight** { for the group The representation of L-�encs a� Mellin tran�form� of modulir form�, which we introduced m the case of the Riemann Leta function, 1� one of the hasic tmd �eminal principle� of current number-theoretic rcsc:uch {see [1061).

§ 2. Dirichlet £-series

The most immediate relatives of the Riemann zeta function are the Dirichlet L-serie5. They are <lclined as follow�. Let m be a natural number. A **Dirichlet character** mod m i'> by definition a character

X '(Z/m'L)' - *S'* �1, EC | 1,1 �I\.

It is called **primitive** if it does not arise a5 the compo�ite

(Z/mzr--------)' (Z/ni'Z)* � *S¹*

of a Dirichlet character *x'* mod *m'* for any proper divi�or *m'lm*. In the general case. the gcd of all �uch divisors i� called the **conductor** *f* of *X· Sox* is alway<, induced from a primitive character *X'* mod *(.* Given *X,* we define the multiplicative function *x* : Z → C by

$$x(n) = \begin{cases} x(n \bmod m) & \text{for(n.m)=L} \\ 0 & \text{for } (n,m) \text{ -=I-I.} \end{cases}$$

The *flfriaf charwter* X^0 mod *m,* X^0(n) = I for *(n,m)* = I. X^0(n) = 0 for (n, m) -=*I*- I, plays a �pecial role, When read mod I, we denote it by X = I.

It is also called the principal character. Considering it in the theory to be developed now has the effect of subsuming here everything we have done in the last section. For a Dirichlet character χ, we form the Dirichlet L-series

$$L(\chi,s)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

where s is a complex variable with $\mathrm{Re}(s)>1$. In particular, for the principal character $\chi=1$, we get back the Riemann zeta function $\zeta(s)$. All the results obtained for this special function in the last section can be transferred to the general L-series $L(\chi,s)$ using the same methods. This is the task of the present section.

(2.1) Proposition. *The series* $L(\chi,s)$ *converges absolutely and uniformly in the domain* $\mathrm{Re}(s)\geq 1+\delta$, *for any* $\delta>0$. *It therefore represents an analytic function on the half-plane* $\mathrm{Re}(s)>1$. *We have Euler's identity*

$$L(\chi,s)=\prod_{p}\frac{1}{1-\chi(p)p^{-s}}.$$

In view of the multiplicativity of χ and since $|\chi(n)|\leq 1$, the proof is literally the same as for the Riemann zeta function. Since, moreover, we will have to give it again in a more general situation in § 8 below (see (8.1)), we may omit it here.

Like the Riemann zeta function, Dirichlet L-series also admit an analytic continuation to the whole complex plane (with a pole at $s=1$ in the case $\chi=\chi^0$), and they satisfy a functional equation which relates the arguments to the argument $1-s$. This particularly important property does in fact hold in a larger class of L-series, the *Hecke L-series*, the treatment of which is an essential goal of this chapter. In order to provide some preliminary orientation, the proof of the functional equation will be given here in the special case of the above L-series $L(\chi,s)$. We recommend it for careful study, also comparing it with the preceding section.

The proof again hinges on an integral representation of the function $L(\chi,s)$ which has the effect of realizing it as the Mellin transform of a theta series. We do, however, have to distinguish now between *even* and *odd* Dirichlet characters χ mod m. This phenomenon will become increasingly important when we generalize further. We define the exponent $p\in\{0,1\}$ of χ by

$$\chi(-1)=(-1)^p\chi(1).$$

Then the rule

$$\chi\big((n)\big)=\chi(n)\Big(\frac{n}{|n|}\Big)^p$$

defines a multiplicative function on the semigroup of all ideals (n) which are relatively prime to m. This function is called a *Größencharakter* mod m. These *Größencharaktere* are capable of substantial generalization and will play the leading part when we consider higher algebraic number fields (see §7).

We now consider the gamma integral

$$\Gamma(\chi,s) = \Gamma\left(\frac{s+p}{2}\right) = \int_0^\infty e^{-y} y^{(s+p)/2}\,\frac{dy}{y}.$$

Substituting $y \mapsto \pi n^2 y/m$, we obtain

$$\left(\frac{m}{\pi}\right)^{\frac{s+p}{2}} \Gamma(\chi,s)\frac{1}{n^s} = \int_0^\infty n^p e^{-\pi n^2 y/m} y^{(s+p)/2}\,\frac{dy}{y}.$$

We multiply this by $\chi(n)$, sum over all $n \in \mathbb{N}$, and get

$$(*) \qquad \left(\frac{m}{\pi}\right)^{\frac{s+p}{2}} \Gamma(\chi,s) L(\chi,s) = \int_0^\infty \sum_{n=1}^\infty \chi(n) n^p e^{-\pi n^2 y/m} y^{(s+p)/2}\,\frac{dy}{y}.$$

Here, swapping the order of summation and integration is again justified, because

$$\sum_{n=1}^\infty \int_0^\infty \left|\chi(n) n^p e^{-\pi n^2 y/m} y^{(s+p)/2}\right| \frac{dy}{y} \le \left(\frac{m}{\pi}\right)^{(\mathrm{Re}(s)+p)/2} \Gamma\left(\frac{\mathrm{Re}(s)+p}{2}\right) \zeta(\mathrm{Re}(s)) < \infty.$$

The series under the integral (*),

$$g(y) = \sum_{n=1}^\infty \chi(n) n^p e^{-\pi n^2 y/m},$$

arises from the theta series

$$\theta(\chi,z) = \sum_{n\in\mathbb{Z}} \chi(n) n^p e^{\pi i n^2 z/m}$$

where we adopt the convention that $0^0 = 1$ in case $n = 0$, $p = 0$. Indeed, $\chi(n)n^p = \chi(-n)(-n)^p$ implies that

$$\theta(\chi,z) = \chi(0) + 2\sum_{n=1}^\infty \chi(n) n^p e^{\pi i n^2 z/m}$$

so that *R(y) = {(O(x,iy)* - x(O)) with x(O) = I, if *x* is the trivial character **I,** and *)(* (0) = 0 otherwise. When *m* = I, this is Jacobi "s theta function

0(c)� I: e""'0,
/IC:'!:

which i� aswcialed with Riemann's .t:eta function as we o:,aw in *I. We view the factor

L,.(x,s) = *(�),n I'(x,-'-)*

in(*) as the "Euler factor" at the infinite prime. It joins with the Euler factors *L1,(s)* = 1/(1 - x(p)p-') of the product representation (2.1) of L(x.-1) to define the **completed** L-series of the character x:

$$\Lambda(\chi,s) = L_\infty(\chi,s)L(\chi,s), \quad \mathrm{Re}(s) > 1.$$

For this function(*) gives us the

(2.2) **Proposition.** *The function A(x,* n *admit.� lhc integr,-1./ represcnwtion*

A(x,s) =� 2 *f* *(O(x,iy) - xW))y1'* i,,112!!!..., \'

where $c(\chi) = (\frac{\pi}{m})^{p/2}$.

Let us emphasize the fact that the rnmmation in the *L* -�cries i� only over the natural numhers, whereas in the theta �cries we sum over *all* integers. This is why the factor *nP* had to be included in order to link the L-�erics lo the theta series.

We want to apply the Mellin principle to the above integral reprc..,cntation. So we have to show that the theta series *H(x,* iy) o:,atisfies a transformation formula a� a�sumed in theorem (1.4). To do this, we use the following:

(2.3) **Proposition.** *Let a, h, µ be* real *numbers,µ* > 0. *Then the* �eric.-,

01,(a,h.z) = $e^{\pi i(a+g)^2 z + 2\pi i h g}$

convc1gcs ;1b.rnlutely ;.md uniformly in rile *domain* hn(z) 2: *8,* for *every 8* > 0, and for: E llil, one *Ji.is the* transformation fomw/a

$$\vartheta_\mu(a,b,-1/z) = e^{2\pi i ab}\frac{\sqrt{z/i}}{\mu}\theta_{1/\mu}(-b,a,z).$$

This proposition will be proved in§ 3 in much greater generality (see (3.6)), so we take it for granted here. The series *0_1,(a,h,z)* is locally unifonnly convergent in the variables *a, h.* This will also he shown in § 3. Differentiating *p* times *(p* = 0, I) in the variahle *a,* we obtain the function

$$+ g)^p e^{\pi i(a+g)^2 z+2\pi ibg}$$

More precisely, we have

$$\frac{d^p}{da^p}\theta_\mu(a,b,z) = (2\pi i)^p z^p \theta_\mu^p(a,b,z)$$

and

$$\frac{d^p}{da^p} e^{\ 2\pi iab}\theta_{1/\mu}(-b,a,z) = (2\pi i)^p e^{-2\pi iab}\theta_{1/\mu}^p(-b,a,z).$$

Applying the differentiation *di'/ dal'* to the transformation formula (2.3), we get the

(2.4) Corollary. For *a, h, fl* E IR, *11* > 0, *one ha.� the transformation* form11fa

$$\theta_\mu^p(a,b,-1/z) = \left[i^p e^{2\pi iab}\mu\right]^{-1}(z/i)^{p+\frac{1}{2}}\theta_{1/\mu}^p(-b,a,z)$$

Thi� corollary give:-. u:-. the required transformation formula for the theta series *O(x.a),* if we introduce the *Gauss sums* which are defined as follow5.

(2.5) Definition. For *n* E Z, *the* Gauss sum *r(x,n)* associated *to the Dirichlet character x* mod *m* is defined *to be the complex. number*

$$\tau(\chi,n) = \sum_{\nu=0}^{m-1}\chi(\nu)e^{2\pi i\nu n/m}$$

For11 = I, we write r(x) = *r(x.* I).

(2.6) Proposition. *For a* primitive *Dirichlet character x* mod *m, one hw,*

r(x,n) = *X(n)r(x)* *:md* lr(x)I = *,Im.*

Proof: The first identity in the case $(n,m) = 1$ follows from $\chi(\mu n) = \chi(n)\chi(\mu)$. When $d = (n,m) \neq 1$, both sides are zero. Indeed, since χ is primitive, we in this case choose an $a \equiv 1 \bmod m/d$ such that $a \not\equiv 1 \bmod m$ and $\neq 1$. Multiplying $\tau(\chi,n)$ by $\chi(a)$ and observing that $e^{2\pi i \mu a n/m} =$ gives $\chi(a)\tau(\chi,n) = \tau(\chi,n)$, so that $\tau(\chi,n) = 0$. Further, we have

$$|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \tau(\chi)\sum_{\nu=0}^{m-1}\overline{\chi}(\nu)e^{-2\pi i\nu/m} = \sum_{\nu=0}^{m-1}\tau(\chi,\nu)e^{-2\pi i\nu/m}$$

$$= \sum_{\nu=0}^{m-1}\sum_{\mu=0}^{m-1}\chi(\mu)\,e^{2\pi i\nu\mu/m}\,e^{-2\pi i\nu/m} = \sum_{\mu=0}^{m-1}\chi(\mu)\sum_{\nu=0}^{m-1}e^{2\pi i\nu(\mu-1)/m}.$$

The last sum equals m for $\mu = 1$. For $\mu \neq 1$, it vanishes because then $\xi = e^{2\pi i(\mu-1)/m}$ is an m-th root of unity $\neq 1$, hence a root of the polynomial

$$\frac{X^m - 1}{X - 1} = X^{m-1} + \cdots + X + 1.$$

Therefore $|\tau(\chi)|^2 = m\chi(1) = m$. □

We now obtain the following result for the theta series $\theta(\chi, z)$.

(2.7) Proposition. *If χ is a primitive Dirichlet character* mod m*, then we have the transformation formula*

$$\theta(\chi, -1/z) = \frac{\tau(\chi)}{i^p\sqrt{m}}(z/i)^{p+\frac{1}{2}}\theta(\overline{\chi}, z),$$

where $\overline{\chi}$ is the complex conjugate character to χ, i.e., its *inverse.*

Proof: We split up the series $\theta(\chi, z)$ according to the classes a mod m, $a = 0, 1, \dots, m-1$, and obtain

$$\theta(\chi, z) = \sum \chi(n)n^p e^{\pi i n^2 z/m} = \sum_{a=0}^{m-1}\chi(a) \qquad + g)^p e^{\pi i(a+g)^2 z/m},$$

hence

$$\theta(\chi, z) = \sum_{a=0}^{m-1}\chi(a)\theta_\mu(a, 0, z/m).$$

By (2.4), one has

$$\theta^{p}_{m}(a,0,-1/mz) = \frac{1}{i^{p}m}(mz/i)^{p+\frac{1}{2}}\theta^{p}_{1/m}(0,a,mz)$$

and this gives

$$\vartheta^{p}_{1/m}(0,a,mz) = \quad g^{p}\, e^{\pi i g^2 mz+2\pi i a g} = \frac{1}{m^{p}} \sum_{n\in\mathbb{Z}} e^{2\pi i a n/m} n^{p}\, e^{\pi i n^2 z/m}\,.$$

Multiplying this by x(a), then summing over *a*, and observing that r(x.11) = X(n)r(x), we find:

Hix, -1/cJ � $\frac{1}{{}^{;}{}^{p}m}(mz/i)^{p+\frac{1}{2}\,m}$,E *x(a)e/;/11(0,a.m;;)*

$$= \frac{1}{i^{p}m^{p+1}}(mz/i)^{p+\frac{1}{2}} \sum_{n\in\mathbb{Z}}\Big(\sum_{a=0}^{m-1}\chi(a)\, e^{2\pi i a n/m}\Big) n^{p}\, e^{\pi i n^2 z/m}$$

$$= \frac{1}{i^{p}\sqrt{m}}(z/i)^{p+\frac{1}{2}}\,\tau(\chi) \sum_{n\in\mathbb{Z}} \overline{\chi}(n) n^{p}\, e^{\pi i n^2 z/m}$$

$$= \frac{\tau(\chi)}{i^{p}\sqrt{m}}(z/i)^{p+\frac{1}{2}}\,\theta(\overline{\chi},z)\,. \qquad \square$$

The analytic continuation and functional equation for the function *J\.(x. s)* now falls out immediately. We may restrict oun,elve� to the ea<;e of a *primitive* character mod *m.* For *x* is alway� induced by a primitive character X' mod *f,* where *f* i� the conductor of X (see p. 434), and we clearly have

L(x,,,) � TT(! - xlp)p-')L(x',.,),
/Jim
f!'f

so that the analytic continuation and functional equation of *J\.(x, \')* follows from the one for J\.(x', *s).* We may further exclude the case $m = 1$ (thb **i�** not really necessary, ju�t to make life easy). this being the case of the Riemann zeta function which wa� settled in *§* I. The pole:,, in thb case are different.

(2.8) **Theorem.** *If* X is *a nontrivial* primirive *Dirichlet character. then the completed* L-series *J\.(x.s)* admit.� *an wwlytic continuation to the* **whole** *complex* plane C *and sati8fie:,, the functional* equation

$$\Lambda(\chi,s) = W(\chi)\Lambda(\overline{\chi},1-s)$$

with the factor $W(x) =$ This *factor* /rn:,, *ab:,,o/utc value* I.

Proof: Let $f(y) = \frac{c(\chi)}{2}\theta(\chi, iy)$ and $g(y) = \frac{c(\chi)}{2}\theta(\overline{\chi}, iy)$, $c(\chi) = \left(\frac{\pi}{m}\right)^{p/2}$. We have $\chi(0) = \overline{\chi}(0) = 0$, so that

U(x, iy) = 2 f: x(n)n1 c n:,, 2 •im.
11=1

and therefore O(c n:i/111), and likewi<,c g(y)
By (2.2), one

$$A(\chi, s) = \frac{c(\chi)}{2} \int_0^\infty \theta(\chi, iy) y^{\frac{s+p}{2}} dy$$

We therefore obtain A(x ..1) and similarly abo A(X,.,) as Mellin transforms

A(x.s) = L(f,s') and A(X,s) = L(g,s')

of the functions f(y) and g(y) at the points' = The tram.formation formula (2.7) give"

I(-') = c(x)/2 O(x, - l/iv)=((�)T(X) yfl-f '!ocx.1_r)= $\frac{\tau(\chi)}{i^p\sqrt{m}} y^{p+\frac{1}{2}} g(y)$.
y 2 - 2,t'Jrii

Theorem (1.4) therefore telb u� that A(x . .'I) admits an analytic continuat10n to all of C and that the equation

A(x,,,)�L(/,"f') �W(x)L(t,P+ ½-½") �W(x)L(g,' t")
�W(x)A(j', I - ,,)

hokh with $W(x)$ = By (2.6), we have jW(x)I = I. □

The hehaviour of the special values at integer argumcnb of the Riemann 1cta function generalizes to the Dirichlet L-scric� L(x,s) if we introduce, for nontrivial primitive Dirichlet characters x mod m, the **generalized Bernoulli numbers** B1x. defined hy the formula

F,1.(f) = m ,�l x(a) te''1 emf- l = ex,).;) Bi..x 1A k!"

Thc:-e are algebraic numbers which lie in the field Q(x) generated by the valuc5 of X. Since

Fx(-t) = m � 1 1 x(-l)x(m-a) te(m-a)l emr 1 = x(-l)Fx(/).

wc fin<l (-l){H1. x = x(-l)Bk.x, sothat

B1..x =0 for J. ""fop mod 2,

if p E /0. I} i� defined by x(-1) = (-l)"x(l).

(2.9) Theorem. *For any integer $k \geq 1$, one has*

$$L(\chi, 1-k) = -\frac{B_{k,\chi}}{k}.$$

Proof: The proof is the same as for the Riemann zeta function (see (1.8)): the meromorphic function

$$F_\chi(z) = \sum_{a=1}^{m} \chi(a) \frac{ze^{az}}{e^{mz}-1} = \sum_{k=0}^{\infty} B_{k,\chi} \frac{z^k}{k!}$$

has poles at most at $z = \frac{2\pi i\nu}{m}$, $\nu \in \mathbb{Z}$. The claim therefore reduces to showing that

(1) $$\frac{L(\chi, 1-k)}{(-1)^{k-1}(k-1)!} = \text{residue of } F_\chi(z)z^{-k-1} \text{ at } z = 0.$$

Multiplying the equation

$$\Gamma(s)\frac{1}{n^s} = \int_0^\infty e^{-nt} t^s \frac{dt}{t}$$

by $\chi(n)$, and summing over all n, yields

(2) $$\Gamma(s)L(\chi, s) = \int_0^\infty G_\chi(t) t^s \frac{dt}{t}$$

with the function

(3) $$G_\chi(z) = \sum_{n=1}^{\infty} \chi(n)e^{-nz} = \sum_{a=1}^{m} \chi(a) \frac{e^{(m-a)z}}{e^{mz}-1} = F_\chi(-z)z^{-1}.$$

From the equations (2) and (3) one deduces equation (1) in exactly the same manner as in (1.8). □

The theorem immediately gives that

$$L(\chi, 1-k) = 0 \quad \text{for } k \not\equiv p \bmod 2,$$

$p \in \{0, 1\}$, $\chi(-1) = (-1)^p \chi(1)$, provided that χ is not the principal character $\mathbf{1}$. From the functional equation (2.8) and the fact that $L(\chi, k) \neq 0$, we deduce for $k \geq 1$ that

$$L(\chi, 1-k) = -\frac{B_{k,\chi}}{k} \neq 0 \quad \text{for } k \equiv p \bmod 2.$$

The functional equation also gives the

(2.10) Corollary. *Fork* =′= *p* mod 2, *k* ::'.: I, *one has*

L(X, k)= (-1)1+{�-p}/2�(�)1. $\frac{B�X.}{k!}$ 2if′ m

For the values $L(x,A)$ at positive integer arguments k ¢ p mod 2, similar remarks apply a� the ones we made in § 1 about the Riemann zeta function at the points *2k*. Up to unknown algebraic factors, these values are certain "regulators" defined via canonical mapr, from higher K -groupr, into Minkowski space. A detailed treatment of this deep result of the Russian mathematician A.A. B1c1uN.\ON can be found in fl 10].

Exercise **l.** Let $F_1(t,x)$ = Z:=;;[1] The **Bernoulli polynomials** *B*, ,.(r)

ass�ociated to the Dirichlet character X arc by

$$F1(t,x) = \ldots x(x)k!\cdot$$

Thu� Rc,.(0) = *Ri* X. Show that

$$B_{k,\chi}(x) = \sum_{i=0}^{k}\binom{k}{i}B_{i,\chi}x^{k-i}$$

Exercise 2. *B,* xfx)- *B,1(x* -m) =*kL;;•-i x(a)(a+x -m)'* 1, *k* 2". 0.

Exercise 3. For the numbeVi *S,* xft') = Z:=;;=1x(a)1/, *k* 2". 0, one ha�

$$S_{-1}(vm) = \frac{1}{k+1}[(B_{,+1}(vm) - B_{,+1}(0)].$$

Exercise **4.** For a primitive odd character x, one ha�

§ 3. Theta Series

Riemann's zeta function and Dirichlet's L-series are attached to the field IQ. They have analogues for any algebraic number field K, and the re�ults obtained in § 1 and 2 extend to these generalizations in the same way, with the same methods. In particular, the Mellin principle applies again, which allows us to view the L-serie5 in question a5 integrals over theta 5eries. But now higher dimensional theta series are required which live on a higher dimensional analogue of the upper half-plane IH'.. *A priori* they do not have any relation with number fields and deserve to be introduced in complete generality.

The familiar objects C, !R, find their higher dimensional analogues a� follows. Let X be a i.e., a finite set with an involution TR f (r EX), and let $n = \#X$. /e consider the n-dimensional C-algebra

of all tuples $z =$ (Zr)r'=x, z, E with componenlwisc addition and multiplication. **lf:** = (:,) E C, then the element Z E C is detincd to have the following componenb:

We call the involution : r----+ Z the **con_jugation** on C. In addition, we have the involutions : i---+ ::* and z !---'I- �z given by

$$\overset{*}{\tau} = z_{\bar\tau}, \quad \text{resp.} \quad {}^{*}z_\tau = z_\tau .$$

One clearly has : = The set

$$: = \Big[\prod_\tau \mathbb{C} \Big]^+ = \big\{ z \in \mathbf{C} \mid z = \bar z \big\}$$

form� an n-dimensional commutative IR-algebra, and C = **R** ®;-t

If K is a number field of degree n and $X =$ Hom(K. C), then **R** is the **Minkowski** space KIR (� K ®G l?l.) which was introduced in chapter I, �5. The number-theoretic applications will occur there. But for the moment we leave all number-theoretic aspects aside.

For the additive, re�p. multiplicative, group <.:. ret-.p. **C�,** we have the homomorphism

$$Tr : \mathbf{C} \to \mathbb{C}, \quad Tr(z) = \sum_\tau z_\tau, \quad \text{resp.}$$
$$N : \mathbf{C}^* \to \mathbb{C}^*, \; N(z) = \prod z_\tau .$$

Here Tr(:), resp. N(':), denotes the trace, resp. the determinant, of the endomorphism C-. C, .tr--+ zx. Furthcnnorc we have on C the hcnnitian scalar product

$$\langle x, y \rangle = \sum x_\tau y_\tau = Tr(x^{*}y).$$

It is invariant under conjugation, $\underline{(x,y)}$ = (X.. V). and restricting it yields a scalar product (.). i.e., a euclidean metric, on the R-vcctor �pace **R.** If z EC, then '? is the adjoint element with respect to (.). i.e., In **R**, we consider the subspace

$$\mathbf{R}_\pm = \{x \in \mathbf{R} \mid x = x^*\} = \Big[\prod_\tau \mathbb{R}\Big]^+.$$

Thus we find for the components of $x = (x_\tau) \in \mathbf{R}_\pm$ that $x_\tau = x_{\bar\tau} \in \mathbb{R}$. If $\delta \in \mathbb{R}$, we simply write $x > \delta$ to signify that $x_\tau > \delta$ for all τ. The multiplicative group

$$\mathbf{R}_+^* = \{x \in \mathbf{R}_\pm \mid x > 0\} = \Big[\prod_\tau \mathbb{R}_+^*\Big]^+$$

will play a particularly important part. It consists of the tuples $x = (x_\tau)$ of positive real numbers x_τ such that $x_\tau = x_{\bar\tau}$, and it occurs in the two homomorphisms

$$|\ | : \mathbf{R}^* \longrightarrow \mathbf{R}_+^*, \qquad x = (x_\tau) \longmapsto |x| = (|x_\tau|),$$

$$\log : \mathbf{R}_+^* \xrightarrow{\ \sim\ } \mathbf{R}_\pm, \qquad x = (x_\tau) \longmapsto \log x = (\log x_\tau).$$

We finally define the **upper half-space** associated to the $G(\mathbb{C}|\mathbb{R})$-set X by

$$\mathbf{H} = \mathbf{R}_\pm + i\mathbf{R}_+^*.$$

Putting $\operatorname{Re}(z) = \frac{1}{2}(z + \bar z)$, $\operatorname{Im}(z) = \frac{1}{2i}(z - \bar z)$, we may also write

$$\mathbf{H} = \{z \in \mathbf{C} \mid z = z^*, \ \operatorname{Im}(z) > 0\}.$$

If z lies in $\mathbf{H}$, then so does $-1/z$, because $z\bar z \in \mathbf{R}_+^*$, and $\operatorname{Im}(z) > 0$ implies $\operatorname{Im}(-1/z) > 0$, since $z\bar z \operatorname{Im}(-1/z) = -\operatorname{Im}(\bar z^{-1} z \bar z) = \operatorname{Im}(z) > 0$.

For two tuples $z = (z_\tau)$, $p = (p_\tau) \in \mathbf{C}$, the power

$$z^p = (z_\tau^{p_\tau}) \in \mathbf{C}$$

is well-defined by

$$z_\tau^{p_\tau} = e^{p_\tau \log z_\tau},$$

if we agree to take the principal branch of the logarithm and assume that the z_τ move only in the plane cut along the negative real axis. The table

$$\mathbb{H} \subseteq \mathbb{C} \supseteq \mathbb{R} = \mathbb{R} \supseteq \mathbb{R}_+^*, \quad |\ | : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*, \quad \log : \mathbb{R}_+^* \xrightarrow{\ \sim\ } \mathbb{R},$$

$$\mathbf{H} \subseteq \mathbf{C} \supseteq \mathbf{R} \supseteq \mathbf{R}_\pm \supseteq \mathbf{R}_+^*, \quad |\ | : \mathbf{C}^* \longrightarrow \mathbf{R}_+^*, \quad \log : \mathbf{R}_+^* \xrightarrow{\ \sim\ } \mathbf{R}_\pm,$$

shows the analogy of the notions introduced with the familiar ones in the case $n = 1$. We recommend that the reader memorize them well, for they will be used constantly in what follows without special cross-reference. This also includes the notation

$$\bar z,\ z^*,\ {}^*z,\ Tr,\ N,\ \langle\ ,\ \rangle,\ x > \delta,\ z^p.$$

The functional equations we arc envisaging originate in a general formula from functional analysis, the *Puiswn summation formula.* It will be proved tlr5t. A **Schwartz function** (or *rapidly decreasing fum rion)* on a euclidean vector space Risby definition a C'";C-function f : **R--+** which tends to Lero as x --+ oo. even if multiplied by an arbitrary power llx llm, m =:::. 0, and which shares this behaviour with all its derivatives. For every Schwartz function f, one form:;. the **Fourier transform**

$$\{(y) = \int_R f(x)e-2Jr,1<,,\cdot)\,dx,$$

where dx i� the Haar measure on **R** associated to ( ) which ascribe5 the volume I to the cube spanned by an orthonormal basis, i.e.. it is the Haar measure which is selfdual with respect to (.). The improper integral converges ab�olutely and uniformly and gives again a Schwartz function f. This **i,;** ea"ily proved by elementary analytical technique-,; we refer also to !98]. chap. XIV. The prototype of a Schwartz function is the function

$$h(x) =$$

All functional equation.. we are going to prove depend, in the final analysis, on the special property of this function of being its own Fourier transfonn:

(3.1) Proposition. **(i)** *The function* $h(x)$ = e-n(.\,,) i,._ its own Fourier *tran.._fo,m.*

(ii) ff/ is *an 1irbitrary* Schwartz function *and A is* a linear tramfonmllion ofR, *then the funclion* $f_4(x) = /(Ax)$ *has* Fourier *transform*

$$\widehat{f}_A(y) = \frac{1}{|\det A|}\widehat{f}({}^tA^{-1}y),$$

where ${}^1A$ *is the adJoint* transformation of *A.*

Proof: (i) We identify the euclidean vector space **R** with R" via "ome isometry. Then the Haar mea�ure turns into the Lebesgue meaf>urc *dx1 ••• dxn.* Since $h(x)$ = n;'=I 'wehave h = n7=1(t' ;n,C)', �o wc may assume $11 = 1$. Differentiating

$$\widehat{h}(y) = \int h(x)e^{-2\pi ixy}\,dx$$

in y under the integral, we find by partial integration that

$$= -2\pi i \int x h(x) e^{-2\pi i xy}\,dx = -2\pi y h(y).$$

This implies that $h(y) = Ce^{-\pi y^2}$ for some constant C. Putting $y = 0$ yields $C = 1$, since it is well-known that $\int e^{-\pi x^2}dx = 1$.

(ii) Substituting $x \mapsto Ax$ gives the Fourier transform of $f_A(x)$ as:

$$\hat{f}_A(y) = \int f(Ax)e^{-2\pi i\langle x,y\rangle}dx = \int f(x)e^{-2\pi i\langle A^{-1}x,y\rangle}|\det A|^{-1}dx$$

$$= \frac{1}{|\det A|}\int f(x)e^{-2\pi i\langle x,{}^tA^{-1}y\rangle}dx = \frac{1}{|\det A|}\hat{f}({}^tA^{-1}y). \qquad \square$$

From the proposition ensues the following result, which will be crucial for the sequel.

(3.2) Poisson Summation Formula. *Let Γ be a complete lattice in* **R** *and let*

$$\Gamma' = \{ g' \in \mathbf{R} \mid \langle g', g\rangle \in \mathbb{Z} \text{ for all } g \in \Gamma\}$$

be the lattice dual to Γ. Then for any Schwartz function f, one has:

$$\sum_{g\in\Gamma} f(g) = \frac{1}{\operatorname{vol}(\Gamma)} \sum_{g'\in\Gamma'} \hat{f}(g'),$$

where $\operatorname{vol}(\Gamma)$ is the volume of a fundamental mesh of Γ.

Proof: We identify as before **R** with the euclidean vector space $\mathbb{R}^n$ via some isometry. This turns the measure dx into the Lebesgue measure $dx_1 \cdots dx_n$. Let A be an invertible $n \times n$-matrix which maps the lattice $\mathbb{Z}^n$ onto Γ. Hence $\Gamma = A\mathbb{Z}^n$ and $\operatorname{vol}(\Gamma) = |\det A|$. The lattice $\mathbb{Z}^n$ is dual to itself, and we get $\Gamma' = A^*\mathbb{Z}^n$ where $A^* = {}^tA^{-1}$, as

$$g' \in \Gamma' \iff {}^t(An)g' = {}^tn\,{}^tAg' \in \mathbb{Z} \quad \text{for all } n \in \mathbb{Z}^n$$
$$\iff {}^tAg' \in \mathbb{Z}^n \iff g' \in A^*\mathbb{Z}^n.$$

Substituting the equations

$$\Gamma = A\mathbb{Z}^n, \quad \Gamma' = A^*\mathbb{Z}^n, \quad f_A(x) = f(Ax), \quad \hat{f}_A(y) = \frac{1}{\operatorname{vol}(\Gamma)}\hat{f}(A^*y)$$

into the identity we want to prove, gives

$$\sum_{n\in\mathbb{Z}^n} f(n) = \sum_{n\in\mathbb{Z}^n} \hat{f}(n).$$

In order to prove this, let us write f instead of f_A and take the series

$$g(x) = \sum_{k\in\mathbb{Z}^n} f(x+k).$$

It converges absolutely and locally uniformly. For since f is a Schwartz function, we have, if x varies in a compact domain,

$$|f(x+k)|\,\|k\|^{n+1} \le C$$

for almost all $k \in \mathbb{Z}^n$. Hence $g(x)$ is majorized by a constant multiple of the convergent series $\sum_{k\neq 0}\frac{1}{\|k\|^{n+1}}$. This argument works just as well for all partial derivatives of f. So $g(x)$ is a C^∞-function. It is clearly periodic,

$$g(x+n) = g(x) \quad \text{for all } n \in \mathbb{Z}^n,$$

and therefore admits a Fourier expansion

$$g(x) = \sum a_n e^{2\pi i\,{}^t n x},$$

whose Fourier coefficients are given by the well-known formula

$$a_n = \int_0^1 \cdots \int_0^1 g(x) e^{-2\pi i\,{}^t n x}\, dx_1 \ldots dx_n.$$

Swapping summation and integration gives

$$a_n = \int_0^1 \cdots \int_0^1 g(x)\, e^{-2\pi i\,{}^t\mathbf{n} x}\, dx = \sum_{\mathbf{k}\in\mathbb{Z}^n} \int_0^1 \cdots \int_0^1 f(x+\mathbf{k})\, e^{-2\pi i\,{}^t\mathbf{n}x}\, dx$$

$$= \hat{f}(n).$$

It follows that

$$\sum_{n\in\mathbb{Z}^n} f(n) = g(0) = \sum_{n\in\mathbb{Z}^n} a_n = \sum_{n\in\mathbb{Z}^n} \hat{f}(n) \qquad \text{q.e.d.} \qquad \square$$

We apply the Poisson summation formula to the functions

$$f_p(a,b,x) = N((x+a)^p)\, e^{\pi i\langle (x+a)\tau,\, x+a\rangle + 2\pi i\langle b, x\rangle}$$

with the parameters $a, b \in \mathbf{R}$ and a tuple $p = (p_\tau)$ of nonnegative integers such that $p_\tau \in \{0,1\}$ if $\tau = \bar\tau$, and $p_\tau p_{\bar\tau} = 0$ if $\tau \neq \bar\tau$. Such an element

$p \in \Pi$, will henceforth be called **admh,sible.**

(3.3) **Proposition.** *The function f(x) = fp(a. h,.\)* is a Sd1wart/ *function on* **R.** *Its* Fourier *transform* is

$$\widehat{f}(y) = \left[i^{Tr(p)} e^{2\pi i \langle a,b \rangle} \right]^{-1} f_p(-b, a, y).$$

Proof: It is clear that *fi,(a, h,* t) is a Schwartz function, because

$$\left| f_p(a, b, x) \right| = \left| P(x) \right| e^{-\pi \langle a+x, a+x \rangle},$$

for �ome polynomial *P(x).*

Let $p = 0$. By (3.1), the function h(J.) = *e* :rr(i. 1, equals its own Fourie1 lransfonn and one has

$$f(x) = f_0(a, b, x) = h(a + x) e^{2\pi i \langle b, x \rangle}.$$

We therefore obtain

f(y)= ih(a+\)e2:rr,{h.,,e 2:r1,1.v1dx

= *i* h(x)c-2rrr{r-h. *,-a) dx*

= c2rrr{r-h.aJj;(y _ h)

$$= e^{-2\pi i \langle a,b \rangle} e^{-\pi \langle y-b, y-b \rangle + 2\pi i \langle y, a \rangle}$$

$$= e^{2\pi i \langle a,b \rangle} f_0(-b, a, y).$$

For an arbitrary admis1,ible *p,* we get the fonnula by differentiating *p* times the identity

fo(a,h.y) = e lm{a,/Ji *fo(-h.a,y)*

in the variable *a.* No\\- the functions are neither analytic in the individual componcnh *Or* of *a,* nor arc !hc1>c independent of each other, when there exists a couple r *-j.* f. We therefore proceed as follow1>. Let *p* vary over the elements of *X* such that *p* = *p,* and let *rr* run through a �y�tem of representatives of the conjugation classes {r,T) such that r *-j. T.* Since *pT* Pr = 0, we may choose *a* in such a way that *Pa* = 0. Then one has

(a+ i,a + \-) = *L<a1, + \-p)2* C $+ x_\sigma)(a_{\bar\sigma} + x_{\bar\sigma})$

We no\\- differentiate *Pp* times both sides of(*) in the real variable *ap,* for all *p,* and apply *p(T* time� the differential operator

il I (il il)
ilao= 2 il�o- i il7Jo •

for all *a.* Here we con�ider *aii* = *�Fi+* i */Ja* as a function in the real variables t,. */Ja* ("'Wirtinger calculus"). On the left-hand side

.fO(a, *h. y)*= $\int$ *e-rr¹a+1.a* 1 1J+2;r1(h, 1\ e-21r1(t, ,·\ *dx.*

may differentiate under the integral. Then, observing that *pr,* = 0 and + *Xa)(a,r* + *Xo))* = *(aa* + ta), we obtain

$\int$ *TI(-2n(ap* +*xp)} /!p*

P Q(*-2rr(aa+ x"*)) *P" e-TC'u+\.a+-1)+2Jr1\h, ,)-21r1'1, r) dx*

=N((-2;r)1' $\int$ } *N((a+x)P)e* ;r1a+,.11+11-,-21r1(h.1·)e-l;r1(x.v,dx

� *N((-2nc)")];,(a,b,y).*

The right-hand �ide of(*),

$$e^{-2\pi i\langle a,b\rangle-\pi\langle -b+y,\,-b+y\rangle+2\pi i\langle a,y\rangle} = e^{2\pi i\langle a,-b+y\rangle-\pi\langle -b+y,}$$

in view of

(a, *-h+y)* =*L* , *ap(-hp+Yp)+L*₁₁*(arr(-hii+Ya)+ao(-ho* +Yrr)},
, ,

and as *p,r* = 0, becomes accordingly

N ((2rri)"} *N((-h* + *y)") e-hi'a.h\fil(-h.a,* y)

= *N(* (2::rri)") e-2rr1:a.h1*fj,(-h,a.y).*

Hence

$$\widehat{f}_p(a,b,y) = N(i^{-p})e^{\;2\pi i\langle a,b\rangle}f_p(-b,a,y).$$ lJ

We now create our general theta scric� on the upper half-.,pace

H� {'EC|'�,'. Im(,)> 0} � R, + iR�.

(3.4) Definition. *For* every *complete* lattice *I'* of **R,** we *define the* **theta series**

Or(:::) = *L,* *eJr'\½�-is',* *z* EH.
)sEJ'

More generally, foru.h ER *,md any admissible p* E TTrZ, *wcpul*

Oj'.(a,h,z)= *L, N((a+* /?)/!} t'rr1:(a+.d *,u+g1+2:r11h,is).*
KicT

(3.5) Proposition. *The series $\theta_\Gamma^p(a,b,z)$ converges absolutely and uniformly on every compact subset of* $\mathbf{R}\times\mathbf{R}\times\mathbf{H}$.

Proof: Let $\delta\in\mathbb{R}$, $\delta>0$. For all $z\in\mathbf{H}$ such that $\operatorname{Im}(z)\geq\delta$, we find

$$\left|N((a+g)^p)e^{\pi i\langle(a+g)z,a+g\rangle+2\pi i\langle b,g\rangle}\right|\leq\left|N((a+g)^p)\right|e^{-\pi\delta\langle a+g,a+g\rangle}.$$

Let

$$f_g(a)=N\big((a+g)^p\big)\,e^{-\pi\delta\langle a+g,a+g\rangle}\qquad(a\in\mathbf{R},\ g\in\Gamma).$$

For $K\subseteq\mathbf{R}$ compact, put $\|f\|_K=\sup_{x\in K}|f(x)|$. We have to show that

$$\sum_{g\in\Gamma}\|f_g\|_K<\infty.$$

Let $g_1,\dots,g_n$ be a $\mathbb{Z}$-basis of Γ, and for $g=\sum_{i=1}^n m_ig_i\in\Gamma$, let $\mu_g=\max_i|m_i|$. Furthermore, define $\|x\|=\sqrt{\langle x,x\rangle}$. If $\|g\|\geq 4\max_{x\in K}\|x\|$, then for all $a\in K$:

$$\langle a+g,a+g\rangle\geq(\|a\|-\|g\|)^2\geq\|g\|^2-2\|a\|\,\|g\|\geq\frac{1}{2}\|g\|^2\geq\frac{c}{2}\sum_i m_i^2\geq\frac{c}{2}\mu_g^2,$$

where $\|g\|^2=\sum_{i,j=1}^n\langle g_i,g_j\rangle m_im_j$, and c is the smallest eigenvalue of the matrix $(\langle g_i,g_j\rangle)$.

$N((a+\sum m_ig_i)^p)$ is a polynomial of degree q in the m_i, ($q=Tr(p)$), the coefficients of which are continuous functions of a. It follows that

$$\left|N((a+g)^p)\right|\leq\mu_g^{q+1}\quad\text{for all } a\in\mathbf{K},$$

provided μ_g is sufficiently high. One therefore finds a subset $\Gamma'\subseteq\Gamma$ with finite complement such that

$$\sum_{g\in\Gamma'}\|f_g\|_K\leq\sum_{\mu=0}^{\infty}P(\mu)\mu^{q+1}e^{-\pi\delta c\mu^2/2},$$

where $P(\mu)=\#\{\mathbf{m}\in\mathbb{Z}^n\mid\max_i|m_i|=\mu\}=(2\mu+1)^n-(2\mu-1)^n$. The series on the right is clearly convergent. □

From the Poisson summation formula we now get the general

(3.6) Theta Transformation Formula. *One h;.is*

$$O/!,(a,h, - 1/::) = [1T,Cp)l'^{2}ITl(U h)\mathrm{vol}(I')r^{1}N((z/i)"-!)erc-h.a,z).$$

Inparticufor, one has for *the function* $Or(z) = 0Y,(O, 0, ::)$:

$$Hr(-lj,) � \frac{\sqrt{N(.ji)}}{\mathrm{vol}(I')} Hr\bullet(c).$$

Proof: Both sides of the transfonnation formula are holomorphic in : by (3.5). Therefore it suffices to check the identity for $z = iy$, with y ER�. Put $1 = y^{-1}1^{2}$. �o that

$$:= i� \quad \text{and} \quad -1/:= it^{2}.$$

Ob�erving that $t = t^* =*I$, sothat (�t. 11) = (�.*rr1) = (�, fr/), we obtain

$$Uj,(a, h\_, \quad J/:) = N(t-1')\sum_{IfE/'} N((ta+ tg)'') \; C\text{-}IT,1a+1�,1a+tg)\text{-}2.rrrir\text{-}^{1}h.tg^{1}$$

Let $a= ta$, $\beta = ,-^{1}h$. We consider the function

$$fi,(a,/3.,)= N((a+ r)'') \; c\text{-}''r,¥+,.<Y+>\backslash+2.,1,fl.1,$$

and put

$$\varphi_t(\alpha, \beta, x) = f_p(\alpha, \beta, tx).$$

This gives

(l) $$\theta_{I'}^{p}(a, b, -1/z) = N(t^{-p}) \sum_{g\in\Gamma} \varphi_t(\alpha, \beta, g)$$

and :-imilarly $z = i$ -/,s gives that

(2) $$0j',(-h,a.z) = N(tfl) \sum_{g'\in\Gamma'} \varphi_{t^{-1}}(-\beta, \alpha, g')$$

Now apply the Poisson summation formula

(3) $$\sum_{g\in\Gamma} f(g) = \frac{1}{\mathrm{vol}(\Gamma)}$$

to the function

$$f(x) = (\{Jr(a,/3,x) = .t;,(a,fJ,t,\cdot).$$

Its Fourier tran-;form is computed as follows. Let h(.1) = ,-), so that /(r) = $h(tx) = h_1(x)$. The tram,formation A: $x \mapsto lx$ **R** �elf-adjoint and has determinant $N(f)$. **Thu�** (3.1), (ii), gives

$$f(y) = \frac{�}{N(l)} h(t^{1} v).$$

The Fourier transform $\hat h$ has been computed in (3.3). This yields

$$f(y) = [N(i^{\mathfrak p})N(t)e^{2\pi i\langle a,b\rangle}]^{-1}\,\hat\varphi(-\beta, b, t^{-1}y)$$

$$= [N(i^{\mathfrak p})N(t)e^{2\pi i\langle a,b\rangle}]^{-1}\,\varphi_{t^{-1}}(-\beta, a, y).$$

Substituting this into (3) and multiplying by $N(t^{-1})$ gives, by (1) and (2):

$$\theta_\Gamma(a,b,-1/z) = [N(i^{\mathfrak p}t^{2\mathfrak p+1})e^{2\pi i\langle a,b\rangle}]\,\mathrm{vol}(\Gamma)^{-1}\theta_{\Gamma'}(-b,a,z).$$

Since $t = (z/i)^{-1/2}$, i.e., $(t^{2\mathfrak p+1})^{-1} = (z/i)^{\mathfrak p+1/2}$, this is indeed the transformation formula sought. □

For $n = 1$, we obtain proposition (2.3), which at the time was used without proof for proving the functional equation of the Dirichlet L-series (and Riemann's zeta function).

§ 4. The Higher-dimensional Gamma Function

The passage from theta series to L-series in § 1 and § 2 was afforded by the gamma function

$$\Gamma(s) = \int_0^\infty e^{-y}y^s\frac{dy}{y}.$$

In order to generalize this process, we now introduce a higher-dimensional gamma function for every finite $G(\mathbb C|\mathbb R)$-set X, building upon the notation of the last section. First we fix a Haar measure on the multiplicative group $\mathbf R_+^*$.

Let $\mathfrak p = \{\tau, \bar\tau\}$ be the conjugation classes in X. We call $\mathfrak p$ real or complex, depending whether $\#\mathfrak p = 1$ or $\#\mathfrak p = 2$. We then have

$$\mathbf R_+^* = \prod_{\mathfrak p}\mathbf R_{+\mathfrak p}^*,$$

where

$$\mathbf R_{+\mathfrak p}^* = \mathbb R_+^*, \quad \text{resp.} \quad \mathbf R_{+\mathfrak p}^* = \left[\,\mathbb R_+^* \times \mathbb R_+^*\right]^+ = \left\{(y,y) \mid y \in \mathbb R_+^*\right\}.$$

We define isomorphisms

$$\mathbf R_{+\mathfrak p}^* \xrightarrow{\ \sim\ } \mathbb R_+^*$$

by $y \mapsto y$, resp. $(y,y) \mapsto y^2$, and obtain an isomorphism

$$\mathbf R_+^* \xrightarrow{\ \sim\ } \prod_{\mathfrak p}\mathbb R_+^*.$$

We now denote by $\frac{dy}{y}$ the Haar measure on $\mathbf{R}_+^*$ which corresponds to the product measure

$$\prod_{\mathfrak p} \frac{dt}{t}$$

where $\frac{dt}{t}$ is the usual Haar measure on $\mathbb{R}_+^*$. The Haar measure thus defined is called the **canonical measure on $\mathbf{R}_+^*$.** Under the logarithm

$$\log : \mathbf{R}_+^* \xrightarrow{\ \sim\ } \mathbf{R}_\pm ,$$

it is mapped to the Haar measure dx on $\mathbf{R}_\pm$ which under the isomorphism

$$\mathbf{R}_\pm = \prod_{\mathfrak p} \mathbf{R}_{\pm\mathfrak p} \xrightarrow{\ \varphi\ } \prod_{\mathfrak p} \mathbb{R} ,$$

$x_{\mathfrak p} \mapsto x_{\mathfrak p}$, resp. $(x_{\mathfrak p}, \bar x_{\mathfrak p}) \mapsto 2x_{\mathfrak p}$, corresponds to the Lebesgue measure on $\prod_{\mathfrak p} \mathbb{R}$.

(4.1) Definition. *For $\mathbf{s} = (s_\tau) \in \mathbf{C}$ such that $\operatorname{Re}(\mathbf{s}) > 0$, we define the* **gamma function** *associated to the $G(\mathbb{C}|\mathbb{R})$-set X by*

$$\Gamma_X(\mathbf{s}) = \int_{\mathbf{R}_+^*} N(e^{-\mathbf{y}} \mathbf{y}^{\mathbf{s}}) \frac{d\mathbf{y}}{\mathbf{y}} .$$

The integrand is well-defined, according to our conventions from p. 445, and the convergence of the integral can be reduced to the case of the ordinary gamma function as follows.

(4.2) Proposition. *Decomposing the $G(\mathbb{C}|\mathbb{R})$-set X into its conjugation classes $\mathfrak p$, one has*

$$\Gamma_X(\mathbf{s}) = \prod_{\mathfrak p} \Gamma_{\mathfrak p}(\mathbf{s}_{\mathfrak p}),$$

where $\mathbf{s}_{\mathfrak p} = s_\tau$ for $\mathfrak p = \{\tau\}$, resp. $\mathbf{s}_{\mathfrak p} = (s_\tau, s_{\bar\tau})$ for $\mathfrak p = \{\tau, \bar\tau\}$, $\tau \neq \bar\tau$. The factors are given explicitly by

$$\Gamma_{\mathfrak p}(\mathbf{s}_{\mathfrak p}) = \begin{cases} \Gamma(\mathbf{s}_{\mathfrak p}), & \text{if } \mathfrak p \text{ real,} \\ 2^{1-Tr(\mathbf{s}_{\mathfrak p})}\,\Gamma(Tr(\mathbf{s}_{\mathfrak p})), & \text{if } \mathfrak p \text{ complex,} \end{cases}$$

where $Tr(\mathbf{s}_{\mathfrak p}) = s_\tau + s_{\bar\tau}$.

Proof: The first statement is clear in view of the product decomposition

$$\Big(\mathbf{R}_+^*, \frac{dy}{y}\Big) = \prod_{\mathfrak p}\Big(\mathbf{R}_{+,\mathfrak p}^*, \frac{dy_{\mathfrak p}}{y_{\mathfrak p}}\Big)$$

The second is relative to a $G(\mathbb{C}|\mathbb{R})$-set X which has only one conjugation class. If $\#X = 1$, then trivially $\Gamma_X(s) = \Gamma(s)$. So let $X = \{\tau, \bar\tau\}$, $\tau \neq \bar\tau$. Mapping

$$\psi : \mathbb{R}_+^* \longrightarrow \mathbf{R}_+^*, \quad t \longmapsto (\sqrt{t}, \sqrt{t}),$$

one then gets

$$\int_{\mathbf{R}_+^*} N(e^{-y}y^{s})\frac{dy}{y} = \int_{\mathbb{R}_+^*} N\big(e^{-\psi(t)}\psi(t)^{s}\big)\frac{dt}{t}$$

$$= \int_{\mathbb{R}_+^*} e^{-2\sqrt{t}}\, t^{Tr(s)/2}\frac{dt}{t}$$

and, since $d(t/2)^2/(t/2)^2 = 2dt/t$, the substitution $t \mapsto (t/2)^2$ yields

$$\int_{\mathbf{R}_+} N(e^{-y}y^{s})\frac{dy}{y} = 2^{1-Tr(s)}\Gamma(Tr(s)). \qquad \square$$

The proposition shows that the gamma integral $\Gamma(s)$ converges for $s = (s_\tau)$ with $\mathrm{Re}(s_\tau) > 0$, and admits an analytic continuation to all of $\mathbf{C}$, except for poles at points dictated in the obvious way by the ordinary gamma function $\Gamma(s)$.

We call the function

$$L_X(\mathbf{s}) = N(\pi^{-\mathbf{s}/2})\Gamma_X(\mathbf{s}/2)$$

the **L-function** of the $G(\mathbb{C}|\mathbb{R})$-set X. Decomposing X into the conjugation classes $\mathfrak p$, yields

$$L_X(\mathbf{s}) = \prod_{\mathfrak p} L_{\mathfrak p}(\mathbf{s}_{\mathfrak p}),$$

where as before we write $\mathbf{s}_{\mathfrak p} = s_\tau$ for $\mathfrak p = \{\tau\}$ and $\mathbf{s}_{\mathfrak p} = (s_\tau, s_{\bar\tau})$ for $\mathfrak p = \{\tau, \bar\tau\}$, $\tau \neq \bar\tau$. The factors $L_{\mathfrak p}(\mathbf{s}_{\mathfrak p})$ are given explicitly, by (4.2), as

$$L_{\mathfrak p}(\mathbf{s}_{\mathfrak p}) = \begin{cases} \pi^{-\mathbf{s}_{\mathfrak p}/2}\Gamma(\mathbf{s}_{\mathfrak p}/2), & \text{if } \mathfrak p \text{ real},\\ 2(2\pi)^{-Tr(\mathbf{s}_{\mathfrak p})/2}\Gamma(Tr(\mathbf{s}_{\mathfrak p})/2), & \text{if } \mathfrak p \text{ complex}.\end{cases}$$

For a single complex variable $s \in \mathbb{C}$, we put

$$\Gamma_X(s) = \Gamma_X(s\mathbf{1}),$$

where $\mathbf{1} = (1, \dots, 1)$ is the unit element of $\mathbb{C}$. Denoting r_1, resp. r_2, the number of real, resp. complex, conjugation classes of X, we find

$$\Gamma_X(s) = 2^{(1-2s)r_2}\,\Gamma(s)^{r_1}\,\Gamma(2s)^{r_2}.$$

In the same way we put

$$L_X(s) = L_{X}(s\mathbf{1}) = \pi^{-ns/2}\,\Gamma_X(s/2), \quad n = \#X,$$

and in particular

$$L_{\mathbb{R}}(s) = L_X(s) = \pi^{-s/2}\Gamma(s/2), \quad \text{if } X = \{\tau\},$$

$$L_{\mathbb{C}}(s) = L_X(s) = 2(2\pi)^{-s}\Gamma(s), \quad \text{if } X = \{\tau, \bar\tau\},\ \tau \neq \bar\tau.$$

Then we have, for an arbitrary $G(\mathbb{C}|\mathbb{R})$-set X:

$$L_X(s) = L_{\mathbb{R}}(s)^{r_1} L_{\mathbb{C}}(s)^{r_2}.$$

With this notation, (1.2) implies the

(4.3) Proposition. (i) $L_{\mathbb{R}}(1) = 1$, $L_{\mathbb{C}}(1) = \frac{1}{\pi}$.

(ii) $L_{\mathbb{R}}(s+2) = \frac{s}{2\pi} L_{\mathbb{R}}(s)$, $L_{\mathbb{C}}(s+1) = \frac{s}{2\pi} L_{\mathbb{C}}(s)$.

(iii) $L_{\mathbb{R}}(1-s)L_{\mathbb{R}}(1+s) = \dfrac{1}{\cos \pi s/2}$, $\quad L_{\mathbb{C}}(s)L_{\mathbb{C}}(1-s) = \dfrac{2}{\sin \pi s}$.

(iv) $L_{\mathbb{R}}(s)L_{\mathbb{R}}(s+1) = L_{\mathbb{C}}(s)$ **(Legendre's duplication formula).**

As a consequence we obtain the following functional equation for the L-function $L_X(s)$:

(4.4) Proposition. $L_X(s) = A(s) L_X(1-s)$ *with the factor*

$$A(s) = (\cos \pi s/2)^{r_1+r_2}(\sin \pi s/2)^{r_2} L_{\mathbb{C}}(s)^{r_2}.$$

Proof: On the one hand we have

$$\frac{L_{\mathbb{R}}(s)}{L_{\mathbb{R}}(1-s)} = \frac{L_{\mathbb{R}}(s)L_{\mathbb{R}}(1+s)}{L_{\mathbb{R}}(1-s)L_{\mathbb{R}}(1+s)} = \cos \pi s/2\, L_{\mathbb{C}}(s),$$

and on the other

$$\frac{L_{\mathbb{C}}(s)}{L_{\mathbb{C}}(1-s)} = \frac{L_{\mathbb{C}}(s)L_{\mathbb{C}}(s)}{L_{\mathbb{C}}(1-s)L_{\mathbb{C}}(s)} = \frac{1}{2}\sin \pi s\, L_{\mathbb{C}}(s)^2$$

$$= \cos \pi s/2 \,\sin \pi s/2\, L_{\mathbb{C}}(s)^2.$$

The proposition therefore results from the identity $L_X(s) = L_{\mathbb{R}}(s)^{r_1} L_{\mathbb{C}}(s)^{r_2}$. $\square$

Thi� conclude& the purely function-theoretic preparations. They will now be applied to number theory.

§ 5. The Dedekind Zeta Function

The Riemann zeta function ((s) $= L$�$_1$"[> is associated with the field Q of rational numbers. It generalizes in the following way to an arbitrary number field K of degree 11 $= [K:$:Qi].

(5.1) Definition. *The* **Dedekind** zeta **function** of *the number field K is defined by the .�eries*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}\,,$$

where a varies over *the integral ideals* of *K, and* O't(a) *denotes their :ibsolute*

(5.2) **Proposition.** *The series (K* (�) converge *abi,,olutely :.md* uniformly *in the domain* Rc(.1·) � I $+ 8$ for *every* $8 > 0$, *and* one *ha&*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}}\,,$$

where � nms *through the prime ideals of K.*

The proof proceeds in the same way as for the Riemann zeta l'unction (sec (1.1)), hecau"e the absolute nonn O't(a) is multiplicative. We do not go into it here, because it is the same argument that also applie� to *Hee/. (:' L-sai(:'s,* which will be introduced in 98 as a common generalintion of Dirichlet L-serie" and of the Dedekind zeta function.

Ju�l like the Riemunn zeta function, the Dedekind Leta function also admit� an analytic continuation to the complex plane with I removed, and it satbfies a functional equation relating the argument s to I - s. This is what we are now going to prove. The argument will turn out to he a higher dimensional gencrali.t:ation of the one used in 9 I for the Riemann zeta function.

First we split up the series $\zeta_K(s)$, according to the classes $\mathfrak{K}$ of the usual ideal class group $Cl_K = J/P$ of K, into the **partial zeta functions**

$$\zeta(\mathfrak{K},s) = \sum_{\substack{\mathfrak{a}\in\mathfrak{K}\\ \text{integral}}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s},$$

so that

$$\zeta_K(s) = \sum_{\mathfrak{K}} \zeta(\mathfrak{K},s).$$

The functional equation is then proved for the individual functions $\zeta(\mathfrak{K},s)$. The integral ideals in $\mathfrak{K}$ are described as follows. If $\mathfrak{a}$ is a fractional ideal, then the unit group $\mathcal{O}^*$ of $\mathcal{O}$ operates on the set $\mathfrak{a}^* = \mathfrak{a} \setminus \{0\}$, and we denote by $\mathfrak{a}^*/\mathcal{O}^*$ the set of orbits, i.e., the set of classes of non-zero associated elements in $\mathfrak{a}$.

(5.3) Lemma. *Let $\mathfrak{a}$ be an integral ideal of K and $\mathfrak{K}$ the class of the ideal $\mathfrak{a}^{-1}$. Then there is a bijection*

$$\mathfrak{a}^*/\mathcal{O}^* \xrightarrow{\sim} \{\mathfrak{b}\in\mathfrak{K} \mid \mathfrak{b} \text{ integral}\}, \quad a \mapsto \mathfrak{b} = a\mathfrak{a}^{-1}.$$

Proof: If $a \in \mathfrak{a}^*$, then $a\mathfrak{a}^{-1} = (a)\mathfrak{a}^{-1}$ is an integral ideal in $\mathfrak{K}$, and if $a\mathfrak{a}^{-1} = b\mathfrak{a}^{-1}$, then $(a) = (b)$, so that $ab^{-1} \in \mathcal{O}^*$. This shows the injectivity of the mapping. But it is surjective as well, since for every integral $\mathfrak{b} \in \mathfrak{K}$, one has $\mathfrak{b} = a\mathfrak{a}^{-1}$ with $a \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$. $\square$

To the $G(\mathbb{C}|\mathbb{R})$-set $X = \operatorname{Hom}(K,\mathbb{C})$ corresponds the Minkowski space

$$K_{\mathbb{R}} = \mathbb{R}^n = \Big[\prod_{\tau}\mathbb{C}\Big]^+.$$

The field K may be embedded into $K_{\mathbb{R}}$. Then one finds for $a \in K^*$ that

$$\mathfrak{N}((a)) = |N_{K|\mathbb{Q}}(a)| = |N(a)|,$$

where N denotes the norm on $\mathbb{R}^n$ (see chap. I, § 5). The lemma therefore yields the

(5.4) Proposition. $\displaystyle \zeta(\mathfrak{K},s) = \mathfrak{N}(\mathfrak{a})^s \sum_{a\in\mathfrak{a}^*/\mathcal{O}^*} \frac{1}{|N(a)|^s}.$

By chap. I, (5.2), the ideal $\mathfrak{a}$ forms a complete lattice in $\mathbb{R}^n$ whose fundamental mesh has volume

$$\operatorname{vol}(\mathfrak{a}) = \sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}),$$

where *da* = �*(a)²1dK* I denotes the absolute value of the di1>criminant of *a,* and *dK* is the discriminant of *K.* To the series ((Jl,s) we a5sot:iate the theta series

$$\theta(\mathfrak{a}, z) = \theta_{\mathfrak{a}}(z/d_{\mathfrak{a}}^{1/n}) = \sum e^{\pi i (az/d_{\mathfrak{a}}^{1/n}, a)}$$

It is related to ((Jl,s) via the gamma integral associated lo the G(CIIR)�set *X = 1-Iom(K,C),*

I'K(I) = *I'x(s)* = $\int N(e^{-y} y^{s}) \frac{dy}{}$

",

wheres E *Re(s)* > 0 (1,ee (4.1)). In the integral, we substitute

y f------+ *rrlal²y/d�/n*

with I I denoting the map R* _,,. R�. (x,) i---+ (lxrl). We then ohtain

IdK I'n-"'*I'K(s)* IN(a)12' �(a)².1 = ∫ e-:rr(ar;J" 1,,, *.a)N(y)'* Jy y.

R'.

Summing thir,, over a full system 91. of representative� of 0⁴ */O*,* yields

$$|d_K|^s \pi^{\;ns} \Gamma_K(s)\zeta(\mathfrak{K}, 2s) = \int_{\mathbf{R}_+^*} g(y) N(y)^s \frac{dy}{y}$$

with the 1,eries

g(y) =

Swapping summation and integration i� legal, for the same rca<.on a� in the case of the Riemann Leta function (seep. 422). We view the function

Zcx_(s) = *IdKl·'12n* *11'i²rK(s/2)* = lthl•'i²Lx(.1)

a1> the "Euler factor at infinity" of the zeta function ((Jl..1) (1,ee *4, p.455) and define

Z(Jl,s) = Z""(.1)({.R,s).

The desire to reali/e this function as an integral over the theta �eric� *0(a.* s) is frustrated by the fact that in the theta seric.:, we 1,um over *all a* E *a,* whereas summation in the '-Cries *g(y)* is only over a s,y1,lem of repre�entalivc<, of *a*/o*.* This difficulty - which was already hinted at in the ca�c of the Riemann zeta function - will now be overcome in the general ca1>c a� follow1>.

The image $|\mathcal{O}^*|$ of the unit group under the mapping $|\ |: \mathbf{R}^* \to \mathbf{R}^*_+$ is contained in the **norm-one** hypersurface

$$\mathbf{S} = \{ x \in \mathbf{R}^*_+ \mid N(x) = 1 \}.$$

Writing every $y \in \mathbf{R}^*_+$ in the form

$$y = x t^{1/n}, \quad x = \frac{y}{N(y)^{1/n}}, \quad t = N(y),$$

we obtain a direct decomposition

$$\mathbf{R}^*_+ = \mathbf{S} \times \mathbb{R}^*_+ .$$

Let d^*x be the unique Haar measure on the multiplicative group $\mathbf{S}$ such that the canonical Haar measure dy/y on $\mathbf{R}^*_+$ becomes the product measure

$$\frac{dy}{y} = d^*x \times \frac{dt}{t}.$$

We will not need any more explicit description of d^*x.

We now choose a fundamental domain F for the action of the group $|\mathcal{O}^*|^2 = \{ |\varepsilon|^2 \mid \varepsilon \in \mathcal{O}^* \}$ on $\mathbf{S}$ as follows. The logarithm map

$$\log : \mathbf{R}^*_+ \to \mathbf{R}_\pm, \quad (x_\tau) \mapsto (\log x_\tau),$$

takes the norm-one hypersurface $\mathbf{S}$ to the trace-zero space $H = \{ x \in \mathbf{R}_\pm \mid Tr(x) = 0 \}$, and the group $|\mathcal{O}^*|^2$ is taken to a complete lattice Γ in H (Dirichlet's unit theorem). Choose F to be the preimage of an arbitrary fundamental mesh of the lattice 2Γ. Any such choice satisfies the

(5.5) Proposition. *The function* $Z(\mathfrak{a}, 2s)$ *is the Mellin transform*

$$Z(\mathfrak{a}, 2s) = L(f, s)$$

of the function

$$f(t) = f_F(\mathfrak{a}, t) = \frac{1}{w} \int_F \theta(\mathfrak{a}, ixt^{1/n})\, d^*x$$

where $w = \#\mu(K)$ *denotes the number of roots of unity in* K.

Proof: Decomposing $\mathbf{R}^*_+ = \mathbf{S} \times \mathbb{R}^*_+$, we find

$$Z(\mathfrak{a}, 2s) = \int_0^\infty \int_F \sum e^{-\pi \langle a x t^{1/n}, a \rangle}\, d^*x\, t^s \frac{dt}{t},$$

with $t' = (tjd")^{1}1^{11}$_ The fundamental domain F cuts up the nonn-onc hyperwrfacc S into the disjoint union

$$S= \quad ry2F.$$

The transformation x i---+ $ry2$ r of S leaves the Haar measure d^*x invariant and maps F to $r?F$, so that

$$\int_{\mathbf{S}} \sum_{a\in\mathfrak{R}} e^{-\pi\langle axt',a\rangle}\, d^*x = \int_{\eta^2 F} \sum_{a\in\mathfrak{R}} e^{-\pi\langle axt',a\rangle}\, d^*x$$

= _!f_ L L ('-::r,uu1'.a1-)d*x
w cco•ac:ll
r

�_I_ j(e(a.;.n'1") - 1) J•x � f(I) - l(oc).
U'
F

Observe here that we have to divide by 11J $= \#1l(K)$, bccau�e $/L(K)$ is just the kernel of ---+ 1t1*l (sec chap.I. (7.1)). hence Litl = ¾L'°- Ob�erve furthcnnore that at: runs through the :,ct a* = a " {O) exactly once, and finally that /(oc) = �.J� d*x, as A(a.ix:::,o) = I. This rc�ult doe� indeed show that

Z(K2.,)� j(i(t)-f(oc))r''¥-�L(f.,). n
"

Using this proposition, the functional equation for the function Z (Jl. s) follows via the Mellin principle from a corresponding transformation formula for the function f",:(a. t), which in turn derive� from the general theta transfonnation fonnula (3.6). In order to find the prcci<,c equation, we have to compute the volume vol(F) of the fundamental domain P with re�pect to d* \. and the lattice which is dual to a in **R.** This i� achieved by the following two lemmas.

(5.6) **Lemma.** *The tlindamental* domain F of S *has the* fol/owing *volume with* respect to d* \ :

$$\mathrm{vol}(F) = 2^{r-1}R\,,$$

where r i:. the number of infinite place,; and R is *!he* **regulator** of K (see *chap.* I, (7.5)).

Proof: The canonical measure dy/y on **R�** is transformed into the product measure d^*x x dt/I hy the isomorphism

$$a:SxR�\text{-----}+R:,\qquad (x,f)i \text{------} +xt^1 1^{11}.$$

Since *I=* */t* E IR: 11 *:St :Se)* has measure I with respect to *dt/t,* the quantity vol(F) is also the volume of *F* x *I* with respect to *d*.,* x *dt/t,* i.e., the volume of *a(F* x /) with respect to *dy/y*. The compo�itc *ifr* of the isomorphbms

$$R�� \quad R\_i\_ � \quad \prod_{P \models} lFt = R'$$

(see S4, p. 454) transforms dy/y into the Lebesgue measure of *IF!.*[1],

$$\text{vol(F)} � \text{vol}_0, (v,a(F \text{ x } I))$$

Let *w,* compute the image *ifra(F* x *1).* Let **1** =(I. ...., **I)EST.** hen we find

$$\text{ifra((l,t))} = clogt^{11}n = �elogt$$

with the vector e = (ep$_1$, ... , ep,) E *!Rr, ep* = I, re'-p. = 2, depending whether p$_1$ is real or complex. By definition of *F,* we also have

$$\psi\alpha(F \times \{1\}) = 2\Phi$$

where <*P* denote:. a fundamental mesh of the unit lallice *G* in trace-tern space *JI=* {(x,) E IR' I *Lx,* = 0). Thb gives

$$v,a(F \text{ x } I) � 2<P + [0. �]\text{ c.}$$

the parallelepiped �panned hy the vectors $2e_1 \ldots 2c,\_1$. *i* c. if c$_1$. , c, _1 span the fundamental mesh <*P*. Its volume is *t2*$^{t}_{-}$**1** times the absolute value of the determinant

$$\det\begin{pmatrix} \text{'''} & e, & \text{L,} & Ce,) \\ : & & & \\ \text{,,,} & c,\text{-}1,, & & <p, \end{pmatrix}$$

Adding the first *r* - I lines to the last one, all entries of the last line become zero, except the last one. which is *11* = *L* ep,. The matrix above these zeroes has the absolute value of its determinant by definition equal to the regulalOr *R.* Thus we get

$$\text{vol(F)} = 2^1\text{-IR}. \qquad \square$$

(5.7) **Lemma.** *The lattice I" in* **R** *which is dual to lhe lattice I' = a* is *given by*

$$^*\Gamma' = (\mathfrak{a}\mathfrak{d})^{-1},$$

where *the aMerisk denotes the involution* (xT) r---+ (" T) *on KR 1:md* () *the different* of *K* IQ.

Proof: As (x._v) = fr(�ly). we have

T' ~ /'a E **R** | (N.*a)* E Z foe all *a* E a} ~ |X E **R** | *T,·(xu)* C:: Z j

Tr(xa) £ Z implies immediately *x* E *K,* for if a_1 *,an* if, a Z-baf,if, of *a* and *x* = x1a1 +· · ·+*XnIln,* with *x,* ER., then *Tr(xa1)* = *L, x1* E Z i,; a system of linear equations with coefficient� *Tr(a,a;)* = E Q. so all *x,* E QI, and thut. *x* E *K.* Il follows lhat

'*r*· ~ {*x* E *K* | *h(xa)* C:: Z | .

By dclinition we have ()-I = {x E *K* | £ Z}, and we obtain the equivalences *x* E� *I"* � *TrKI,(J(xao)* £ for all *a* E *a* � *xa* £ ()-1 �XE(u())-1. n

(5.8) **Proposition.** *The* functions *fF(a,t) satisfy the transfonmition formula*

fF(a,})=t^112^*f{.* 1((0())-^1^,t),

and one ha.

$$f_F(\mathfrak{a},t) = \frac{2^{r-1}}{w}\, R + O(e^{-ct^{1/n}}) \qquad \textit{fixt----+}\ \infty,\ t > 0.$$

Proof: We make Uf,e of fonnula (3.6)

$$\theta_\Gamma(-1/z) = \frac{\sqrt{N(z/i)}}{\mathrm{vol}(\Gamma)}\,\theta_{\Gamma'}(z)$$

for the lattice *I'* in **R,** whose fundamental mesh ha,; volume vol(I') = IJ1(a)ld« The lattice *I"* dual to *r* it. by (5.7) a<, **I"* = (aD) 1. compatibility ();z. *g) = implies that *Or(:::)= O,r(z).* Furthermore we have

d(aiJJ-1 = IJ1(a)-²1J1(D) ²*ld«* I= l/(IJ1(a)²ld« ll = 1/da.

The trant.fonnation r r---+ *x·* 1 of the multiplicative group S fixes the Haar measure d^*x (in !he same way as x r---+ -r fixes a Haar measure on *JR.n)* and maps the fundamental domain F onto the fundamental domain p-[1], whose image log(p-[1]) is again a fundamental mesh of the lattice 2 log lo* I. Observing that $N(x(tda)^{1}i'') = tda$ for x ES, we obtain

fr(a �) � ± $/_F$ 0,(;,;':/fd:) $d'x$

? ± f e,(-w,':/td:),r.,

p-,

=-;;; I (fd)l/2 / vo�(a) O(aw1(ix�)tr.,

r-1

= ,::., 2 / e(aw1(i..j1Jd(ao)-1)d*x

/'-I

$= t1/2fi'$ -1((ai'l)-1,1)

This 5hows the first formula. To prove the �ecoml. we write

(F(a,t)=-l;, / lrx+; (A(a,ixt lln)-l)d�x= V_o l(F_)+r(t).

F <

[he function $r(t)$ satlsties $r(t) = O(e^{-''1''})$ $c > 0$, t ---,. ex;, a� the summand� of $\theta(\mathfrak{a}, ixt^{1/n})$ - 1 are of the form

$$e^{-\pi (ax,a)\sqrt[n]{t'}}, \quad a \in \mathfrak{a},\ a \neq 0,\ t' = t/d_{\mathfrak{a}}.$$

The point $x = (x,)$ varic� in the compact clo�ure $F,;;$ [nr IR:]- of F. Hence Xr 2: 0 > 0 for all r, i.e.,

$$(a.\backslash,a) = L \ |w|^2 x, \ 2: O(a.a)$$

and so

$r(t)$:':: vo:�JF) (OaU8Vf')- I).

Writing m = min{(a,a) I a Ea.a -1- 0\ and M = #\a Eal (a.a)= m), ii follows that

$$\theta_{\mathfrak{a}}\big(i\delta\sqrt[n]{t'}\big) - 1 = \qquad + \ L \quad {}^{\cdot\pi\delta((a,a)-m)\sqrt[n]{t'}}\Big) = O(e^{-ct^{1/n}})$$

where (= Jr8m/dl/n We thus get a:,, claimed

$$/F(a, I)= \frac{\mathrm{vol}(F)}{U'} + O(c\_,11 ''=) \quad ? \quad \frac{R}{w} + O(c\text{-}111 '').$$ □

This last proposition now enables us to apply the Mellin principle (1.4) to the functions $f_F(\mathfrak{a}, t)$. For the partial zeta functions,

this yields the following result, where the notations d_K, R, w, and r signify as before the discriminant, the regulator, the number of roots of unity and the number of infinite places, respectively.

(5.9) **Theorem.** *The function*

$$Z(\mathfrak{K}, s) = Z_\infty(s)\zeta(\mathfrak{K}, s), \quad \operatorname{Re}(s) > 1,$$

$Z_\infty(s) = |d_K|^{s/2}\pi^{-ns/2}\Gamma_K(s/2)$, *admits an analytic continuation to* $\mathbb{C} \setminus \{0, 1\}$ *and satisfies the functional equation*

$$Z(\mathfrak{K}, s) = Z(\mathfrak{K}', 1-s),$$

where the ideal classes $\mathfrak{K}$ *and* $\mathfrak{K}'$ *correspond to each other via* $\mathfrak{K}\mathfrak{K}' = [\mathfrak{d}]$. *It has simple poles at* $s = 0$ *and* $s = 1$ *with residues*

$$-\frac{2^r}{w}R, \quad \text{resp.} \quad \frac{2^r}{w}R.$$

Proof: Let $f(t) = f_F(\mathfrak{a}, t)$ and $g(t) = f_{F^{-1}}((\mathfrak{a}\mathfrak{d})^{-1}, t)$. Then (5.8) implies

$$f\left(\frac{1}{t}\right) = t^{n/2}g(t)$$

and

$$f(t) = a_0 + O(e^{-ct^{1/n}}), \quad g(t) = a_0 + O(e^{-ct^{1/n}}),$$

with $a_0 = \frac{2^{r-1}}{w}R$. Proposition (1.4) thus ensures the analytic continuation of the Mellin transforms of f and g, and the functional equation

$$L(f, s) = L\left(g, \frac{n}{2} - s\right)$$

with simple poles of $L(f, s)$ at $s = 0$ and $s = \frac{n}{2}$ with residues $-a_0$, resp. a_0. Therefore

$$Z(\mathfrak{K}, s) = L\left(f, \frac{s}{2}\right)$$

admits an analytic continuation to $\mathbb{C} \setminus \{0, 1\}$ with simple poles at $s = 0$ and $s = 1$ and residues

$$-2a_0 = -\frac{2^r}{w}R, \quad \text{resp.} \quad 2a_0 = \frac{2^r}{w}R$$

and :,,ati�fies the functional equation

$$Z(\mathfrak{K}, s) = L\Big(f, \frac{s}{2}\Big) = L\Big(g, \frac{1-s}{2}\Big) = Z(\mathfrak{K}', 1-s). \qquad \square$$

This theorem about the partial Leta functions immediately implies an analogow, result for the **completed zeta function** of the number field *K,*

ZK(s) = *L,::_(s)(K(s)* = LZ(Jt,,1).

(5.10) Corollary. *The completed zeta function* ZA (5) *1:1dmib an analytic continuation to* C "- {O, I) *and* satisfies *the functional eqwition*

$$Z_K(s) = Z_K(1-s).$$

It has *simple poles* at., = 0 *and* .1 = I *with* residues

$$\frac{2^r hR}{w}, \quad \textit{resp.} \quad \frac{2^r hR}{w},$$

where h is the c/w,s number of *K.*

The last result can be immediately generalized as follows. For every character

X: *J/P*-------+ .51

of the ideal cla:,,s group, one may form the zeta function

$$Z(\chi, s) = Z_\infty(s)\zeta(\chi, s),$$

where

x(a)
'll(a)'

and *x(a)* denotes the value *x(R}* of the class f-t = lo] of an ideal *a.* Then dearly

Z(x..,) � I : x(JlJZ(.<L,).

and in view of .ff' = .R [1]10], we obtain from (5.9) lhc functional equation

Z(x ..,) � x(O)Z(x. I - .,).

If *x #-* **I,** then *Z(x,* �) is ho\omorphic on all of:['._ a:-, :[;11 *x(m* = 0.

We now conclude with the original Dedekind zeta function

$$(K(s)=L_{a}\ \text{�}\text{•}1(a)^{1} \qquad \mathrm{Rc}(s) > \mathrm{I}$$

The Euler factor at infinity, Zc,o(s), i� given explicitly by §4 a�

$$2\text{-.,Js}) = ldKl'\cdot/^{2}Lx(.'i) = ldKl^{512}Llli.(sY^{1}LcC1f^{2}.$$

where r_1, resp. $r2$, denotes the number of real, resp. complex, place�. By (4.3), (i), one has L,_,(l) $=$ $ldK\ 1^{1}/^{2}/nr^{1}$. As

$$(K(s) = \mathrm{Z,x,(1)}\text{-}^{1}ZK(s) = ldK\ 1\text{-}s/^{2}Lx(s)\ ^{1}ZK(S),$$

we obtain from (4.4) the

(5.ll) Corollary. (i) *The Dedekind* zc/1:l *function* (K(.1·) *has* an *analytic continuation to* C '- !I}.

(ii) *Ats=* I *it has a simple pole with residue*

$$\frac{2r^{1}(2nY''}{!<:= \underline{wldKil/2hR=hR/e''}.}$$

Here *h denote.� the class number* and

$$.\mathrm{R} = \log$$

the genus of *l11e number field K (see chap.* III, (3.5)).

(iii) *It s,iti.�fks the functional* equation

$$'_K(1-s) = A(s)\zeta_K(s)$$

with the factor

$$A(s) = {}^{1}\!d_K|^{s-\frac{1}{2}}\Big(\cos\frac{\pi s}{2}\Big)^{r_1+r_2}\Big(\sin\frac{\pi s}{2}\Big)^{r_2}L_{\mathbb{C}}(s)^{n}.$$

The proof of the analytic continuation and functional equation of the Dedekind zeta function was first given by the mathematician *ERtC/1 H1cKt* (1887-1947). along the <;ame general lines we have pre�ented here, albeit in a somewhat different fonnulation. Further, the theory we are about to develop in the following section"§ §6-8 also substantially goe� back to *Hf.CKE*

The formul.i for the residue

$$\mathrm{es}_{s=1}\,\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}}{w|d_K|^{1/2}}hR$$

is commonly known as the analytic class **number formula.** It doe1, allow us to delcnnine the class number *h* of the field *K,* provided we know the law for the decompo�ition of primes in this field sufficiently well to lay our hands on the Euler product and thu1, compute the .t:eta function.

The following Hpplication of corollary (5.11) to Dirichlet L-series *L(x, s)* (see *2) i� highly remarkable, It results from studying the Dedekind zeta function *(K* (s) for the licld K = Q(μ,,,,) of m-th roob of unity. and i� based on the

(5.12) Proposition. *ff* K = *Q(μm) is the held* ofm-t/1 roofs of *unity, then*

(K (,) � G(.,) $\bigcap$ *L(X,.,),*
X

where x varie.� *over all Dirichlet* diarnc1cr1, mod *m.* and

G(,,)� n(l-'.l'l(p)-'J-'.
Pim

Proof: The proof hinge1, on the law of decomposition of prime numbers *p* in the field *K.* Let p = (p1 .. , p,f be the decomposition of the prime number pin *K,* and let *f* be the degree of the p;, i.e., \Jt(p1) =*pI.* Then (K(s) contaim the factor

n(l-'.l'l(p) ')_, �(1-p ,,>-'.
Pl/!

On the other hand, the L-series give the factor *nX*< I - x(p)p_'•)-1. For *plm* thi5 is I. So let *pf m.* By chap. **I,** (10.3). *f'* i5 the order of *p* mod *m* in and *c* = I. Since *efr* = tp(m), the quotient *r* = is the of the subgroup *Gr>* generated by *p* in *G* = A1,1,ociating *X* 1--'1' *X (p)* defines an i:-.omorphism *G* fl � *11f,* and gives the exacl 1,cquence

1-----+G/Gp-----+G-----+ /JJ-----+ I.

where� indicate1, character group.s,. We therefore find r = #(G/G1,) = *(G* : Gp) clement1, in the preimage of *x(p).* It follow� that

n(l - x(p)p-l)-I = n (I - (p-') I = (I - /J {.,)-/
X (E/11

�no-'.l'l(p) •1-'.
Pl/!

Finally. taking the product over all *p,* we get (K(s) = G(s) TTX *L(x.s).* □

For the trivial character x^0 mod m. we have $L(x^0,s) = $ **n,,** nr(l - p ') $((s)$. sothat

$$\backslash K(,) \text{?} G(.,) \text{ ITO } - p\text{-'}m,) \quad \underset{xcf'Y^{11}}{\text{TT}} \; L(x,.,).$$

plm

Since ((s) and $(K$ (s) both have a simple pole at $s = \text{I}$, we obtain the

(5.13) Proposition. *For every non-trivial Dirichlet ch:.1racler x,* one *ha?*

This innocuous looking result is in fact rather profound. and yield? as a concrete con?equencc

(5.14) Dirichlet's Prime Number Theorem. *Every* **arithmetic progression**

$$a, \; a\pm m, \; a\pm 2m. \; a\pm 3m, \; \ldots, \; with(a.m) = \text{I}.$$

i.e., eve1y class a mod *m. conwim infinitely* many *prime number.?.*

Proof: Let X he a Dirichlet character mod m. Then one has, for Re(s) > I,

$$logL(x.s) = - \underset{p}{L} \log(1\text{-}x(p)p\text{-}\cdot') = \underset{p \; m\text{?}I}{LI:} \frac{x(p''')}{mp'''^{1}} = \underset{p}{L} \frac{x(p)}{P\text{-}'} + gy(.1),$$

where $gx(s)$ is holomorphic for Re(s) > ½ - this follows from a trivial estimate. Multiplying by x(a-^{1}) and summing over all character? mod m. yields

$$\underset{X}{L} \; x(a^{-1}) \, logL(x._1) = \underset{X \; I'}{LL} \frac{x(a\text{-}.j\,p)}{p} + g(s)$$

$$\text{?} \underset{h=I \;\; X}{\overset{II}{I}}{:}I{:}x(u\text{-'}h) \quad \underset{p=/,(111)}{I:} \; \overset{I}{-}{+}s{<}{<}I \; p\text{-}'$$

$$\text{?} \quad \underset{f!='C1("1)}{I:} \quad \frac{\text{?}^1\text{?'J+x(.s)}}{/J}.$$

Nole here that

$$\underset{\cdot.,}{I{:}x(u\text{-'}h)} \text{?}\Big|0. \qquad \text{if } a\#\text{-} \; h,$$
$$ip(m) \; = \; \#(Z/mZ)\text{?}. \qquad \text{if } a = \; h.$$

When we pas? to the limit s -----+ I (.1 real > I). logL(x,.1) ?lays bounded for $x \neq x^0$ because $L(x, 1) \neq 0$, whereas $\log L(x^0, 1) =$

$\lim \log(1-p^{-1}) + \log\zeta(s)$ tends to ∞ because $\zeta(s)$ has a pole. The left-hand side of the above equation therefore tends to ∞, and since $\mathfrak{G}(s)$ is holomorphic at $s = 1$, we find

$$\lim_{s\to 1} \varphi(m) \sum_{p \equiv a (m)} \frac{1}{p^s} = \infty .$$

Thus the sum cannot consist of only finitely many terms, and the theorem is proved. □

For $a = 1$, Dirichlet's prime number theorem may be proved by pure algebra (see chap. I, § 10, exercise 1). Searching for a proof in the general case Dirichlet was led to the study of the L-series $L(\chi, s)$. This analytic method gives sharper results on the distribution of prime numbers among the classes a mod m. We will come back to this in a more general context in § 13.

§ 6. Hecke Characters

Let $\mathfrak{m}$ be an integral ideal of the number field K, and let $J^{\mathfrak{m}}$ be the group of all ideals of K which are relatively prime to $\mathfrak{m}$. Given any character

$$\chi : J^{\mathfrak{m}} \to S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \},$$

we may associate to it, as a common generalization of the Dirichlet L-series as well as the Dedekind zeta function, the L-series

$$L(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}.$$

Here $\mathfrak{a}$ varies over all integral ideals of K, and one defines $\chi(\mathfrak{a}) = 0$ whenever $(\mathfrak{a}, \mathfrak{m}) \neq 1$. Searching for the most comprehensive class of characters χ for which the corresponding L-series could be shown to have a functional equation, HECKE was led to the notion of *Größencharaktere*, which we define as follows.

(6.1) Definition. *A* **Größencharakter** *mod* $\mathfrak{m}$ *is a character* $\chi : J^{\mathfrak{m}} \to S^1$ *for which there exists a pair of characters*

$$\chi_f : (\mathcal{O}/\mathfrak{m})^* \to S^1, \quad \chi_\infty : \mathbf{R}^* \to S^1,$$

such that

$$\chi((a)) = \chi_f(a)\chi_\infty(a)$$

for every algebraic integer $a \in \mathcal{O}$ *relatively prime to* $\mathfrak{m}$.

A character x of *.1m* i� a *GriJjJem harakter* mod mas 5oon as there exist:;, a character *X-x.,* of **R*** :c.uch that

$$\chi\big((a)\big) = \chi_\infty(a)$$

for all a E o such that a = I mod m. For if thi� is the case. then the rule $X_1(a)$ = x((a))x-x,(a) [1] define5 a character xr of (o/mr which sati5tle&

X((al) � Xr(a)h(a)

for all algebraic integers a E n relatively prime to m. This last identity underlines the fact that the restriction of a *Gri4ienr-haraktcr* to principal ideal5 breaks up into a finite and an infinite part. From

o(ml = { *a* E *o* | *(a,* m) =I).

it extend& uniquely to the group

K(m) � {a EK' | (a,m) � I}

of all fractions relatively prime to m, hecau<se every a E K{ml determines a well-defined class in (o/m)*. The character and thus also the character Xi, are determined uniquely by the *G,·i!Ber1ch,,ml,ta x,* since the group

Km=/ aE K(m) | a= 1 mod m)

is dense in **R�,** hy the approximation theorem, and one has Xc-x,(a) = x((a)) for a E *Km.* Let us recall that the congruence a =I mod m signilie� that a = *h/(,* for two integers *h, c* relatively prime tom, such that h = c mod m or, equivalently, a E utf'1 t;; *Kp* for Pim, if m = TIP p"P.

The character *x'">,)* factors automatically through **R***/*o'",* where

om=/£ E IF= I mod m)

In fact, for *F* E *o'''* we have xde) = 1, and thus x((F)) = I. The two character� Xt and *Xoo* (o/m)*, as�ociated with a *GriHJencharakter X* &atisfy the relation

Xr(f)xcx,(£) = I for all *E* E

and it can he shown that every "uch pair of characters (xr- X~) comes from a *Grfdlenchara/..ter x* (exercise 5).

The attempt to understand l,n>/in1< hrrmA/m in a conceptual way leads one to introduce **ideles.** In fact, *Griif.iencharaktere* arise as characters of the **idele** class **group** of the number field *K.* We will not use this more abstract interpretation in what follows, but it will be explained at the end of this section.

(6.2) **Proposition.** Let *x* be a *Gr6Jiencharokter* mod m, *and let* m' be a divisor ofrn. Then *the* following conditions are equivalent.

(i) *x* i.� *the restriction* of a *Griij3cncharoktcr x* :.Im'----+ S^I mod m'.

(ii) Xt factors *through* (o/m'r.

Proof: (i) => (ii). Let be the restriction of the *x'* : *.1m'* ----+ and let *x*� be the pair of character� wilh X'. Let *Xt,* rc�p. be the compo�ite of

(o/m)•------+ (o/m')*� S^1. re�p. $\mathbf{R}^*/\mathcal{O}^{\mathfrak{m}} \longrightarrow \mathbf{R}^*/\mathcal{O}^{\mathfrak{m}'} \xrightarrow{\chi'_\infty} S^1$

We then find for $a \in \mathcal{O}^{(\mathfrak{m})} \subseteq \mathcal{O}^{(\mathfrak{m}')}$:

$$\chi\big((a)\big) = \chi'\big((a)\big) = \chi'_{\mathfrak{f}}(a)\chi'_\infty(a) = \widetilde{\chi}_{\mathfrak{f}}(a)\widetilde{\chi}_\infty(a),$$

so that Xi = Xr and *X,.,_* = ;(c"' because Xt and *Xxo* are uniquely determined by *X*· Thus Xt !'actors through (o/m')� (and *x'>J* through **R+/o'"**

(ii)==} (i). Let *Xt* be the composite of (o/rn)* ....- (o/m')� __!| 5^1. In every das� *a'* mod *pm'* E *1m';pm',* there is an ideal *a* E *]"'* which j1, relatively prime tom. i.e., a'= *aa* for some (a) E pm'. We put

$$\chi'(\mathfrak{a}') = \chi(\mathfrak{a})\chi'_{\mathfrak{f}}(a)\chi_\infty(a).$$

Thi� definition doc� not depend on the choice of the ideal *a* E Jm. for if *a'=* a1a1. a1 E *J"',* (a1) E *pm',* then one has (aaJ^1) E *Jm,* and

x(a)xi(a)xo-.(a) = *x* (a)x ((aaJ^1)) *xr(a ^1adx""'(a-^1ai)x;(a)x""'(a)*
= x(adxi'(a1 *)x,-,_,(ai).*

The restriction of the character *x'* from *1m'* to 1m **i�** the *Gr6Jk11charakter* of J^111 and if *(a')* is a principal ideal prime tom' and *a'=* *ah, (a)* E (h) E *pm',* then we have

x'((a'J) � *X* ((aJ) x'((h)) � x((a)) x,'(hJh(hJ
= xr(a)xc,.,(a)x;(h)x,.,_,(h) = *xi'(ah)X--x.,(ah)* = *x;(a'Jxc,.,(a').*

Thus *x'* is a *Grij.fienc lwraktcr* mod m' with corre�ponding pair of characters �h LJ

The *Größencharakter* *X* mod m is called **pl'imitive** if it is not lhc a *Grfdiencharaktcr* x' mod m' for any proper divisor m'lm.

According to (fi.2). thb b the case if and only if the character *Xt* of (o/m)* is primitive in the 1,ern,e that it does not factoriLe through for any proper divisor m'lm. The **conductor** of is the smallest f of m �uch that *x* b the restriction of a *ChiWo,clu,m/.te,-* mod f. By (6.2), f i5 the conductor of Xi. i.e.. the 5mallest divisor of m such that X_1 factors through (o/f)*.

Let us now have a closer look at the character X_1, and then at the character Xrx,-

(6.3) Definition. Let x_1 *be a character* of (o/m)* *and y* E $m^{-1}D^{-1}$, *where()* i1, */he* different of *K* IQ. *111cn we define the* **Gauss sum** of x_1 fo *be*

$$\chi_f(x)\, e^{2\pi i\, Tr(xy)},$$

where x varies over a system of *rcprcsenlalives* of (o/m)*.

The Gau�s sum doe1, not depend on the choice of representatives r, for if *x' =x* mod m, then - *,y* E $mm^{-1}D^{-1} = D^{-1}$ = {a EK | *Tr(a)* E Z), so that

$$Tr(x'y) = Tr(ty) \bmod Z$$

and therefore $c^2rr1_{r,(i'yJ} = c^2rr$, i,(,Jl. The same argument shows that rm(x_1,y) depends only on the cosct $y +$ ll-^{1}, i.e.. it defines a function on the CJ/m-module m $^1D^1/D^{-1}$. **In** the case K = Q, m = (m). 'we get back the Gaus1, sum introduced in (2.5) by r($x_{1.11}$) = define theta series and L-serie'> attached to Hecke·� *Gn',Pe,,ch,mnltm* with a view to proving functional equations. For this, the propertie-" of Gau1,1, sums will play a crucial rOle.

(6.4) Theorem. *Let* x_1 *be* a *primitive* character of (o/m)*, *Jc1 y* E $m^{-1}z$, ^{1} *and a* E *o. Then* one *ha,,*

$$\tau_m(\chi_f, ay) = \begin{cases} \overline{\chi}_f(a)\tau_m(\chi_f, y), & i((a.m) = 1, \\ 0, & \text{if}(a.m) \neq 1. \end{cases}$$

and *furthermore*

$$|\tau_m(\chi_f, y)| = \sqrt{\mathfrak{N}(m)}, \quad if\ (y m\mathfrak{d}, m) = 1$$

The most difficult part of the theorem is the last claim. To prove it, we make the following preparations. For integral ideals $\mathfrak a = \mathfrak p_1^{\nu_1}\cdots\mathfrak p_r^{\nu_r}$, $\nu_i \geq 1$, consider the **Möbius function**

$$\mu(\mathfrak a) = \begin{cases} 1, & \text{if } r = 0, \text{ i.e., } \mathfrak a = (1), \\ (-1)^r, & \text{if } \nu_1 = \cdots = \nu_r = 1, \\ 0, & \text{otherwise.} \end{cases}$$

For this function we have the

(6.5) Proposition. *If* $\mathfrak a \neq 1$, *then* $\sum_{\mathfrak b \mid \mathfrak a} \mu(\mathfrak b) = 0$.

Proof: If $\mathfrak a = \mathfrak p_1^{\nu_1}\cdots\mathfrak p_r^{\nu_r}$, $\nu_i \geq 1$, then

$$\begin{aligned}\sum_{\mathfrak b \mid \mathfrak a} \mu(\mathfrak b) &= \mu(1) + \sum_i \mu(\mathfrak p_i) + \sum_{i_1 < i_2} \mu(\mathfrak p_{i_1}\mathfrak p_{i_2}) + \cdots + \mu(\mathfrak p_1 \cdots \mathfrak p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ &= (1 + (-1))^r = 0. \qquad \square\end{aligned}$$

Now, for $y \in \mathfrak m^{-1}\mathfrak d^{-1}$ and for every integral divisor $\mathfrak a$ of $\mathfrak m$, we look at the sums

$$T_{\mathfrak m}(y) = \sum_{\substack{x \bmod \mathfrak m \\ x \in (\mathcal O/\mathfrak m)^*}} e^{2\pi i\, Tr(xy)} \quad \text{and} \quad S_{\mathfrak a}(y) = \sum_{\substack{x \bmod \mathfrak m \\ x \in \mathfrak a}} e^{2\pi i\, Tr(xy)}.$$

These sums do not depend on the choice of representatives x, for if $x' \equiv x \bmod \mathfrak m$, then $(x'-x)y \in \mathfrak d^{-1}$, hence $Tr(x'y) \equiv Tr(xy) \bmod \mathbb Z$. We find the

(6.6) Lemma. *One has*

$$T_{\mathfrak m}(y) = \sum_{\mathfrak a \mid \mathfrak m} \mu(\mathfrak a) S_{\mathfrak a}(y),$$

and for every divisor $\mathfrak a \mid \mathfrak m$,

$$S_{\mathfrak a}(y) = \begin{cases} \mathfrak N(\frac{\mathfrak m}{\mathfrak a}), & \text{if } y \in \mathfrak a^{-1}\mathfrak d^{-1}, \\ 0, & \text{if } y \notin \mathfrak a^{-1}\mathfrak d^{-1}. \end{cases}$$

Proof: In view of (6.5), we have

$$\sum_{\mathfrak a|\mathfrak m}\mu(\mathfrak a)S_{\mathfrak a}(y) = \sum_{\mathfrak a|\mathfrak m}\mu(\mathfrak a)\sum_{\mathfrak a|\mathfrak b|\mathfrak m}T_{\mathfrak b}(y) = \sum_{\mathfrak b|\mathfrak m}T_{\mathfrak b}(y)\sum_{\mathfrak a|\mathfrak b}\mu(\mathfrak a) = T_{\mathfrak m}(y),$$

If $y \in \mathfrak a^{-1}\mathfrak d^{-1}$ and $x \in \mathfrak o$, then $xy \in \mathfrak d^{-1}$, so that $Tr(xy) \in \mathbb Z$, i.e., all summands of $S_{\mathfrak a}$ are 1 and there are $\#(\mathfrak o/\mathfrak a) = \mathfrak N(\mathfrak a)$ of them. If on the other hand $y \notin \mathfrak a^{-1}\mathfrak d^{-1}$, then we can find in $\mathfrak o/\mathfrak a$ a class z mod $\mathfrak a$ such that $zy \notin \mathfrak d^{-1}$, i.e., $Tr(zy) \notin \mathbb Z$, so that $e^{2\pi i Tr(zy)} \neq 1$, and we obtain

$$e^{2\pi i Tr(zy)}S_{\mathfrak a}(y) = \sum_{x \bmod \mathfrak a} e^{2\pi i Tr((x+z)y)} = S_{\mathfrak a}(y),$$

since $x+z$ varies over all the classes of $\mathfrak o/\mathfrak a$ as x does, so that we do find $S_{\mathfrak a}(y) = 0$. □

Proof of Theorem (6.4): Let $a \in \mathfrak o$, $(a, \mathfrak m) = 1$. As x runs through a system of representatives of $(\mathfrak o/\mathfrak m)^*$, so does xa. We get

$$\tau_{\mathfrak m}(\chi_{\mathfrak f}, ay) = \sum \chi_{\mathfrak f}(x)e^{2\pi i Tr(xay)}$$

$$= \overline{\chi}_{\mathfrak f}(a)\sum \chi_{\mathfrak f}(xa)e^{2\pi i Tr(xay)}$$

$$= \overline{\chi}_{\mathfrak f}(a)\tau_{\mathfrak m}(\chi_{\mathfrak f}, y).$$

Let $(a, \mathfrak m) = \mathfrak m_1 \neq 1$. Since $\chi_{\mathfrak f}$ is primitive, we can find a class b mod $\mathfrak m \in (\mathfrak o/\mathfrak m)^*$ such that

$$\chi_{\mathfrak f}(b) \neq 1 \quad\text{and}\quad b \equiv 1 \bmod \frac{\mathfrak m}{\mathfrak m_1}.$$

As a consequence, $ab \equiv a \bmod \mathfrak m$, so that $aby - ay \in \mathfrak d^{-1}$, and by what we have just shown,

$$\overline{\chi}_{\mathfrak f}(b)\tau_{\mathfrak m}(\chi_{\mathfrak f}, ay) = \tau_{\mathfrak m}(\chi_{\mathfrak f}, bay) = \tau_{\mathfrak m}(\chi_{\mathfrak f}, ay).$$

Finally, in view of $\chi_{\mathfrak f}(b) \neq 1$, we find $\tau_{\mathfrak m}(\chi_{\mathfrak f}, ay) = 0$.

As for the absolute value of the Gauss sum, we '>CC from (6.6) that

$$|\tau_m(\chi_f, y)|^2 = \tau_m(\chi_f, y)\overline{\tau_m(\chi_1, y)}$$

$$= \sum_{\substack{\mathrm{mod}\ m\\ (x,m)=1}} \tau_m(x_1, y)\chi_1(t)e^{-2\pi i Tr(t y)}$$

$$= \sum_{\substack{\mathrm{mod}\ m\\ (x,m)=1}} \tau_m(\chi_f, xy)\, e^{-2\pi i Tr(xy)}$$

$$= \sum_{\substack{\mathrm{mod}\ m\\ (z,m)=1}} \sum_{\substack{x\ \mathrm{mod}\ m\\ (x,m)=1}} \chi_f(z)\, e^{2\pi i Tr(xy(z-1))}$$

$$= \sum_{\substack{\mathrm{mod}\ m\\ (z,m)=1}} \chi_f(z) T_1\big(y(z-1)\big)$$

$$= \sum_{\substack{\mathrm{mod}\ m\\ (z,m)=1}} \chi_f(z) \sum_{a|m} \mu(a) S_a(y(z-1))$$

We now make me of the condition $(ymi'l, m) = I$. It implies that

$$y(z-1) \in a^{-1}\mathfrak{D}^{-1} \iff z \equiv 1 \bmod \mathfrak{f}.$$

Indeed, if $z - 1 \in \mathfrak{f}$, then $y(z-1) \in m^{-1}\mathfrak{D}^{-1}a^{-1}m = a^{-1}\mathfrak{D}^{-1}$. If on the other hand $z \not\equiv 1 \bmod \mathfrak{f}$, i.e., $1 (z-1)$. then $v_\mathfrak{p}(z-1) <$ for a prime divisor p of $\mathfrak{f}$. Since $= 1$, we have $v_\mathfrak{p}(.rrnV) =$ so that $v_\mathfrak{p}(y) = -v_\mathfrak{p}(m) - v_\mathfrak{p}(\mathfrak{D})$ and

$$v_\mathfrak{p}(y(z-1)) < v_\mathfrak{p}(m) - v_\mathfrak{p}(a) + v_\mathfrak{p}(y) = -v_\mathfrak{p}(a) - v_\mathfrak{p}(\mathfrak{D}) = v_\mathfrak{p}(a^{-1}\mathfrak{D}^{-1}),$$

and thu� $y(z-1) \notin a^{-1}\mathfrak{D}^{-1}$. Thit-., together with (6.6). gives

$$|\tau_m(\chi_1, y)|^2 = \sum_{a|m} \mu(a) \, \mathfrak{N}(a) \sum_{z \equiv 1} \ldots$$

For $a \neq 1$ the last character sum vanishes since is primitive. and therefore nonzero on the subgroup of z mod m $\in$ such that $z \equiv 1 \bmod m/a$: the sum reproduces itself under mulltiplication with a value $\chi_f(x) \neq 1$ of the character. So we finally have that $= \mathfrak{N}(m)$. This prove� all the �tatemcnts of the theorem. □

Having studied the character'> χ_1 we now tum to the character� χ_∞ of $\mathbf{R}^*$. They arc given explicitly a�

(6.7) **Proposition.** *The* characters A of **R*,** i.e., *the* continuou� homomor-*phisms*

;._: **R*-+** .51_

are *given explicitly by*

$$\lambda(x) = N\left(x^{p}|x|^{-p+iq}\right),$$

for *some admi.,sih/c* p E TTr Z (see §3, p.448) and *a* q ER±. p and q arc *uniquely detennined by* A.

Proof: For every x E **R+** we may write x = and obtain in this way a decomposition

R* = U x R�_,

where U = { r E **R*** | IxI = I). It therefore suffices to determine separately the characters of U and those of **R�.** We write p instead of r for elements of Hom(K, :C) to indicate that r = f. and we choo�e an element *u* from each pair {r, f} �uch that r *cp T.* Then we have

u�[$\prod_{T}$ s']' � TTi±l IX $\prod_{rr}$ [*s'* x *s't.*

and S^1---+ [S^1 x S^1]+, trr i--+ (r<J,.ta), i� a topological i�omorphism. The characters of{± I} corrc�pond one-to-one to exponentiating by a *Pp* E {O, I}, and the character!-. of S^I corrc<,pond one-to-one to the mappings i--+ *x*�, fork E Z. f--<"rom the correspondence *k* i--+ *(k.* 0), rc�p. (0, - k), for *I..* 2: 0, resp. *k* _s 0, we obtain the character5 of [S^1 x S^1j� in a one-to-one way from the pairs *(fh,* Pr) with *Pr, Pr* 2: 0 and *Pr Pr* = 0. The characters of LT are therefore given by

$$\lambda(x) = N(x^{p}),$$

with a uniquely detennincd admissible p E TT,

The character!-. of **R"..,** arc obtained via the topological isomorphi�m

log: **R�----+ R+.**

Writing a!-. above

$$\mathbf{R}_{+} = \prod_{\rho} \mathbb{R} \times \prod_{\sigma} \left[\, \mathbb{R} \times \mathbb{R} \,\right]^{+},$$

and observing the isomorphism *[* H x IR:.] 1 __:::_,.. R., *(X*$_O$, Irr) i--+ *2xrr,* we sec that a character of **R±** corresponds one-to-one to a system *(qp,t/o)* via the rule

.t f------:> TT *e"fi,""* TT e21q"-1"_

It is therefore given by an clement q E **R=** viu The bomorphisrn log then gives a character A of R"... via *y* i--+

with a uniquely determined q E R±. In view of the decomposition we finally obtain the characters A of R* as

$$.(x) = N\left(\left(\frac{x}{|x|}\right)^{p}|x|^{iq}\right) = N\left(x^{p}|x|^{\;\;p+iq}\right). \qquad \square$$

If the character *Xcx.* associated to the *Griljiencharakter* x : *,1m* -+ S^1 is given by

$$(_{\infty}(x) = N\left(x^{p}|x|^{-p+iq}\right),$$

then we say that X is of type *(p,* q), and we call *p - iq* the exponent of *X.* Since Xoo factor& through R�/om, not all exponents aclUally occur (<see exercise 3).

The class of all *Gri�/Jent haraktcre* subsumes in particular the generalized *Dirichlet characters* defined as follows. To the module

$$m� \prod_{Pl�} p''e.$$

we associate the ray class group ./°'/ *pm* mod m (see chap. VI, *I). Here *Jm* is the group of all ideals relatively prime to m, and *pm* is the group of fractional principal ideals *(a)* such that

$$a = I \bmod m \quad \text{and } a \text{ totally positive.}$$

Thi5 last condition means that *ra* > 0 for every real embedding *r : K* → Ill.

(6.8) Definition. *A* Dirichlet character mod mis a *charnclcr*

$$X \;:Jmjpm \to SI$$

of the ray clas� *group* mod m, *i.e.,* a *character x* : *J'''* → S^I such *thar* $x(P''') = I$.

The conductor of a Dirichlet character X mod m is defined to be the smalle�t module f dividing m such that X factor� through Jf/pf_

(6.9) Proposition. *The Dirichlet characten; X* mod m *are preci�cly* the *Gri;j,emharaktere* mod m *of type* (p.O), p = (pr), *such* tliat *Pr=* 0 for *all complex r. In other* words, *one has*

$$x((a)) = X1(a)N((\,T,;"j)'\}$$

for some *charnctcr* xi of (o/mt. *The conductor* oft/Je *Dirichlet character* is *,it* the *same time* aho *the* conductor of tile *corresponding GriHiencharakter.*

Proof: Let χ be a *Größencharakter* mod $\mathfrak{m}$ with corresponding characters $\chi_{\mathfrak{f}}$, χ_∞ of $(\mathcal{O}/\mathfrak{m})^*$, $\mathbf{R}^*$, such that χ_∞ is of type $(p, 0)$ with $p_\tau = 0$ for τ complex. For totally positive $a \in \mathcal{O}$ such that $a \equiv 1 \bmod \mathfrak{m}$, we then obviously have $\chi_{\mathfrak{f}}(a) = 1$, and $\chi_\infty(a) = 1$, and then $\chi((a)) = \chi_{\mathfrak{f}}(a)\chi_\infty(a) = 1$. Therefore χ factorizes through $J^{\mathfrak{m}}/P^{\mathfrak{m}}_+$, and is thus a Dirichlet character mod $\mathfrak{m}$.

Conversely, let χ be a Dirichlet character mod $\mathfrak{m}$, i.e., a character of $J^{\mathfrak{m}}$ such that $\chi(P^{\mathfrak{m}}_+) = 1$. Let $K^{\mathfrak{m}} = \{a \in K^* \mid a \equiv 1 \bmod \mathfrak{m}\}$, $K^{\mathfrak{m}}_+ = \{a \in K^{\mathfrak{m}} \mid a$ totally positive$\}$ and $\mathbf{R}^*_+ = \{(x_\tau) \in \mathbf{R}^* \mid x_\tau > 0$ for τ real$\}$. Then we have an isomorphism

$$K^{\mathfrak{m}}/K^{\mathfrak{m}}_+ \longrightarrow \mathbf{R}^*/\mathbf{R}^*_+ \cong \prod_{\tau \text{ real}} \{\pm 1\}.$$

Then the composite

$$K^{\mathfrak{m}}/K^{\mathfrak{m}}_+ \xrightarrow{(\;)} J^{\mathfrak{m}}/P^{\mathfrak{m}} \xrightarrow{\chi} S^1$$

defines a character of $\mathbf{R}^*/\mathbf{R}^*_+$. It is induced by a character χ_∞ of $\mathbf{R}^*$ which – because $\chi_\infty(\mathbf{R}^*_+) = 1$ – is of the form $\chi_\infty(x) = N(x^p|x|^{-p})$ with $p = (p_\tau)$, $p_\tau \in \{0, 1\}$ for τ real, and $p_\tau = 0$ for τ complex. We have $\chi((a)) = \chi_\infty(a)$ for $a \in K^{\mathfrak{m}}$, and

$$\chi_{\mathfrak{f}}(a) = \chi\big((a)\big)\,\chi_\infty(a)^{-1}$$

gives us a character of $(\mathcal{O}/\mathfrak{m})^*$. Therefore χ is indeed a *Größencharakter* of the type claimed.

Let $\mathfrak{f}$ be the conductor of the Dirichlet character χ mod $\mathfrak{m}$, and let $\mathfrak{f}'$ be the conductor of the corresponding *Größencharakter* mod $\mathfrak{m}$. $\chi: J^{\mathfrak{m}}/P^{\mathfrak{m}} \to S^1$ is then induced by a character $\chi': J^{\mathfrak{f}}/P^{\mathfrak{f}} \to S^1$, so the *Größencharakter* $\chi: J^{\mathfrak{m}} \to S^1$ mod $\mathfrak{m}$ is the restriction of the *Größencharakter* $\chi': J^{\mathfrak{f}} \to S^1$. This implies that $\mathfrak{f}' \mid \mathfrak{f}$. On the other hand, the *Größencharakter* $\chi: J^{\mathfrak{m}} \to S^1$ is the restriction of a *Größencharakter* $\chi'': J^{\mathfrak{f}'} \to S^1$, so $\chi_{\mathfrak{f}}$ is the composite of $(\mathcal{O}/\mathfrak{m})^* \to (\mathcal{O}/\mathfrak{f}')^* \xrightarrow{\chi''_{\mathfrak{f}}} S^1$ (see (6.2)). By the above, χ'' gives a character $J^{\mathfrak{f}'}/P^{\mathfrak{f}'} \to S^1$ such that the Dirichlet character $\chi: J^{\mathfrak{m}}/P^{\mathfrak{m}} \to S^1$ factors through $J^{\mathfrak{f}'}/P^{\mathfrak{f}'}$. Hence $\mathfrak{f} \mid \mathfrak{f}'$, so that $\mathfrak{f} = \mathfrak{f}'$. □

(6.10) Corollary. *The characters of the ideal class group $Cl_K = J/P$, i.e., the characters $\chi: J \to S^1$ such that $\chi(P) = 1$, are precisely the Größencharaktere χ mod 1 satisfying $\chi_\infty = 1$.*

Proof: Form= I we have (o/mr = {I}. A character X of *J/P* is mod I. The a-;sociated character *Xt* i� trivial, so $= x_1(ar^1x((a)) =$ I, and thus *Xe,.,*= I, hecausc K^* is dense If conversely *x* is a *Gn?[:encharakter* mod I satisfying *Xoc.* = I, lhcn

$$\chi\big((a)\big) = \chi_f(a)\chi_\infty(a) = \chi_f(a) = 1,$$

for *a EK�*. Therefore *x(P)* = I, and xis a character of the ideal da�� group. □

To conclude this section, let us study the relation of *Gn!fiencharaAterc* to characters of lhc idele clai,i, group.

(6.11) Definition. *A* **Hecke character** is .1 *ch::irac/cr* of *the idclc ci.'1s.� group* $C = I/K$� of *the number field K,* i.e.. a *contimwu,; homomorphism*

$$X: I \longrightarrow S^1$$

of *the ideJe* group *I*= []PK; such *that x(K�)* = I.

In order to deal with Hecke characteri, concretely. consider an integral ideal m = np pllp of *K,* i.e., *!lp* :::_ 0 and *np* = 0 for p IX. We ai,i,ociate to this ideal the *s11hf{mup Jm* of *I.*

$$Jm = Ii'' \times L,\_, \quad \text{where} \quad lt'' = \prod_{\text{pt-x.}} U\text{�}nf'\backslash, \quad I\text{-...,} = \prod_{\text{Pl-...,}} K\text{�}.$$

If p f *x,,* then $U_{;}^{111}$ is the group of units *Up* if $n = 0$, and the n-th group of higher units for *n* :::_ I. We interpret /"" as the multiplicative group **R*** of the R-algebra **R** = *K* R = TTpl-x. *Kp*. Observe that *Jm* differs i,\ightly from the congruence suhgroup *I"'* = TIP u?pl introduced in chap. VI,* I, in that, for real p, we have the factor U�^{01} = R:, imtead of the component *K;*. The effect is that/ *;JmK** is not the ray class group *r'/Pm* mod m, but i<;ornorphic to the quotienl *J* "'/ *pm* by the group *pm* of all principal ideab *(a)* such that *a==* I mod m - this is seen as in chap. VI. (1.9). We will refer to *J* "'/ *pm* as the *smalt ray class f.iroup.*

We call ma **module of definition** for the Hecke character X if

Every Hecke character admits a module of definition, i,ince the image of X : nrtcx. *Up* .... .5¹ is a compact and totally disconnected subgroup of

S^1, hence finite, and so the kernel has to contain a subgroup of the form $\prod_{\mathfrak p\nmid\infty} U_{\mathfrak p}^{(n_{\mathfrak p})}$, where $n_{\mathfrak p} = 0$ for almost all $\mathfrak p$. For it we can take the ideal $\mathfrak m = \prod_{\mathfrak p\nmid\infty}\mathfrak p^{n_{\mathfrak p}}$ as a module of definition.

Since $\chi(I_f^{\mathfrak m}) = 1$, the character $\chi : C = I/K^* \to S^1$ induces a character

$$\chi : C(\mathfrak m) \longrightarrow S^1$$

of the group

$$C(\mathfrak m) = I/I_f^{\mathfrak m}K^*.$$

But it will not in general factor through the small ray class group $I/I^{\mathfrak m}K^* \cong J^{\mathfrak m}/P^{\mathfrak m}$ (see chap. VI, (1.7), (1.9)), which bears the following relation to $C(\mathfrak m)$.

(6.12) Proposition. *There is an exact sequence*

$$1 \longrightarrow \mathbf R^*/\mathcal O^{\mathfrak m} \longrightarrow C(\mathfrak m) \longrightarrow J^{\mathfrak m}/P^{\mathfrak m} \longrightarrow 1$$

Proof: The claim follows immediately from the two exact sequences

$$1 \longrightarrow I^{\mathfrak m}K^*/I_f^{\mathfrak m}K^* \longrightarrow I/I_f^{\mathfrak m}K^* \longrightarrow I/I^{\mathfrak m}K^* \longrightarrow 1,$$

$$1 \longrightarrow I^{\mathfrak m}\cap K^*/I_f^{\mathfrak m}\cap K^* \longrightarrow I^{\mathfrak m}/I_f^{\mathfrak m} \longrightarrow I^{\mathfrak m}K^*/I_f^{\mathfrak m}K^* \longrightarrow 1.$$

In the second one has $I^{\mathfrak m}\cap K^* = \mathcal O^{\mathfrak m}$, $I_f^{\mathfrak m}\cap K^* = 1$ and $\bar I^{\mathfrak m}/I_f^{\mathfrak m} = I_\infty = \mathbf R^*$, and so $\bar I^{\mathfrak m}K^*/I_f^{\mathfrak m}K^* = \mathbf R^*/\mathcal O^{\mathfrak m}$. □

Given a Hecke character χ with module of definition $\mathfrak m$, we may now construct a *Größencharakter* mod $\mathfrak m$ as follows. *For* every $\mathfrak p \nmid \infty$, we choose a fixed prime element $\pi_{\mathfrak p}$ of $K_{\mathfrak p}$ and obtain a homomorphism

$$c : J^{\mathfrak m} \longrightarrow C(\mathfrak m)$$

which maps a prime ideal $\mathfrak p \nmid \mathfrak m$ to the class of the idele $(\pi_{\mathfrak p}) = (\dots, 1, 1, \pi_{\mathfrak p}, 1, 1, \dots)$. This mapping does not depend on the choice of the prime elements, since the ideles $(u_{\mathfrak p})$, $u_{\mathfrak p} \in U_{\mathfrak p}$, for $\mathfrak p \nmid \mathfrak m$, lie in $I_f^{\mathfrak m}$. Taking the composite map

$$J^{\mathfrak m} \xrightarrow{c} C(\mathfrak m) \xrightarrow{\chi} S^1$$

yields a 1-1 correspondence between Hecke characters with module of definition $\mathfrak m$ and *Größencharaktere* mod $\mathfrak m$. The reason for this is the following

(6.13) Proposition. *There* i.<; a *canonic,il exact sequence*

I ---+ K(ml/*d''* � *Jm* x (o/m)* x **R***/om --*1*..+ C(m)---+ I,

where O is given by

O(a) = ((a)-^{1}, *a* modm, *a* modom).

Proof: For every *a* E *K* \ml, let *a* E / be the idele with components Gp = *a* for p f moo and *(IP* = I for p I moo. Il is then obviou<; that

(((a)) =Zimodli'''K.*

Let us decompose the principal idCle *a* according to its components in *I* = *1*$_{1}$ x $_{r\times,}$ asaproduct *a*= *a*$_{1}$*acx.*, and define the homomorphi-;ms

cp: (o/m)*---+ C(m). ifr: R*/om---+ C(m)

by

cp(a) = *Jax,* mod*I;''K*,* *ifr(h)* = h-¹ mod*Ir'K*.*

where every *h* E **R*** = *lex* i� considered a� an ide!e in /. For *a* E *o,* *a* � I mod m, we have *afG* ^{I} E *It'* <; *I,* so we get in C(m) the equation rp(a) = [{Ja''''J = *[a*$_{1}$*a-x,l* = [aj = I, where I J indicates taking classe-''. This -''hows that *cp* is well-defined. For every *E* E om, one has F1 E *tt,* :-o *[e,,J* = [E:xfr] = [sl = I in C(m). and thus 1/1(£,.,J = I. Con�equently *1/f* is well-defined. We now define the homomorphism

f'': .*Im* x (o/m)* x **R***/om------+ C(m)

by

f''((a, *a* mod m, *h* mod om)) = c(o)rp(a),fr(h),

and we :-how that the resulting sequence is exact. The homomorphism *8* i� dearly injective. For *o* E K(mJ one has

f (*8(a))* = *C(* (o))- ^{1}({'(a)i,lr(o) = *Q* ¹*Zia-x,a�.}* mod *ItK** = I,

sothat *f''* o *8* = I. Conversely, let

j ((a. *o* mod m, *h* mod o''')} = c(a)rp(a)ijr(h) = I,

and let *a*= nr-tmx):!''''. Then

c(o) = *y* mod *Ir'K**

for some idele *y* with components *Yr* = *n?* for p f moo, and *Yp* = I for p I moo. This yields an identity *ylla""h-*^{1} = *l;x* with I; EI/" and *x* EK*.

For p 1 moc one has $(ycia'''-h-^{1})_p$ = $rr?a$ = $.!;px$ in $KP\cdot$ and so $v_p = V_p(a-^1x)$. For p Im one has $(ycia,x,h-^1)_p$ = I = .!;px, 50 that x E utrl, and also O = l'p = $v.,(a-^1x)$ since a is relatively prime tom. This gives

$$a=(ax-^1).$$

As x E Ut �^{1}, one has x == I mod m, hence

$$rp(a.t-^1) = rp(a).$$

Finally, for ploo we find $(ycia''''h-^1)p$ = ahp^1 = x in Kp, so that h = $ar;cx$ -I. and thus

$$\psi(ax^{-1}) = \psi(b).$$

So we have

$$(a, a \bmod m, h \bmod CJm) = ((ax-^1), ax-^1 \bmod m, ax-^1 \bmod o''').$$

and this shows the exactness of our �equence in the middle.

The surjcctivity of/ j5 proved as follows. Let a mod ttK^* be a cla�� in C(m). By the approximation theorem. we may modify the representing ide!e a, multiplying it by a suitable x EK*, in -;uch a way that Gip E ut''J for p Im. Let a = TTptrn'''- pvp(<>pJ. Then we have

$$c(a) = y \bmod /�nK�.$$

where the idele y has components Yp = Ep E $Up.$ for p f moo. and Yp = I for p Imoo. This gives E and if we define $h = a$�^{1}• then f((n. l mod m,h mod vm)) = $yh-^1$ = $ya-x,$ = a mod $lt'''K^*$.

□

By the preceding propo�ition, the characters of C (m) corre�pond I - I to the characters of 1m x (o/m)� x R*/o'n that vanish on O(K(rn) /om). i.e., to the triple� X, $xr.$ x,...., of characters of ,/^{111}, rc�p. (o/m)*. resp. R*/0^{11}, such that

$$x((a))-^1xr(a \bmod m)x''''(a \bmod om)= I$$

for a E K(m). This makes X a *Griif]cntharakter* mod rn, and �ince X_1 and x,...., are uniquely determined by X, we obtain the

(6.14) Corollary. *The correspondence x r+ x :ic is* 1-1 *between characters* of C(m), *i.e..* Hecke *character.� with module* of *detini1i011* m, *and Gri!ao,ch,rmi,tere* mod m.

Exercise 1. Let $\mathfrak{m} = \prod_{i=1}^r \mathfrak{m}_i$ be a decomposition of $\mathfrak{m}$ into integral ideals which are pairwise relatively prime. Then one has the decompositions

$$(\mathcal{O}/\mathfrak{m})^* \cong \prod_{i=1}^r (\mathcal{O}/\mathfrak{m}_i)^*$$

and

$$\mathfrak{m}^{-1}\mathfrak{d}^{-1}/\mathfrak{d}^{-1} \cong \bigoplus_{i=1}^r \mathfrak{m}_i^{-1}\mathfrak{d}^{-1}/\mathfrak{d}^{-1}.$$

Let χ_f be a character of $(\mathcal{O}/\mathfrak{m})^*$, and let χ_{fi} be the characters of $(\mathcal{O}/\mathfrak{m}_i)^*$ defined by χ_f. If $y \in \mathfrak{m}^{-1}\mathfrak{d}^{-1}/\mathfrak{d}^{-1}$, and if $y_i \in \mathfrak{m}_i^{-1}\mathfrak{d}^{-1}/\mathfrak{d}^{-1}$ are the components of y with respect to the above decomposition, then

$$\tau_{\mathfrak{m}}(\chi_f, y) = \prod_{i=1}^r \tau_{\mathfrak{m}_i}(\chi_{fi}, y_i).$$

Exercise 2. Prove the **Möbius inversion formula:** let $f(\mathfrak{a})$ be any function of integral ideals $\mathfrak{a}$ with values in an additive abelian group, and let

$$g(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} f(\mathfrak{b}).$$

Then one has

$$f(\mathfrak{a}) = \sum_{\mathfrak{b} \mid \mathfrak{a}} \mu\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right) g(\mathfrak{b}).$$

Exercise 3. Which of the characters $\chi(x) = N(x^p|x|^{-p+iq})$ of $\mathbf{R}^*$ are characters of $\mathbf{R}^*/\mathcal{O}^*$?

Exercise 4. The characters of the "small ray class group" $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ mod $\mathfrak{m}$ are the *Größencharaktere* mod $\mathfrak{m}$ such that $\chi_\infty = 1$.

Exercise 5. Show that every pair of characters $\chi_f: (\mathcal{O}/\mathfrak{m})^* \to S^1$ and $\chi_\infty: \mathbf{R}^*/\mathbf{R}^*_+ \to S^1$ such that

$$\chi_f(\varepsilon)\chi_\infty(\varepsilon) = 1 \quad \text{for all } \varepsilon \in \mathcal{O}^*$$

comes from a *Größencharakter* mod $\mathfrak{m}$.

Exercise 6. Show that the homomorphism $c: J^{\mathfrak{m}} \to C(\mathfrak{m})$ is injective.

§ 7. Theta Series of Algebraic Number Fields

The group P of fractional principal ideals (a) is constituted from the elements $a \in K^*$, and it sits in the exact sequence

$$1 \to \mathcal{O}^* \to K^* \to P \to 1.$$

In order to form the theta series we will need, let us now extend K^* to a group $\mathcal{K}^*$ whose elements represent *all* fractional ideals $\mathfrak{a} \in J$.

(7.1) Proposition. *There is a commutative exact diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathfrak{o}^* & \longrightarrow & K^* & \longrightarrow & P & \longrightarrow & 1 \\ & & \| & & \cap & & \cap & & \\ 1 & \longrightarrow & \mathfrak{o}^* & \longrightarrow & \widehat{K}^* & \longrightarrow & J & \longrightarrow & 1 \end{array}$$

with a subgroup $\widehat{K}^* \subseteq \mathbb{C}^*$ *containing* K^*, *such that* $(a) \in J$, and

$$\mathfrak{N}\big((a)\big) = |N(a)|$$

for all $a \in \widehat{K}^*$.

Proof: Let the ideal class group J/P be given by a basis $[\mathfrak{b}_1], \dots, [\mathfrak{b}_r]$, and choose, for every one of these basic classes, an ideal $\mathfrak{b}_1, \dots, \mathfrak{b}_r$. Then every fractional ideal $\mathfrak{a} \in J$ can be written in the form

$$\mathfrak{a} = a\mathfrak{b}_1^{\nu_1} \cdots \mathfrak{b}_r^{\nu_r}$$

where $a \in K^*$ is well-determined up to a unit $\varepsilon \in \mathfrak{o}^*$, and the exponents $\nu_i \bmod h_i$ are uniquely determined, h_i being the order of $[\mathfrak{b}_i]$ in J/P. Let $\mathfrak{b}_i^{h_i} = (b_i)$. For every $\tau \in \operatorname{Hom}(K, \mathbb{C})$, we choose a fixed root

$$\widehat{b}_{i\tau} = \sqrt[h_i]{\tau b_i}$$

in $\mathbb{C}$ in such a way that $\widehat{b}_{i\bar\tau} = \overline{\widehat{b}}_{i\tau}$ whenever τ is complex. We define $\widehat{K}^*$ to be the subgroup of $\mathbb{C}^*$ generated by K^* and by the elements $\widehat{b}_i = (\widehat{b}_{i\tau}) \in \mathbb{C}^*$. Each class $[\mathfrak{b}] \in J/P$ contains a uniquely determined ideal of the form

$$\mathfrak{b} = \mathfrak{b}_1^{\nu_1} \cdots \mathfrak{b}_r^{\nu_r} \quad \text{with} \quad 0 \le \nu_i < h_i\,,$$

and we consider the mapping

$$f : J/P \longrightarrow \widehat{K}^*/K^*, \quad f([\mathfrak{b}]) = \widehat{b}_1^{\nu_1} \cdots \widehat{b}_r^{\nu_r} \bmod K^*.$$

It is a homomorphism. For if $\mathfrak{b} = \mathfrak{b}_1^{\nu_1} \cdots \mathfrak{b}_r^{\nu_r}$ and $\mathfrak{b}' = \mathfrak{b}_1^{\nu_1'} \cdots \mathfrak{b}_r^{\nu_r'}$, and if $\nu_i + \nu_i' = \mu_i + \lambda_i h_i$, $0 \le \mu_i < h_i$, then $\mathfrak{b}_1^{\mu_1} \cdots \mathfrak{b}_r^{\mu_r}$ is the ideal belonging to the class $[\mathfrak{b}][\mathfrak{b}']$, and

$$\begin{aligned} f([\mathfrak{b}][\mathfrak{b}']) &= \widehat{b}_1^{\mu_1} \cdots \widehat{b}_r^{\mu_r} = \widehat{b}_1^{\nu_1+\nu_1'} \cdots \widehat{b}_r^{\nu_r+\nu_r'}\, b_1^{-\lambda_1} \cdots b_r^{-\lambda_r} \\ &\equiv (\widehat{b}_1^{\nu_1} \cdots \widehat{b}_r^{\nu_r})(\widehat{b}_1^{\nu_1'} \cdots \widehat{b}_r^{\nu_r'}) \bmod K^* = f([\mathfrak{b}])f([\mathfrak{b}']). \end{aligned}$$

f is clearly surjective. To show the injectivity, let $\widehat{b}_1^{\nu_1} \cdots \widehat{b}_r^{\nu_r} = a \in K^*$, and let $h = h_1 \cdots h_r$ be the class number of K. Then we have for the ideal 1bt'1 b;·, E J that ah = a-$h(h$�^{1h}/hi ···h,'',h/lr,) = a-$hcht'^{1}$ = (1). Since .I is torsion-free, it follow:,, thal a= (I). and so bt^{1} ··· b,^{1}" = (a) E P. From thif> we deduce that every element Q E i'' admit. a unique representation

$$Zi = aht^{1} \cdot h,1'^{1}. \quad 0 :'.:: JJ, < \quad a \text{ EK*}$$

We define a map

c):R*--------+.,

by

$$ll=aht'^{1}\text{-h,}^{1}\text{''}\text{�(G)=ab�}^{\cdot 1} \quad \text{b,''}$$

Arguing as above, we <;Ce that this i:,, a homomorphism. It j:,, surjcctive and obviously ha:,, kernel Finally we have that lhi I= (lhnl) ER� and

<n((b,))''· � 'Tl(b:·1� IN(h,)I � 11) Th, I � I!)�';I �IN(b,ll'''.

so that '.}I((h$_1$)) = IN(h,)I, and thus lal E R'.;_, 91((a)) = IN(a)I for all a E f*. □

The clements a of i'' w,cd to be called **ideal numbers** - a name which i:-. somewhat forgollcn but will be u:,,cd in what follows. The diagram (7.1) implies an i,;omorphism

$$K'/K' \text{'''} J/P.$$

For EK* we write if and lie in the same class, i.e., if ah ^{1} E K^*. We call a an **ideal integer,** or an integral ideal number, an integral ideal. The semigroup of all ideal integer5 will he denoted by Furthermore we write I. i! � E 3. and for every pair E f*, we have the notion of gcd(a.h) E K^* (which is lacking inside K^*). The greatest common divisor i:;. the ideal number d (which is unique up to a unit) such that the ideal (d) is the gcd of the ideals (a).(h). Observe that the ideal numbers are not defined in a canonical way. This is the reason why they have not been able to hold their own in the development of number theory. (They are treated in l46], [651.)

We now form an analogous exten:;.ion of the prime residue groups (Z/ mZ)� For three ideal number� o, h. m, the congruence

signifies that $o \sim h$ and Y, E & U /0). If m = (m), we also write thi� relation as a = h mod rn. Let m be an integral ideal. The semigroup 3(mJ of all integral ideal number5 relatively prime to m i� partitioned by the etjuivalence relation = into classes. which we will write as a mod m. They are given explicitly as follow�.

(7.2) Lemma. *For every* $a \in \widehat{\mathcal O}^{(\mathfrak m)}$ *one has*

$$a \bmod \mathfrak m = a + a(a^{-1})\mathfrak m.$$

Proof: Let $b \in a \bmod \mathfrak m$, $b \neq a$, i.e., $b = a\alpha$ for some $\alpha \in K^*$, $\alpha \neq 1$, and $b - a = \mathfrak c\mathfrak m$, $\mathfrak c \in \mathfrak J$. Then

$$a^{-1}(b-a) = a^{-1}a(\alpha - 1) = (a^{-1})(\mathfrak c)(\mathfrak m) \subseteq (a^{-1})\mathfrak m,$$

so that $b \in a + a(a^{-1})\mathfrak m$. Let conversely $b \in a + a(a^{-1})\mathfrak m, b \neq a$, and thus $b/a = \alpha \in 1 + (a^{-1})\mathfrak m$. Then one has $b \sim a$ and $(b-a) = (a)(\alpha - 1) \subseteq (a)(a^{-1})\mathfrak m = (\mathfrak m)$, i.e., $\mathfrak m \mid b - a$ and therefore $b \equiv a \bmod \mathfrak m$. $\square$

We now consider the set

$$(\widehat{\mathcal O}/\mathfrak m)^* := \{a \bmod \mathfrak m \mid a \in \widehat{\mathcal O}^{(\mathfrak m)}\}$$

of all equivalence classes in the semigroup $\widehat{\mathcal O}^{(\mathfrak m)}$ of ideal integers prime to $\mathfrak m$.

(7.3) Proposition. $(\widehat{\mathcal O}/\mathfrak m)^*$ *is an abelian group, and we have a canonical exact sequence*

$$1 \longrightarrow (\mathcal O/\mathfrak m)^* \longrightarrow (\widehat{\mathcal O}/\mathfrak m)^* \longrightarrow J/P \longrightarrow 1.$$

Proof: For $a, b \in \widehat{\mathcal O}^{(\mathfrak m)}$, the class $ab \bmod \mathfrak m$ only depends on the classes $a \bmod \mathfrak m$, $b \bmod \mathfrak m$, so we get a well-defined product in $(\widehat{\mathcal O}/\mathfrak m)^*$. Every class $a \bmod \mathfrak m$ has an inverse. Indeed, since $(a) + \mathfrak m = \mathcal O$, we may write $1 = \alpha + \mu$, $\alpha \in (a), \mu \in \mathfrak m$. Consequently $a \mid \alpha$, so that $\alpha = ax$, $x \in \widehat{\mathcal O}$, and since $1 \in \alpha(1 + \alpha^{-1}\mathfrak m) = \alpha \bmod \mathfrak m$, we see that $ax \bmod \mathfrak m$ is the unit class, i.e., $x \bmod \mathfrak m$ is inverse to $a \bmod \mathfrak m$.

The right-hand arrow in the sequence is induced by $a \mapsto (a)$. It is surjective since every class of J/P contains an integral ideal relatively prime to $\mathfrak m$. If the class $a \bmod \mathfrak m = a(1 + (a)^{-1}\mathfrak m)$ is mapped to 1, then one has $(a) \in P$, and so $a \in \mathcal O$, $(a, \mathfrak m) = 1$. Hence $a \bmod \mathfrak m = a + \mathfrak m$ is a unit in $\mathcal O/\mathfrak m$. The injectivity of the arrow on the left is completely trivial, i.e., we have shown the exactness. $\square$

For an ideal class $\mathfrak K \in J/P$, we will denote by $\mathfrak K^f \in J/P$ in what follows the class defined by where Di� lhe different of K I:QI. Let m = *(m)* and *D* = (d), wilh some fixed ideal numbers *m, d.* Form = *o* let *m* = I. We now study charactcr1>

X: (3/m)*-------+

and put *x(a)* = 0 for *a* E *o* such that (a, m) #- I. In the applicatiom, *x* will come from a *G,·iifle,nh,,rn!cta* mod m, but the treatment of the theta series is independent an origin of *X·*

(7.4) Definition. *Let a* E 3 *be an ideal* integer, *and let fi. be the cla�s* of(a). *Then* we define *the* Gauss sum

r(x.a)= *L* x(i)e21r1T1(fa/111d),

; mod m

where X mod m *runs through the* cfa.�ses of (3/m)* *which arc mapped lO the* class ff. *In particular, we put T(x)* = r(x. l).

The Gauss sum r(x. a) reduces immediately to the one considered in *6,

*x(.,)c2,.11i\1yJ_*

In fact. on the one hand we have

y = *Xa/md* E m-[1]iJ-[1].

since the class of the ideal (v) = (a)(?)(m)-[1](d) [1] i� the principal class .R.R'm [1]i) [1], soy EK*, and ;ne finds

y E *(y)* = (aX)m-li)-1 S; m-1i)-1,

because *a* and *X* are integral. On the other hand, if *X* mod m is a fixed class of (0/mr which maps to .R.', then, in view of (7.3), we the others by *Xx* mod m, with *A* mod m varying over the clas5c5 of Therefore

r(x,a) = x(X)rn,(x,y),

and in particular

$$\tau(\chi) = \chi(\widehat{x})\tau_{\mathfrak{m}}(\chi, y)$$

with *y* = which sati5fies (ymtl. m) = I since *ymi.'l* = (*X)* and ((?),m) = Consequently, r(x,a) doc<, not depend on the choice of rcprc5cl1lative� ?, and theorem (6.4) yields at once the

(7.5) **Proposition.** *For a primitive character x* of (0/mf, *one has*

r(x,a) = Y(a)r(x)

and Ir(x)I =�-

The thela series $H(x, z)$ used in §2 in the treatment of Dirichlet L-1->cric;, arc attached to the field We now have to find their analogue� relative to an arbitrary number field K. Given admissible clement p E nr 2 (see §3, p.448) and a character X of we form the Hecke theta series

X (a)N (a") c::r1 la;/ ,mdl,a),

where $m.d$ are fixed ideal numbers such that (m) = m and (d) = D. We take m = I if m = I. The case m = I, $p = 0$ i� exceptional in that the constant term of the theta series j5 X(O)N(OI') = 1, whereas it is O in all other casc1>.

Let us decompose the theta series according to the ideal classe!-. .R E J/P into partial Hecke theta series

$$\theta^{p}(\mathfrak{K},\chi,z) = \quad x(a)N(a'')cJT1(a�/lrmll,al,$$

where a varies over all ideal integer1> in the class rt E R^*/K^* which corresponds to the ideal cla1->s Jt under the i'iomorphism R^*/K^* � J/P. For these partial theta 1->cric'>, we want to deduce a transformation formula. and to thi� end we decompo�e them further into theta 1->erie1> for which we have the general transformation formula (3.6) al our di�posal.

Let a be an ideal relatively prime to m ½hich belong;, to the clas1> Jt and let a E be an ideal number such that (a) = a.

(7.6) Lemma. A.�sume !hat m i- I *or* p i- 0. *If* X mod m varies over *the* c/1,1.�ses of (o/m)*, *lhen* one has

$$\theta^{p}(\mathfrak{K},\chi,z) = \chi(a)N(a^{p}) \sum_{x \bmod m} \chi(x)\theta_{\Gamma}^{p}\left(x,0,z|a^2/md|\right),$$

where r *is the lattice* m/a S; Rand

Hj-(r.O, :)= L N((,· + -1;)1'} e::ri((,+gl� ,+,:,
�E/'

Proof: In the theta �eries ()l'(Jt X.:). it suffices to �um over the elements of fl n d'''1 because X i!-. zero on the others. Every X mod m E (?i/m)* i� either disjoint from Ji. or else it b contained in In view of the exact �equence (7.3)

I------+ (o/mr------+ (3/m)*------+ .!JP------+ 1,

the clas1->e1>

$$ax \bmod \mathfrak{m} = a(x + \mathfrak{a}^{-1}\mathfrak{m})$$

arc the different residue classes of (3/m)* contained in�- Thi:-. givc5

f)f!(Jtx,7)= L L x(ax)N((at+t(!;)l')c;r1la(1+�)�/1r11d,a(<+i:J\
-1 m"<lm g<cr

$$= \chi(a)N(a^p) \sum_{x \bmod m} \chi(x)\theta_I^p\big(x,0,z|a^2/md|\big).$$ []

For any admissible element $p = (p_\tau)$, we will write $\overline{p}$ for the admis�ible clement with componcnb $\overline{p}_\tau = p_{\overline{\tau}}$. From the transformation formula (3.6) for the series θ_I^p and propo,;ition (7.5) on Gauss sums. we now obtain the

(7.7) **Theorem.** For a *primitive* character χ of (3/m)*. *one has the transformation formula*

$$\theta^p(\mathfrak{K}, \chi, -1/z) = W(\chi, \overline{p})N\big((z/i)^{p+\frac{1}{2}}\big)\theta^{\overline{p}}(\mathfrak{K}', \overline{\chi}, z)$$

wilh the const;mt factor

W(x.fi) = [ir,(fi1N((.!!!!!)")]-1 lmdl J<Tilm)

This factor ha.� absolute value $|W(\chi, p)| = 1$.

Proof: The lattice Γ dual to the lattice $\Gamma = $ m/a S; **R** is given. according to (5.7), by *r' = a/mD. (Here as in §4, the asterisk �ignilies adjunction with rc:-.pcct to { .). i.e.. = (*ax.y).) The volume of the fundamental mesh of Γ is by chap. I.

,ul(r) �<Jl(m/a)/id;l � N(lm/al)N(ldl)'1,

From (3.6) we now get

(I) 0/'.(cO, - l/lmd/a²1,) � A(cJH;,(o,x.,lmdja"l).

with the factor

A(,)� [l'""'N(lm/al)N(ldll"'] _, N((lmd/a'l,j!)"+l)

�[,""'�] _,N(lmdja'l") N((c/l)l'+l)

and the ,;cric�

(2) ot,(n,x. -1md/ti21) = L N(g'1')c2,,,,,,,, g') ,,πi(g'z md/a²), g'cl

Writing $g' =$ the rules c.;tated in § 3 give

$$\backslash t,g') = Tr(a,\cdot g/md),$$

$$1/\mathrm{lmd}/a'\mathrm{lc},,') \text{ � } \mathrm{l'g},\mathrm{lmd}/a^2 1/\mathrm{lmd}/a\mathrm{l}','g) \text{ � } \{g,\mathrm{flmdl}\ \ g)$$

and $N((*g)P) = N(gl')$. If g' varies over the lattice I'', then g varies over the set

$$(md/a)T' = (md/a)a(mD)^{-1} = (j' \ \mathrm{n}\, 0) \ \mathrm{U}\ \{O\}.$$

Suhstituting all this into (2) yields

(3) $0J'.,(O,x,,\mathrm{lmd}/a^2 1)$

$$\text{�}\ N((\_!!\ )'^{1}) \ L \qquad N(i./')e2''''1t\ !1(axg/md)en11\_g:/,mdl.;:).$$
$$nz\overline{d} \qquad ;:E(.\text{�}'nc;Ju[OI$$

Let us now consider fir�t the special case m = I, $p = 0$ (which was essentially treated already in §5). In thi� case, we have (An 6) U {O} = $\backslash ag \mid g$ EK. (ag) S; $o) = aa^{-1} = aI'$. Consequently

$$0''(.R,x,z) = \sum_{g'\in T'} erriiag:/ldl,a;: = \backslash \sum_{\text{�}Er} en1(\text{�}:1a''/d1.g1 = 0r(zla2/dl),$$

$$\vartheta^{p}(\mathfrak{K}', \overline{\chi}, z) = \sum_{g\in(\hat{\mathfrak{K}}'\cap\hat{\mathfrak{O}})\cup\{0\}} e^{\pi i\langle gz/|d|, g\rangle} = \theta_{I'}\left(z|d/a^2|\right)$$

Equation (I) thus becomes

$$\vartheta^{p}(\mathfrak{K}, \chi, -1/z) = N(z/i)^{\frac{1}{2}}\theta^{\overline{p}}(\mathfrak{K}', \overline{\chi}, z).$$

Now assume m -/- I or p # 0. Then we have x(O)N(OI') = 0. Substituting (3) into (I) and (I) into formula (7.6), with - I/Z instead of:, we obtain

$$f;IP(Ji.x, - \mathrm{l}/:) = N(a^1) \sum_{\backslash\ m()J\ m} x(ax)Oj(.1.O. - l/zlmd/a^2 1)$$

$$= B(z) \sum_{g\in\hat{\mathfrak{K}}'\cap\hat{\mathfrak{O}}} N(g^{\overline{p}})\Big(\sum_{x \bmod \mathfrak{m}} \chi(ax)\, e^{2\pi i\, Tr(axg/md)}\Big) e^{\pi i\langle gz/|md|,}$$

with the factor

$$B(z) = A(z)\frac{N(a^p)}{N((md/a)^{\overline{p}})}.$$

No½ consider the sum in parentheses. If x varies over a 1,ystcm of representative<;; of then aA varies over a "Y�lcm of representative!. of those classes of which arc mapped under -----?- J/P to the cla1,s .it Furthermore. i� an integral ideal in the Jf. and since Jt' bear:- the �ame relation Jf.R = fmi)] to Jt as Jt doc5 to J.t'. we recognize the sum in qucqion as the *Gauss sum*

r(x,.iz) = *L* x(a.,)e2Jrl r,(a\�/nrdl.
\ mod m

Suhstituting: in now the rc�ult (7.5),

$$\tau(\chi, g) = \overline{\chi}(g)\tau(\chi),$$

we finally arrive at the identity

(4) *01'(.fl,x,* -1/c)� *W(x,p)N((c/;J"+l)e"(.* �*,X,C)*

with the factor

W(x,P)= [ildp)�rlN(lmd/a21p) *N(afi)r(x)*
N((md/u)l')

= r(xJ
iTi(pl�N ((lmdl)") � *N* ("""""") �

= �*[il,(jj)N((_!!!!!_)I')]* ',
v"TTimJ lmdl

where one has to observe that *Tr(p)* = 'fr([]). *al'*= **al'*, *a*a* = lal[2], and lmdl[1'] = (�lmdl)[1'] = lmdll' because lmdl ER�. Since lr(x)l = �- we have lW(x,l')l = l. n

If m -=l=- I or *p -1-* 0, we find for the special thelil :,,eries:

(;)l'(X,Z) = $\sum$ $\chi(a) N(a^p) e^{\pi i (az/|md|, a)}$ $\sum \theta^p(\mathfrak{K}, \chi, z)$

and (7.7) yields the

(7.8) Corollary. $\theta^p(\chi, -1/z) = W(\chi, \overline{p}) N((z/i)^{p+\frac{1}{2}}) \theta^{\overline{p}}(\overline{\chi}, z)$.

We recommend lhill the reader who has studied the above proof allow himself a moment of contemplation. Looking hack, he will reali/.e !he peculiar ½ay in which almm,t all fundamental arithmetic propertie� of the numher field *K* have been u�ed. Fir�t they served to hreak up the theta serie�, then these con�tituents were re�huflled by the analytic transfonnation law, hut in the end they are reassembled lO form a new theta �eries. Having contemplated this. the reader should reflect upon the admirable �implicity of the theta formula which encapsulates all these a�pect� of the arithme!JC o! the number field.

There is however one important fundamental law of number lheory which does not enter into this fonnula, that is, **Dirichlet's unit theorem.** This will play an e�sential r61e when we now pa<,s from theta �eries to L-serie� in the next section.

Exercise J. Deline ideal prnne numbeVi and '>how that unique prime factorirntion hold, in K^*

Exercise 2. Lct (1 be the scmigroup ideal rnteger,. If $d = (a.h)$ is the gcd of $a.h$, then there cxi�t clements E (0! ,uch th.it

$$d=.w+yh.$$

Furthermore, we have x rc�p. r · � il/h, unle,\ ,1 = 0, re�p. $y = 0$. Here the notation $\alpha \sim \beta$ means c

Exercil'>e 3. The congruence 11,1 = h mod m ha'> a �olulion m 3 with integral ,1 1f and only 1t $(a,m)/h$. Thi'> �olu1iun i'> unique mod m, provided (a,m) = 1.

Exercise **4.** A system of finitcly man) congruence\ with pairwi'>e rel,nivcly prnnc moduli i'> simultaneously solvabl if every congruence i� �olvablc individually m such a way that the individual �olution� arc equivalent (with re�pect to~).

Exercise 5. If a. m E 3. then there cxi�b m every re�idue cla\\ mo<l III prime *tum*, an ideal integer prime to a.

Exercise 6. For the factor group $.I'''/ f'''$ the group pm of all pnnc1pal ideal, (a) such that $a \equiv 1$ mod m, one ha the �cquencc

$$1 \to o'/LJ''' \to (0/ml'----.. .1n\bullet;pm \to 1.$$

where $o''' = \{1,$- E If = I mod m).

Exercil'>e 7. Let $R^\bullet$mi he the preimage of J^m under $\widehat{K}^*$, .I, and let $Km= (a$ E $K' \mid as=$ 1 mod m). Then one ha� $(\widehat{\mathcal{O}}/\mathfrak{m})^* = \widehat{K}^{(\mathfrak{m})}/K^{\mathfrak{m}}$

§ 8. Hecke L-series

Let m be again an integral ideal of the number field K and let

$$X : l'''\text{------}+ S^1$$

be a character of the group of ideals relatively prime to m. With re.,pect to this character. we fom1 fhe L-'>eries

$$\text{Lix.n�I: } \frac{x(a)}{91(0)'}$$

where a varies over the integral ideab of Kand we put $x(a) = 0$ whenever $(a.. \text{m}) -I-$ I. Then the following propo:c,ition holds in complete generality.

(8.1) Proposition. *The L-series $L(\chi, s)$ converges absolutely and uniformly in the domain $\mathrm{Re}(s) \geq 1+\delta$, for all $\delta > 0$, and one has*

$$L(\chi, s) = \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}},$$

where $\mathfrak{p}$ varies over the prime ideals of K.

Proof: Taking formally the logarithm of the product

$$\mathcal{L}(s) = \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}$$

gives the series

$$\log \mathcal{L}(s) = \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{\chi(\mathfrak{p})^n}{n\mathfrak{N}(\mathfrak{p})^{ns}}.$$

It converges absolutely and uniformly for $\mathrm{Re}(s) = \sigma \geq 1+\delta$. In fact, since $|\chi(\mathfrak{p})| \leq 1$, and $|\mathfrak{N}(\mathfrak{p})^s| = \mathfrak{N}(\mathfrak{p})^{\sigma} \geq p^{f_{\mathfrak{p}}(1+\delta)} \geq p^{1+\delta}$ and since $\#\{\mathfrak{p} \mid p\} \leq d = [K:\mathbb{Q}]$, it admits the following convergent upper bound which is independent of σ:

$$\sum_{p,n} \frac{d}{np^{n(1+\delta)}} = d \log \zeta(1+\delta).$$

This shows that the product

$$\mathcal{L}(s) = \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}} = \exp\Big(\sum_{\mathfrak{p},n} \frac{\chi(\mathfrak{p})^n}{n\mathfrak{N}(\mathfrak{p})^{ns}}\Big)$$

is absolutely and uniformly convergent for $\mathrm{Re}(s) \geq 1+\delta$. Now develop in this product the factors

$$\frac{1}{1-\chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}} = 1 + \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^{s}} + \frac{\chi(\mathfrak{p})^2}{\mathfrak{N}(\mathfrak{p})^{2s}} + \cdots$$

for the finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{N}(\mathfrak{p}_i) \leq N$, and multiply them. This yields the equation

$$(*) \qquad \prod_{i=1}^{r} \frac{1}{1-\chi(\mathfrak{p}_i)\mathfrak{N}(\mathfrak{p}_i)^{-s}} = \sum_{\nu_1,\ldots,\nu_r=0}^{\infty} \frac{\chi(\mathfrak{p}_1)^{\nu_1}\cdots\chi(\mathfrak{p}_r)^{\nu_r}}{(\mathfrak{N}(\mathfrak{p}_1)^{\nu_1}\cdots\mathfrak{N}(\mathfrak{p}_r)^{\nu_r})^s} = \sum{}' \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s},$$

where $\sum'$ denotes the sum over all integral ideals $\mathfrak{a}$ which are divisible at most by the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Since the sum $\sum'$ contains in particular the Lenn� such that *91(a) 2 N,* we may also write

$$\prod_{i=1}^{r} \frac{1}{1 - \chi(\mathfrak{p}_i)\mathfrak{N}(\mathfrak{p}_i)^{-s}} = \sum_{\mathfrak{N}(\mathfrak{a})<N} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} +$$

Comparing now in (*) the sum L' with the series $L(\chi,s)$, we get

$$\Big|\prod_{\mathfrak N(\mathfrak p)\le N}\frac{1}{1-\chi(\mathfrak p)\mathfrak N(\mathfrak p)^{-s}} - L(\chi,s)\Big| \le \sum_{\mathfrak N(\mathfrak a)>N}\frac{1}{|\mathfrak N(\mathfrak a)^{s}|}$$

$$\le \sum_{\mathfrak N(\mathfrak a)>N}\frac{1}{\mathfrak N(\mathfrak a)^{1+\delta}}.$$

For $N\to\infty$ the right-hand side tends to zero, as it is the remainder term of a convergent series, since the sequence $\big(\sum_{\mathfrak N(\mathfrak a)\le N}\frac{1}{\mathfrak N(\mathfrak a)^{1+\delta}}\big)_{N\in\mathbb N}$ is monotone increasing and bounded from above. Indeed, with the previous notations we find

$$\sum_{\mathfrak N(\mathfrak a)\le N}\frac{1}{\mathfrak N(\mathfrak a)^{1+\delta}} \le \sum_{\mathfrak a\in J(N)}\frac{1}{\mathfrak N(\mathfrak a)^{1+\delta}}$$

$$= \prod_{i=1}^{r}\big(1-\mathfrak N(\mathfrak p_i)^{-(1+\delta)}\big)^{-1},$$

and

$$\log\Big(\prod_{i=1}^{r}\big(1-\mathfrak N(\mathfrak p_i)^{-(1+\delta)}\big)^{-1}\Big) = \sum_{i=1}^{r}\log\big((1-\mathfrak N(\mathfrak p_i)^{-(1+\delta)})^{-1}\big)$$

$$= \sum_{i=1}^{r}\sum_{n=1}^{\infty}\frac{1}{n\,\mathfrak N(\mathfrak p_i)^{(1+\delta)n}}$$

$$\le \sum_{\mathfrak p}\sum_{n=1}^{\infty}\frac{1}{n\,\mathfrak N(\mathfrak p)^{(1+\delta)n}}$$

$$\le d\sum_{p}\sum_{n=1}^{\infty}\frac{1}{n\,p^{(1+\delta)n}}$$

$$= d\log\big(\zeta(1+\delta)\big). \qquad \square$$

We now face the task of analytically continuing the L-series $L(\chi,s)$ attached to a **Größencharakter** χ mod $\mathfrak m$, and setting up a suitable functional equation for it at the same time. So we are given a character

$$\chi : J^{\mathfrak m}\to S^1,$$

such that

$$\chi((a)) = \chi_f(a)\chi_\infty(a)$$

for all integers $a\in\mathcal O$ relatively prime to $\mathfrak m$, and there are two associated characters

$$\chi_f : (\mathcal O/\mathfrak m)^*\to S^1 \quad\text{and}\quad \chi_\infty : \mathbf R^*\to S^1$$

The character Xt extends in a unique way to a character

$$Xf: (3/m)^* \longrightarrow 5'^1$$

such that the identity(*) holds for all integral ideal numbers a E &(ml prime to Indeed, the restriction of the function $x_1(a)$ of 3(ml to is given by the original character Xt of$(\mathcal{O}/\mathfrak{m})^*$, so it is in particular trivial on 1 + m and thus yields a character of $(\tilde{\mathcal{O}}/\mathfrak{m})^*$.

The L-series of a *Grqj3cncharacter* of 1m is called a Hecke £-series. If X is a (generalized) Dirichlet character mod m, i.e., a character of the ray class group *.rm/ pm,* then we call it a (generalized) Dirichlet £-series. The proof of the functional equation of the Hecke L-scries proceeds in exactly the same way as for the Dedekind zeta function, except that it is based on the theta transformation formula (7.7).

We decompose the Hecke L-series according to the classes Jl of the ideal da�:;, group ./ / P as a sum

$$/,(x.,)=r, \; L(fi.x.s)$$

of the partial L-series

$$L(Rx.-<)=$$

and deduce a functional equation for those. If all one wants is the functional equation of the L-series L (X. s), this decompo�ition is unnecessary; it may also be derived directly using the transformation formula (7.8), because we know how to represent any ideal a. by an ideal number (this wa� not yet the case when we were treating the Dedekind zeta function). However, we prefer to establish the finer result for the partial L-series.

By (7.1). we have a bijective mapping

$$cRnO)/o^* \; � \; \{ \text{ll E Jtl } a \text{ integral}\}' \quad a \longmapsto (a),$$

where J1 E f^* / K^* corresponds to the class Jl E J / P with respect to the iwmorphism $K^\bullet / K^*$ � J / P. Therefore we get

$$L(Rx.s) = \sum_{ae'fl.} \frac{x((a))}{|N(a)|^1}$$

where 9'l is a sy�tem of representatives of
function as a Mellin transform. To this end, we

$$Lx(s) = N(rr-�^{12})I'x(s/2) = N(n-''^{12})$$

We want to write this from *4 the L-function

$N(e^{-y} y^{s/2}) \frac{ay}{\;}$,

which has been attached to the G(C IR)-set X = Hom(K, C). The character *X-x:* of R* corresponding to X is given by (6.7) as

xcx,(x) = N(x''lxl-p+,q),

for an admissible p E fl, Zand a q ER±- We puts= sl + p - *iq,* where s E C is a single complex variable, and

L,,J(x.s) = Lx(s) = *Lx(sl + p- iq).*

In the integral

$$\Gamma_X(\mathbf{s}/2) = \int_{\mathbf{R}_+^*} N(e^{-y}y^{s/2})\frac{dy}{y},$$

we make the subt>litution

y i-------+ nlal^{2}y/lmdl *(a* E 9l),

where *m.d* E 3 are fixed ideal numbers such lhat (m) = m and (d) = i) is the different of KIQ. We then obtain

I'x(s/2) = *N((* l;d,r/2)N(lal') e-rr(ar/lmdl,a)N(y'/2)

and, since $N(|md|^{1s/2}) = (|d_K|\mathfrak{N}(\mathfrak{m}))^{s/2}$,

$$\big(|d_K|\mathfrak{N}(\mathfrak{m})\big)^{s/2}L_\infty(\chi,s)\frac{1}{N(|a|^{\mathbf{s}})} = c(\chi)\int_{\mathbf{R}_+^*} e^{-\pi\langle ay/|md|,a\rangle}N(y^{\mathbf{s}/2})\frac{dy}{y}$$

where *c(x)* = *N(lmdl-!'+*^{1}*'1)*^{1}*1*^{2}_ Mulliplying this by *xr(a)N(aP)* and summing over a E 9l yield5, in view of

x1(a)N(aP) *Xr(a)N(aPlal-p+ul)* / N(lal') ~ *x((a))* / IN(a)l"

the equation

$$|d_K|\mathfrak{N}(\mathfrak{m}))^{s/2}L_\infty(\chi,s)L(\mathfrak{K},\chi,s) = c(\chi)\int_{\mathbf{R}_+^*} g(y)N(y^{\mathbf{s}/2})\frac{dy}{y}$$

with the series

x(y=) L *x1(a)N(af')e-rr{a)'/!mdl,a).*
a,=9'1:

We now consider the completed L-series

$$A(Jl,x,s) \sim (ldKl;Jl(m)l'^{12}Lx(x,s)L(Jl,x,sJ.$$

Then we get

A(Ji,x,,) � c(x) I g(y)N(y'i')r·

We now want to write this function as an integral over the series

$$\theta(\mathfrak{K}, \chi, z) := \theta^p(\mathfrak{K}, \chi_{\mathfrak{f}}, z) = \varepsilon(\chi) + \quad \chi_{\mathfrak{f}}(a) N(a^p) e^{\pi i \langle az/|md|, a \rangle},$$

where the summation is extended not only - as in the case of g(y) - over a system of representatives Vl of (J1 n 3)/o*, but over all *a* E Jin 3. We have *E(X)* = I ifm =land *p* = 0, and e(x) = 0 otherwise. We will proceed in the same way as with the Dedekind zeta function (see (5.5)). Just as we did there, using

y = *Xt!/n'* *x* = *N(:�l/n,* I= *N(y),*

with *n* = I*K* : Ql], we decompose

$$\mathbf{R}_+^* = \mathbf{S} \times \mathbb{R}_+^*, \quad \frac{!!!}{y} = d^*x \times \frac{!!.!}{t}$$

Then, observing that

N(y•/2=) N(xs/2)N(ts/2n)= N(x(p-14)Jl)r-½(s+Tr(p-1q)/n),

we obtain the identity

(*) A(.lt,x,s)=c(x) *JJ* *N(x\l'-"!l/2)g(xt¹1¹¹)d*xt"�*

OS

withs'= ½ *(s* + *Tr(p - iq)/n).* Thefunction under the second integral will be denoted by

$$!,'!}l(X,t) = N(;\cdot/p\text{-}tq)/^2) \sum_{a \in \mathfrak{R}} \chi_{\mathfrak{f}}(a) N(a^p) e^{-\pi \langle a x t^{1/n}/|md|, a \rangle}$$

From it, the theta series fJ(ft. *x, ixt* l/n) is constructed as follows.

(8.2) **Lemma.** $N(x(p\text{-}iql^2)(0(Jt,x,ixt^1 1^{11})\text{-}E(x)) = \sum_{\varepsilon \in \mathcal{O}^*} g_{\mathfrak{R}}(|\varepsilon|^2 x, t)$

Proof: For every unit f E *o**, one has Xcx,(f)X1(f) = *x((F))* = I, :,,o that we get

$$N\left(|\varepsilon|^{p-iq}\right) = \overline{\chi}_{\infty}(\varepsilon)N(\varepsilon^{p}) = \chi_{\mathfrak{f}}(\varepsilon)N(\varepsilon^{p}) \blacksquare$$

We put for short $\mathfrak{R} = xt^{1/n}/|\mathfrak{m}d|$ and obtain

$$R_{\mathfrak{N}}(|\varepsilon|^2x,t) = N(x^{(p-iq)/2}) \sum_{a\in\mathfrak{a}} \chi(a)N(a^p)\, e^{-\pi\langle \mathfrak{R},|a|^2\rangle} = R_{\varepsilon\mathfrak{N}}(x,t).$$

Since $\mathfrak{a} \cap S = \bigcup_{\varepsilon\in\mathcal{O}^*} \varepsilon\mathfrak{N}$, we get

$$N(x^{(p-iq)/2})\big(\theta(\mathfrak{K},\chi,ixt^{1/n}) - \varepsilon(\chi)\big) =$$

$$= \sum_{\varepsilon\in\mathcal{O}^*} \sum_{a\in\varepsilon\mathfrak{N}} N(x^{(p-iq)/2})\chi(a)N(a^p)\, e^{-\pi\langle \mathfrak{R},|a|^2\rangle}$$

$$\sum_{\varepsilon\in\mathcal{O}^*} g_{\varepsilon\mathfrak{N}}(x,t) = \sum_{\varepsilon\in\mathcal{O}^*} g_{\mathfrak{N}}\big(|\varepsilon|^2x,t\big)\,. \qquad \square$$

From this lemma we now obtain the desired integral representation of the function $\Lambda(\mathfrak{K},\chi,s)$. We choose as in § 5 a fundamental domain F of S for the action of the group F is mapped by $\log : \mathbf{R}_+^* \to \mathbf{R}_\pm$ to a fundamental mesh of the lattice This means that we have

$$S = \bigcup_{\eta\in|\mathcal{O}^*|} \eta^2 F$$

(8.3) **Proposition.** The *function*

$$\Lambda(\mathfrak{K},\chi,s) = \big(|d_K|\mathfrak{N}(\mathfrak{m})\big)^{s/2}L_\infty(\chi,s)L(\mathfrak{K},\chi,s)$$

is the Mellin transform

$$\Lambda(\mathfrak{K},\chi,s) = L(f,s')$$

of *the function*

$$f(t) = f_F(\mathfrak{K},\chi,t) = \frac{c(\chi)}{w}\int_F N(x^{(p-iq)/2})\,\theta(\mathfrak{K},\chi,ixt^{1/n})\,d^*x$$

at $s' = \frac{1}{2}(s + Tr(p - iq)/n)$. Here we have set $n = [K : \mathbb{Q}]$, $c(\chi) = N(|\mathfrak{m}d|^{-p+iq})^{1/2}$, and w denotes the number of roots of unity in K.

Proof: One has

$$f(\infty) = \frac{c(\chi)\varepsilon(\chi)}{w}\int_F N(x^{(p-iq)/2})\,d^*x.$$

We have seen before that

$$\Lambda(\mathfrak{X},s) = \int_0^\infty f_0(t)\, t^{s}\,\frac{dt}{t} = L(f_0,s)$$

where

$$f_0(t) = c(\chi)\int_{\mathbf{S}^0} g_{\mathfrak m}(x,t)\,d^*x .$$

Since $\mathbf{S}^0 = \bigcup_{\eta\in|\mathfrak o^*|}\eta^2F$, one has

$$f_0(t) = c(\chi)\sum_{\eta\in|\mathfrak o^*|}\ \int_{\eta^2F} g_{\mathfrak m}(x,t)\,d^*x .$$

In each one of the integrals on the right, we make the transformation $F\to\eta^2F$, $x\mapsto\eta^2x$, and obtain

$$f_0(t) = c(\chi)\int_F \sum_{\eta\in|\mathfrak o^*|} g_{\mathfrak m}(\eta^2x,t)\,d^*x .$$

The fact that we may swap summation and integration is justified in exactly the same way as for the case of Dirichlet L-series in §2, p.436. In view of the exact sequence

$$1\longrightarrow \mu(K)\longrightarrow \mathfrak o^*\longrightarrow |\mathfrak o^*|\longrightarrow 1,$$

where $\mu(K)$ denotes the group of roots of unity in K, one has $\#\{\varepsilon\in\mathfrak o^*\mid |\varepsilon|=1\} = w$, so that we get

$$\sum_{\varepsilon\in\mathfrak o^*} g_{\mathfrak m}(|\varepsilon|^2x,t) = w\sum_{\eta\in|\mathfrak o^*|} g_{\mathfrak m}(\eta^2x,t).$$

Using (8.2), this gives

$$\begin{aligned} f_0(t) &= \frac{c(\chi)}{w}\int_F \sum_{\varepsilon\in\mathfrak o^*} g_{\mathfrak m}(|\varepsilon|^2x,t)\,d^*x \\ &= \frac{c(\chi)}{w}\int_F [\text{illegible}]\,\big(\theta(\mathfrak a,\chi,ixt^{1/n}) - c(\chi)\big)\,d^*x \\ &= f(t) - f(\infty). \end{aligned}$$

This, together with (*) yields the claim of the proposition. □

It is now the transformation formula (7.7) for the theta series $\theta(\mathfrak a,\chi,z) = \theta_\Gamma(\mathfrak a,\chi,z)$ which guarantees that the functions $f(t) = f_F(\mathfrak a,\chi,t)$ satisfy the hypotheses of the Mellin principle.

(8.4) **Proposition.** We *have* fi(Jt X, !) = a0 + O(e-"11/") for some $c > 0$, *and*

ao = N(idl'01 J w--) N(x-,qf'-)d*x

F

if m = 1 *and* p = 0, *and* $a_0 = 0$ *otherwise. Furthennore* we *have*

J,. (..R, *X,* I) = W(x)d+Ti(p)/n *j*F-1(..R', *X.t)*

where ..R..R' = [mi:!]. *and the constant factor* is *given by*

W(x) = [it,(flN((_"'! lmdl)l')]-l �. �

Proof: The first statemenl follows exactly as in the proof of (5.8). For the second, we make use of formula (7.7). It gives us

0(Sl, *X,* - 1/c) = &P(Jl, *X1,* - 1/,) = *W(x)N(* (,j;JP+l)&"(Jl', xr,,)

= ***W(x)N(* c,;;iP+l)e(Jl',** ,,,),

because X'.'X.,(t) = *N(xl'lxl-P+1'!) = N((*x)fllxl-p-,q) = N(xf'lxl-f'-rq).* Observing the fact that the transformation x 1---+ x 1 leaves the Haar measure d^*x invariant and takes the fundamental domain F to the fundamental domain p-l, (7.7) yields for z = *ixt* l/n:

.f''F(Jtx, t�) = w ("(X) *JN(x(p-u;)/2)0(..R,x,ix/tlfn)d*x*

I

= c�) I ,, , *N(x-(p-iqJ/2)0(..R,x, -1/ixt1f'')d*>..*

= *c(x):(x) N(x-9-+r+!)N(t(p+j:)Jn)t)(..R', X, ixt1111)d*x*

p-,

= *c(x) W (x) J* N(x(f+1q\/2)11;2+T,(p)/11a(..R' *y.ixr1fn)d*x*

, , ,

p-,

= W(x)d �l,(p)/nf,.-1(..R',y,!).

We have used in this calculation that $N(x^{1}l^{2})$ = N(t)11² = I and *N(x'') = N((*x)P) = N(xP),* and that the character Xoc, the complex conjugate of *Xx;,* is given by

$$\overline{\chi}_\infty(x) = N\left(x^{\overline{p}}|x|^{-\overline{p}-iq}\right).$$ □

From this proposition and (1.4), we now finally get our main result. We may assume that χ is a primitive *Größencharacter* mod $\mathfrak m$, i.e., that the corresponding character χ_f of $(\mathcal O/\mathfrak m)^*$ is primitive (see §6, p.472). The L-series of an arbitrary character differs from the L-series of the corresponding primitive character only by finitely many Euler factors. So analytic continuation and functional equation of one follow from those of the other.

(8.5) Theorem. *Let χ be a primitive Größencharacter* mod $\mathfrak m$. *Then the* function

$$\Lambda(\mathfrak X,s) = (|d_K|\mathfrak N(\mathfrak m))^{s/2} L_\infty(\chi,s)L(\mathfrak X,s), \quad \mathrm{Re}(s) > 1,$$

has a meromorphic continuation to the complex plane $\mathbb C$ *and satisfies the functional equation*

$$\Lambda(\mathfrak X, s) = W(\chi)\Lambda(\mathfrak X', 1-s)$$

where $\mathfrak X' = \mathfrak X_{\bar\chi}$, *and the constant* factor *is given by*

$$W(\chi) = [i^{\mathrm{Tr}(p)}N(\tfrac{\chi_\infty}{|\chi_\infty|})]^{-1}\frac{\tau(\chi_f)}{\sqrt{\mathfrak N(\mathfrak m)}}.$$

It has absolute value $|W(\chi)| = 1$.

$\Lambda(\mathfrak X,s)$ *is holomorphic* except for *poles of* order *at most* one *at* $s = \mathrm{Tr}(-p+iq)/n$ *and* $s = 1 + \mathrm{Tr}(p+iq)/n$. *In the case* $\mathfrak m \neq 1$ or $p \neq 0$, $\Lambda(\mathfrak X,s)$ *is holomorphic on all of* $\mathbb C$.

Proof: Let $f(t) = \theta(\mathfrak X,t)$ and $g(t) = \theta(\mathfrak X',t)$. From $f(t) = a_0 + O(e^{-ct^{1/n}})$, $g(t) = b_0 + O(e^{-ct^{1/n}})$ and

$$f(\tfrac{1}{t}) = W(\chi)t^{d+\mathrm{Tr}(p)/n}g(t),$$

it follows by (1.4) that the Mellin transforms $L(f,s)$ and $L(g,s)$ can be meromorphically continued, and from (8.3) we get

$$\begin{aligned}
\Lambda(\mathfrak X,s) &= L(f, \tfrac{n}{2}(s+\mathrm{Tr}(p-iq)/n))\\
&= W(\chi)L(g, \tfrac{n}{2}+\mathrm{Tr}(p)/n - \tfrac{n}{2}(s+\mathrm{Tr}(p-iq)/n))\\
&= W(\chi)L(g, \tfrac{n}{2}(1-s+\mathrm{Tr}(p+iq)/n))\\
&= W(\chi)\Lambda(\mathfrak X', 1-s),
\end{aligned}$$

where we have to take into account again that $\bar\chi_\infty(x) = N(x^{-p}|x|^{-p-iq})$.

According to (1.4), in the case $a_0 \neq 0$, $L(f,s)$ has a simple pole at $s = 0$ and $s = \frac{1}{2} + Tr(p)/n$, i.e., $\Lambda(\mathfrak{K}, \chi, s) = L(f, \frac{1}{2}(s + Tr(p - iq)/n))$ has a simple pole at $s = Tr(-p + iq)/n$ and $s = 1 + Tr(p + iq)/n$. If $\mathfrak{m} \neq 1$ or $p \neq 0$, then $a_0 = 0$, i.e., $\Lambda(\mathfrak{K}, \chi, s)$ is holomorphic on all of $\mathbb{C}$. □

For the completed Hecke L-series

$$\Lambda(\chi, s) = (|d_K|\,\mathfrak{N}(\mathfrak{m}))^{s/2} L_\infty(\chi, s) L(\chi, s) = \sum_{\mathfrak{K}} \Lambda(\mathfrak{K}, \chi, s)$$

we derive immediately from the theorem the

(8.6) Corollary. *The L-series $\Lambda(\chi,s)$ admits a holomorphic continuation to*

$$\mathbb{C} \setminus \{Tr(-p+iq)/n,\ 1 + Tr(p+iq)/n\}$$

and satisfies the functional equation

$$\Lambda(\chi, s) = W(\chi)\Lambda(\bar{\chi}, 1-s).$$

It is holomorphic on all of $\mathbb{C}$, if $\mathfrak{m} \neq 1$ or $p \neq 0$.

Remark 1: For a *Dirichlet character* χ mod $\mathfrak{m}$, the functional equation can be proved without using ideal numbers, by splitting the ray class group $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ into its classes $\mathfrak{K}$, and then proceeding exactly as for the Dedekind zeta function. The Gauss sums to be used then are those treated by HASSE in [52]. On the other hand, one may prove the functional equation for the Dedekind zeta function by using ideal numbers, imitating the above proof, without decomposing the ideal group at all.

Remark 2: There is an important alternative approach to the results of this section. It starts from a character of the idele class group and from the representation (8.1) of the corresponding L-series as an Euler product. The proof of the functional equation is then based on the local-to-global principle of algebraic number theory and on the Fourier analysis of p-adic number fields and their idele class group. This theory was developed by the American mathematician JOHN TATE, and is commonly known for short as Tate's thesis. Even though it does meet the goal of this book of presenting modern conceptual approaches, we still decided not to include it here. The reason for this is the clarity and conciseness of Tate's original paper [241], which cannot be improved upon. In addition SERGE LANG's account of the theory [94] provides an illustrative complement.

Thu:;. instead of idly copying thi:;. theory, we have chosen to provide a conceptual framework and a modem treatmenl of Hecke's original proof which is somewhat difficult to fathom. It tum� out that Hecke's approach continues to have a relevance of its own, and can even claim a number of advantages over Tate's theory. For the functional equation of the Riemann zeta function and the Dirichlet L-scries, for example, it would be out of proportion to develop Tate's fonna!ism with all its p-adic expense, since they can be settled at a beginner's level with the method u:;.cd here. Also, L-series, and the very theory of theta series has to be seen as an important arithmetic accomplishment in its own right.

It wa� for pedagogical rear,ons that we have proved the analytic continuation and functional equation of L-series four times over: for the Riemann zeta function, for the Dirichlet L-scries, for the Dedekind zeta function, and finally for general Hecke L-series. This explains the number of pages needed. Attacking the general case directly would shrink the expose to little more than the size of Tate's thesis. Still, it has to be said that Tate's theory ha1- acquired fundamental importance for number theory at large through it1- far reaching generalization1-.

§ 9. Values of Dirichlet L-series at Integer Points

The results of§ I and 92 on the values ((I - k) and *L(X,* I - k) of the Riemann zeta function and the Dirichlet L-scries will now be extended to generalized Dirichlet L-series over a totally real number field. We do this using a method devised by the Japanese mathematician *TAKURO SH1N1At,'l* (who died an early and tragic death) (see [127], [128]).

We first prove a new kind of unit theorem for which we need the following notions from linear algebra. Let V he an n-dimensional JR-vector space, k a subfield of JR, and *Vk* a llxed k-structure of *V,* i.e., a k-subspace such that $V = Vi$ ®*k* !R. By definition, an (open) k-rational simplicial cone of dimension d ir, a 'iubset of the fom1

$$C(v_1, \ldots, v_d) = \left\{ t_1 v_1 + \cdots + t_d v_d \mid t_i \in \mathbb{R}^*_+ \right\}$$

where $v_1, \ldots, v_J$ are linearly independent vectors in *Vk.* A finite disjoint union of k-rational simplicial cones is called a k-rational polyhedric cone. We call a linear fonn L on V *k-rationaf* if its coefficients with re1-pect to a k-basis of Vi, lie ink.

(9.1) Lemma. *Every nonempty subset different* from /0) *of the fonn*

$$P= \{x \in V \mid L_i(t\cdot) \geq 0,\ 0<i \leq \ell,\ M_j(x) > 0,\ 0 < j \leq m\}$$

with nonzero k-rational linear forms L_i, M_j ($\ell = 0$ *or* $m = 0$ *is allowed)* is *a di.�joint union* of *finitely many k-rational cones, and possibly the origin.*

Proof: First let $P = \{x \in V \mid L_i(x) \geq 0, i = 1, \dots ,\ell\}$, with k-rational linear fonns $L_1, \dots , L_\ell \neq 0$. For $n = 1$ and $n = 2$ the lemma is obvious. We asf.ume it is established for all R-vector spaces of dimension smaller than n. If P has no inner point, then there is a linear form L among the $L_1, \dots , L_\ell$ such that P is contained in the hyperplane $L = 0$. In this case the lemma follows from the induction hypothesis. So let $u \in P$ be an inner point, i.e., $L_1(u) > 0, \dots , L_\ell(u) > 0$. Since V_k is dense in V, we may asf.ume $u \in V_k$. For every $i = 1, \dots, \ell$, let $\partial_i P = \{x \in P \mid L_i(x) = 0\}$. If $\partial_i P \neq \{0\}$, then $\partial_i P \setminus \{0\}$ is by the induction hypothesis a disjoint union of a finite number of k-rational simplicial cones of dimension $< n$. If a simplicial cone in $\partial_i P$ has a nonempty intersection with some $\partial_1 P$, then it is clearly contained in $\partial_i P \cap \partial_1 P$. Therefore $\partial_1 P \cup \dots \cup \partial_\ell P \setminus \{0\}$ is a disjoint union of k-rational simplicial cones of dimension $< n$, so that

$$\cup\, \partial_i P \setminus \{0\} = \bigcup_{j \in J} C_j ,$$

where $C_j = C(v_1, \dots, v_{d_j})$, $v_1, \dots, v_{d_j} \in V_k$, $d_j < n$. For every $j \in J$ we put $C_j(u) = C(v_1, \dots, v_{d_j}, u)$. This is a $(d_j + 1)$-dimensional k-rational simplicial cone. We claim that

$$P \setminus \{0\} = \bigcup_{j \in J} C_j \cup \bigcup_{j \in J} C_j(u) \cup \mathbb{R}_+ u.$$

Indeed, if the point $x \in P \setminus \{0\}$ lies on the boundary of P, then it belongs to some $\partial_i P$, hence to $\bigcup_{j \in J} C_j$. On the other hand. if., belongs to the interior of P, then $L_i(x) > 0$ for all i. If x is a scalar multiple of u, then we have $x \in$ As1-ume this is not the case, and let s be the minimum of the numbers Thens > 0 and $x - su$ lies on the boundary of P. Since $x - su \neq$ there is a unique $j \in J$ such that $x - su \in C_j$, and thus there is a unique $j \in J$ such that $x \in C_j(u)$. This proves the claim.

Now let

$$P = \{x \in V \mid L_i(x) \geq 0,\ 0 < i \leq \ell,\ M_j(t) > 0,\ j = 1, \dots ,m\}$$

Then

$$P \subseteq \{x \in V \mid L_i(x) \geq 0,\ M_j(x) \geq 0\}$$

is a disjoint union of a finite number of k-rational simplicial cones and $\{0\}$. For every $j = 1, \dots, m$, let $\partial_j P = \{x \in P \mid M_j(x) = 0\}$. If a simplicial cone in $\bar P$ has nonempty intersection with $\partial_j P$, then it is contained in $\partial_j P$. As $P = \bar P \smallsetminus \bigcup_{j=1}^{m} \partial_j P$, we see that since $\bar P \smallsetminus \{0\}$ is a disjoint union of finitely many k-rational simplicial cones, then so is P. □

(9.2) Corollary. *If C and C' are k-rational polyhedric cones, then $C \smallsetminus C'$ is also a k-rational polyhedric cone.*

Proof: We may assume without loss of generality that C and C' are k-rational cones. Let d be the dimension of C'. Then there are n k-rational linear forms $L_1, \dots, L_{n-d}, M_1, \dots, M_d$ such that

$$C' = \left\{ x \in V \mid L_1(x) = \cdots = L_{n-d}(x) = 0,\ M_1(x) > 0, \dots, M_d(x) > 0 \right\}.$$

If we define, for each $i = 1, \dots, n-d$,

$$C_i^{\pm} = \left\{ x \in C \mid L_1(x) = \cdots = L_{i-1}(x) = 0,\ \pm L_i(x) > 0 \right\},$$

and for each $j = 1, \dots, d$,

$$C_j = \left\{ x \in C \;\middle|\; \begin{array}{l} L_1(x) = \cdots = L_{n-d}(x) = 0, \\ M_1(x) > 0, \dots, M_{j-1}(x) > 0,\ M_j(x) \le 0 \end{array} \right\},$$

then we find, as can be checked immediately, that $C \smallsetminus C'$ is the disjoint union of the sets $C_1^+, C_1^-, \dots, C_{n-d}^+, C_{n-d}^-, C_1, \dots, C_d$. By (9.1), these are either empty or k-rational polyhedric cones. Therefore $C \smallsetminus C'$ is also. □

It is a rare and special event if a new substantial insight is added to the foundations of algebraic number theory. The following theorem, proved by SHINTANI in 1979, falls into this category. Let K be a number field of degree $n = [K:\mathbb{Q}]$, and let $\mathbf{R} = [\prod_\tau \mathbb{C}]^+$ be the corresponding Minkowski space ($\tau \in \mathrm{Hom}(K, \mathbb{C})$). Define

$$\mathbf{R}_{(+)}^* = \{ (x_\tau) \in \mathbf{R}^* \mid x_\tau > 0 \text{ for all real } \tau \}.$$

(Observe that one has $\mathbf{R}_{(+)}^* = \mathbf{R}_+^*$ only in the case where K is totally real.) Since $\mathbf{R} = K \otimes_{\mathbb{Q}} \mathbb{R}$, the field K is a $\mathbb{Q}$-structure of $\mathbf{R}$. The group

$$\mathcal{O}_+^* = \mathcal{O}^* \cap \mathbf{R}_{(+)}^*$$

of totally positive units acts on $\mathbf{R}_{(+)}^*$ via multiplication, and we will show that this action has a fundamental domain which is a $\mathbb{Q}$-rational polyhedric cone:

(9.3) **Shintani's Unit Theorem.** *If E is a* subgroup of *finite index in then there exist.� a* IQl-rational *polyhedric* cone *P such that*

$$\mathbf{R}^*_{(+)} = \bigcup_{\varepsilon \in E} \varepsilon P \qquad \textit{(disjoint union).}$$

Proof: We consider in R7+i the nonn-one hypersurface

$$S = \left\{ x \in \mathbf{R}^*_{(+)} \;\middle|\; |N(x)| = 1 \right\}$$

Every .l E R�+i is in a unique way the product of an element of *S* and of a positive scalar element. Indeed, *x* = IN(x) Il/n(x/lN(x)l 11"). By Dirichlet's unit theorem, £ (being a subgroup of finite index in o*) **i'>** mapped by the mapping

$$\ell : S \longrightarrow \Big[\prod_{\tau} \mathbb{R} \Big]^+, \quad (x_\tau) \longmapsto \big(\log |x_\tau| \big),$$

onto a complete lattice *r* of the trace-zero space *H* = {x E (TTrRJ+/ *Tr(x)* = 0). Let </J be a fundamental me�h of *r,* let *"iii* be the closure of </J in *H,* and put *F* = £ 1("iii). Since *"iii* is bounded and c\o'ied, �o is *F.* It is therefore compact, and we have

(I)

Let\. E *F* and *Us(x)* = */y* ER l lit - yll < 8},; **R�11**, *0* > 0. Then there is clearly a basis 1•1, ... , *Vn* E UA(x) of **R** such that *X* = !1 V1 + ⋯ + *t,,v,.* with $t_1 > 0$. Since *K* i'> den�e in **R** by the approximation theorem, we may even choose the v_1 to lie in *Kn* VJ(\). Then *Cs* = *C(v₁, ...v,,)* is a IQl-rational simplicial cone in R7+i with *x* E *Cs,* and every *y* E *Cii* is of the form *y* = *AZ* with A ER: and *z* E *Uo(x).* We may now choose *8* sufficiently small so that

Con SC/j = 0 for all FE£, *c* #- **l.**

If not, then we would find sequences Avz1,, E C1;,,, A, ,A;, ER:, *z,,,z;,* E and *t',.* E £, #- I, such that = *s"A;,z�*, and thus *PvZv* = and :¹₀ would converge lO *x;* now *Pc-* would converge to I as = *N(z�),* i.e., *x* = (limc,.)x. This would mean that Jim *E,,* = I. is impossible. since£ is discrete in **R.**

F being compact, we thu'i find a finite number of IQl-rational cones **C₁•••••** *Cm* in R�₁l such that

(2) F�LJ(C,nF) l=l

and C; n EC, = 0 for all F E £, t #- 1. and all i = L .. , rn. From (1) and (2), we deduce that

R(1i=U LJtC,.
1=1 FE£

In order to lurn this union into a di5joint one, we put C/^{1}l = C1 and

c,(IJ=Ci-..... L JEC1. i=2, .. ,rn,
, ,,

eC1 and C, are di:,,joint for almost all£ E £. Hence, by (9.2), C,°\ is a Qi-rational polyhedric cone. Observing that C1 n EC, = 0 for EE£, e i- I. we obtain

R�+, = U LJ £C?l
1=1 cc£

and £Cl^{1}l n C?J = 0 for all£ E t,' and i = 2, .. , m.

We now as:,,ume by induction that we have found a tinite system of (Qi-rational polyhedric cones c\vl. . ct^1, v = l, ... , rn - 2 satisfying the following properlies:

(i) c,c"l i;C;,

(ii) R7+ = U LJ £Lt^1,
1 1=1 cc£

(iii) cci�) nC1 =0 for all£ E £, ifi :S v and i -=f-j.

We put c,<"+l) = ci") for i :S \J + I, and

civ+l) =Ci"^{1}" U FC��l for i:::. 11+2.
HcF

Then c[v+^{1}l, ... ,c�;'+lJ is a finile 5ystem of Qi-rational polyhedric cones which enjoys propertie:,, (i), (ii), and (iii) with v+ I instead of \J. Con:,,equently, C/"'-ll, .. c,�;n-lJ b a 5ystem ofQ-rational polyhedric cones wch that

R(+i = LJ LJ cC,i"' 11 (disjoint union). □
1=1 tE.E

Based on Shintani 's unit theorem, we now obtain the following description of Dirichlet'5 L-series. Let m be an integral ideal, 1m; pm the ray class group mod m. Let x : 1m / pm -,,. be a Dirichlet character mod m, and

x(o)
L(x,.<) � � 'Yl(o)'

the associated Dirichlet L-series. If *R* varies over the classc� of *.rm/P'''*, then we have

$$L(x,.n \text{ � } \mathrm{I{:}x(Jl)Wl,.,J} \atop ;;$$

with the partial zeta functions

$$((\mathrm{Jl..,})\text{�} \underset{\text{nmtegral}}{1} \ \text{'ll(a)'}$$

Let *R* be a fixed class, and *a* an integral ideal in .R.. Furthermore let (I+ a-¹mh =(I+ a-¹m) n R7+i be the set of all totally positive elements in I+ a-¹m. The group

E=o�'={eE IF=lmodm,t:ER�+i}

acts on (I+ a-¹m)+, and we have the

(9.4) Lemma. *There* is *a bijection*

$$(1+\mathfrak{a}^{-1}\mathfrak{m})_+/E \xrightarrow{\ \sim\ } \mathfrak{K}_{\mathrm{int}}\,, \quad \bar{a} \longmapsto a\mathfrak{a}\,,$$

on/o the 8et R,₁₁₁ of *integral ideal." in R.*

Proof: Let *a* E (I+ a-¹m)+- Then we have *(a -* l)a C; m, and :;.ince *a* and m are relatively prime, we get *a -* I E m, i.e., *(a)* E p(mJ. Hence *aa* lies in *it* Furthermore, we have *aa* C; a(I + a-¹m) = *a*+ m = *o,* :;,o that *aa* is integral. Therefore *a* 1-l- *aa* gives us a mapping

(I+ a-¹m)+---+R,₁₁₁.

It is sur:jective, for if *aa, a* E *pm,* is an integral ideal in *R,* then *(a -* l)a C; ma C; m, so that *a* E I + *a*· ¹m. and also *a* E Rr+J' and :;,a *a* E (I+ a-¹m)+- For *a,h* E (I+ a-¹m)+, we have *aa* = *ha* if and only if *(a)*= (h), �o that *a*= *he* with EE Since *r* E (I+ a-¹m)+, it follow:;, that *E* E £, i.e., *a* and *h* have exactly the �ame image if and only if they belong to the same class under the action of £. D

The lemma implies the following fonnula for the partial zeta function ((Jl..,),

$$\zeta(\mathfrak{K},s) = \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \sum_{a\in\mathfrak{R}} \frac{1}{|N(a)|^s}\,,$$

where Vl runs through a syslem of representatives of (I+ a-^{1}m)+/ E. To thi,; we now apply Shintani's unit theorem. Let

R�+J = LJ LJ £C,
i=lfE/!,

be a disjoint decomposition of R7+J inlo linilely many Q-rational simplicial cones C,. For every i = I, , m. let v, 1, . , .. v,J be a linearly independent syslem of generators of C,. Multiplying if nece..sary by a convenient totally positive inleger, we may assume that all v;f lie in m. Let

C/ = { t1 v;l + ... + !J, V1J1 | O < ff .:S I},

and

$$R(\mathfrak{K}, C_i) = (1 + \mathfrak{a}^{-1}\mathfrak{m})_+ \cap C_i$$

Then we have the

(9.5) Proposition. *The set.*� R(fi.,C;) *are finite*, and one *has*

$$\zeta(\mathfrak{K}, s) = \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \sum_{i=1}^{m}$$

with the zeta functions

$$\zeta(C_i, x, s) = \sum_{z} \left| N(x + z_1 v_{i1} + \cdots + z_{d_i} v_{id_i}) \right|^{-s}$$

where z = (z1, ...• *z*,*1*) *varies* over *all d;-tuples* of *nonnegative* integers.

Proof: R(fi.,C,) is *a* bounded subset of the lattice u-^{1}m in **R,** translated by I. It is therefore fmite. Since C, £ R(+J is the simplicial cone generated by v, 1, , v_1J_1 Em, every *a* E (I + u-^{1}m) n C, can be written uniquely as

with rational numbcri,, Yt > 0. Putting

Yf = xf + zf, 0 < re .:S I, 0 .:S E Z.

we have E l+a ^{1}mbecauseLztV,t Ems;a-^{1}m.lnotherwords, every *a* E + a-^{1}m) n C_1 can be written uniquely in the form with t $=$ *L:Xev;e* E R(Jt,C1). Since

(I+ a-¹m)+ = lJ LJ (l + a-¹m) *n* cC,,
/=]CE.t.

a=x+LZfV,c runs through a system 9'l: ofrcpre!,cntatives of (l+a-¹m)+/ *E* if i runs through the numbers I, , *m, x* through the elements of *R(.\t,* C1), and z $=$ (z1, , *ZiJ,)* through integer tuples with 2: 0. Thus we indeed find that

$$\zeta(\mathfrak{K}, s) = \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \sum_{i=1}^{m}$$ □

(9.6) Corollary. *For the Dirichlet L-1,eries attached to the Dirichlet character* *x* : *J*m/ *P*'11 --;. C*,we have *the decomposition*

x(a) *m*
L(x,,)� � '1l(a)' ,� $\sum$ $\zeta(C_i, x, s)$

where .lt *runs through the classes 1m;pm,* and a *denotes an integral ideal in* .lt, *one for each class.*

The relation between zeta functions and Bernoulli numbers hinges on a purely analytic fact which is independent of number theory. This is what we will de1-cribe now.

Let *A* be a real *r* x n-matrix, *r* _::: *n,* with *positive* entries *a1,.* 1 .:S *j .:Sr,* 1 :'.:: i :'.:: *n.* From this matrix we con1-truct the linear forms

$L_i(t_1, \dots, t_n) =$ and *L'j(z1. ,z,)=[:a11z1*
J=l

For an r-tuple *x* $=$ (x1, ... ,x,.) of *positive* real numbers, we write the following series

t(A,x,s) = n *L:<,* + *x)-'.*
l=l

On the other hand we define the generalized **Bernoulli polynomials** *B*�(A, t) by

$$B_k(A, x) = \frac{1}{n} \sum_{i=1}^{n} B_k(A, x)^{(i)},$$

where *Bi.(A,* x)(¹l/*(k* !)11 is the coefficient of

U(k-l)n(tl . *l1 1ft1* l., .,,,/-1

in the Laurent expansion at 0 of the function

$$\prod_{i=1}^{n} \frac{\exp(u x_i L_i(t))}{\exp(u L_i(t)) - 1}\Big|_{t_r=1}$$

in the variables $u, t_1, \dots, t_{r-1}, t_{r+1}, \dots, t_n$. For $r = n = 1$ and $A = a$, we have $B_k(a, x) = a^{k-1} B_k(x)$, with the usual Bernoulli polynomial $B_k(x)$ (see § 1, exercise 2). The equation

$$B_k(A, 1-x) = (-1)^{kn} B_k(A, x),$$

where $1 - x$ signifies $(1 - x_1, \dots, 1 - x_n)$, is easily proved.

(9.7) Proposition. *The series* $\zeta(A, x, s)$ *is absolutely convergent for* $\mathrm{Re}(s) > r/n$, *and it can be meromorphically continued to the whole complex plane. Its values at the points* $s = 1 - k$, $k = 1, 2, \dots$, *are given by*

$$\zeta(A, x, 1-k) = (-1)^n \frac{B_k(A, x)}{k^n}.$$

Proof: The absolute convergence for $\mathrm{Re}(s) > r/n$ is deduced from the convergence of a series $\sum$ [illegible] by the same arguments that we have used repeatedly. It will be left to the reader. The remainder of the proof is similar to that of (1.8). In the gamma function

$$\Gamma(s)^n = \int_0^\infty \cdots \int_0^\infty \prod_{i=1}^n e^{-t_i} (t_1 \cdots t_n)^{s-1}\, dt_1 \cdots dt_n$$

we substitute

$$t_i \longmapsto L_i^*(z+x) t_i$$

and obtain

$$\Gamma(s)^n \prod_{i=1}^n L_i^*(z+x)^{-s} = \int_0^\infty \cdots \int_0^\infty \exp\Big[-\sum_{i=1}^n t_i L_i^*(z+x)\Big](t_1 \cdots t_n)^{s-1}\, dt_1 \cdots dt_n.$$

Summing this over all $z = (z_1, \dots, z_r)$, $z_i \in \mathbb{Z}$, $z_i \geq 0$, and observing that

$$\sum_{i=1}^n t_i L_i^*(z+x) = \sum_{j=1}^r (z_j + x_j) L_j(t),$$

yields the equation

$$\Gamma(s)^n\zeta(A,x,s) = \int_0^\infty \cdots \int_0^\infty g(t)(t_1\cdots t_n)^{s-1}\,dt_1\cdots dt_n$$

with the function

$$g(t) = \prod_{i=1}^{r} \frac{\exp((1-x_i)L_i(t))}{\exp(L_i(t))-1}.$$

We cut up the space $\mathbb{R}^n_+$ into the subsets

$$D_i = \{t \in \mathbb{R}^n_+ \mid 0 \le t_\ell \le t_i,\ \ell = 1,\dots,i-1,i+1,\dots,n\}$$

for $i = 1,\dots,n$, and get

(1) $$\zeta(A,x,s) = \Gamma(s)^{-n}\sum_{i=1}^{n}\int_{D_i} g(t)(t_1\cdots t_n)^{s-1}\,dt_1\cdots dt_n.$$

In D_i we make the transformation of variables

$$t = uy = u(y_1,\dots,y_n),$$

where $0<u$, $0 \le y_\ell \le 1$ for $\ell \ne i$ and $y_i = 1$. This gives

$$\Gamma(s)^{-n}\int_{D_i} g(t)(t_1\cdots t_n)^{s-1}\,dt_1\cdots dt_n$$
$$= \Gamma(s)^{-n}\int_0^\infty\Big[\int_0^1\cdots\int_0^1 g(uy)\big(\prod_{\ell\ne i} y_\ell\big)^{s-1}\prod_{\ell\ne i} dy_\ell\Big]u^{ns-1}\,du.$$

For $0<\varepsilon<1$, let now $I_\varepsilon(1)$, resp. $I_\varepsilon(+\infty)$, denote the path in $\mathbb{C}$ consisting of the interval $[1,\varepsilon]$, resp. $[+\infty,\varepsilon]$, followed by a circle around 0 of radius ε in the positive direction, and the interval $[\varepsilon,1]$, resp. $[\varepsilon,+\infty]$. For ε sufficiently small, the right-hand side of the last equation following (1.9) becomes

(2) $$A(s)\int_{I_\varepsilon(+\infty)}\int_{I_\varepsilon(1)^{n-1}}\Big[g(uy)u^{ns-1}\big(\prod_{\ell\ne i} y_\ell\big)^{s-1}\prod_{\ell\ne i} dy_\ell\Big]du,$$

with the factor

$$A(s) = \frac{\Gamma(s)^{-n}}{(e^{2\pi ins}-1)(e^{2\pi is}-1)^{n-1}}$$

where one has to observe that the linear forms $L_1,\dots,L_r$ have positive coefficients. It is easy to check that the above expre5Sion, as a function of the variable .l, is meromorphic on all ofC. As for lhc factor A(s), (1.2) implies that

$$A(s) = \frac{I}{(2rri)n} \frac{I'(l-s)^{11}}{} (c2rrin., \_ l)(e2\text{-}'m \_ 1)\text{-}1\, enrris\bullet$$

Let us now puts= 1 -*k*. The function *eu:rr1.'(e²ru¹¹s -* l)/(e²nn - I) takes the value $(-1)^{11}r^{1}\text{-}^{1}\ln$ at $s = I - k$. Thus expression (2) turns into

$$(-l)"(k-l) \frac{r(k)"}{n} \frac{.-.-n}{(2m)} \int_{K, K�-l} [\ \mu\text{-}(uy)u"(l - AJ\text{-}](TT\ yr) - kn \ dY \Big|_{ff,\ f,i1} f\ du,$$

where *Kc* denotes the positively oriented circumference of the circle of radius f, and where we have to observe that the integrals over (oo,£1 and Le,oo), resp. over 11,c] and [E, Jj, kill each other in (2) ifs= I - *k*. This obviou:;,ly ((- I)"(l- IJ *I'(k)"* /n) times the coefficient of un(k-l)(TTr,,:ci in the Laurent expansion of the function

$$R(U.\}'1, \cdot\text{--},llYi\text{-}1,ll,ll\}';+1, \ldots ,uyn) = \prod_{j=l} \frac{exp(u(l -Xi)Li(y))}{exp(uL_1(y)) - 1}\Big|_{y,=l},$$

which i:;. a holomorphic function of *u*, t1, . ,*t1*. 1, *ft+!, ... !11* in the direct product of *n* copies of the punctured of radius *F*. Therefore the value of (2) at $s = I - k$ equals $(-l)^{11}(k$ I - x)(iJ /*n*. Inserting this into (1) gives

$$((A,x, \ldots k) = \frac{\text{<--l>..-l-k--l-l-k--..}\text{!}}{n} \sum_{i=-1}^{t} Bk(A, \ldots x/1)$$

$$= (-])"\{k\ -1\}\ \underline{Bk(A�!- \quad X).}$$

Together with the equation *Bk(A,* 1 - *x)* = (- l)"(k ¹¹ ,*r Bk(A, x)* mentioned above, this gives the de�ired rc<;ult. 0

Theorems (9.5) and (9.6) now imply our main result concerning the value:;, of Dirichlel L-<;crie5 *L(x,s)* at integer points $s = 1 - k$, A.= 1,2, If *K* is not totally real, then these value� are all zero (except if *X* is the trivial character, for which $s = 0$ is not a zero). Thi<; can be read off immediately from the functional equation (8.6) and (5.11).

So we let *K* be a totally real number field of degree *n*. Numbering the embeddings r : *K* ----+ lP/. identifies the Minkow�ki R with *!Rn.* and R7+i = R� with the set JP/.: of vector� (x1, with positive coefficient<; x_1. Given the Q-rational simplicial cone C � IR: generated by 1•11, ., *Vu/,,* we again consider lhc zeta functions

((C,,r,s)=�IN(x+:11111+· +zd,v111,)l ·'

If

$$v_{ij} = (a_{i1}^{(i)}, \ldots, a_{in}^{(i)}), \quad j = 1, \ldots, d_i$$

then $A_i = (a_{jk}^{(i)})$, a $(d_i \times n)$-matrix with positive entries, and the k-th component of $z_1 v_{i1} + \cdots + z_{d_i} v_{i d_i}$ becomes

$$L_k^*(z_1, \ldots, z_{d_i}) =$$

For $x \in$ R:, we therefore get

$$\zeta(C_i, x, s) = L \prod_{z\ k=1} L_j^*(z_1, \ldots, z_n)^{-s} = \zeta(A_i, x, s),$$

and, from (9.5) and (9.6), we obtain by putting $s = 1 - k$ the

(9.8) Theorem. *The values of the partial zeta function* $\zeta(\mathfrak{K}, s)$ *at the integral points* $s = 1 - k$, $k = 1, 2, 3, \ldots$, *are given by*

$$\zeta(\mathfrak{K}, 1 - k) = \mathfrak{N}(\mathfrak{a})^{k-1} \sum_{i=1}^{m} \Big[(-1)^{d_i} \ _{x}$$

and the values of the Dirichlet L-series $L(\chi, s)$ *are given by*

m [I: $B(A$,)] $L(\chi, 1-k)$

(-1)", I:

!! I=1 $\in N(.fi..(,\}$ k

Here $\mathfrak{a}$ *is an integral ideal in the class* $\mathfrak{K}$ of $J^{\mathfrak{m}}/P^{\mathfrak{m}}$.

This result about the Dirichlet L-series $L(\chi, s)$ also covers the Dedekind zeta function $\zeta_K(s)$. The theorem says in particular that the values $L(\chi, 1-k)$, for $k \geq 1$, are algebraic numbers which all lie in the cyclotomic field $\mathbb{Q}(\chi_1)$ generated by the values of the character χ_f. The values $\zeta_K(1 - k)$ are even *rational* numbers. From the functional equation (5.11),

$$\zeta_K(1 - s) = |d_K|^{s - 1/2} \left(\cos \frac{\pi s}{2}\right)^{r_1 + r_2} \left(\sin \frac{\pi s}{2}\right)^{r_2} L_{\mathbb{C}}(s) n \zeta_K(s),$$

we deduce that $\zeta_K(1 - k) = 0$ for *odd* $k > 1$, and it is $\neq 0$ for *even* $k > 1$. If the number field K is not totally real, then we have $\zeta_K(s) = 0$ for *all* $s = -1, -2, -3, \ldots$

(9.9) Corollary *(SIEGEL-KLINGEN). The values of the partial zeta function* $\zeta(\mathfrak{K}, s)$ *at the points* $s = 0, -1, -2, \ldots$ *are rational numbers.*

Proof: Lcta1, .. ,.ar be nonzero numbers in *K,* and let *A* be the *(r* x *n)*-matrix *(a;* where *a* is the i-th componenl of *a* after identifying **R** = *R.n* according to the chosen numbering of the embeddings r : *K* -----*f* lFL It is enough to show that *B!,_(A,x)* is a rational number for every r-tuple of rational numbers.\ = (x1, ... *Xr),* To see this, let LIQ be the normal closure of KIQ and cr E G(LIQ). Then *a* induces a permutation of the indice� {1,2, ... ,*n)* so that

$$aa_{11}=Gjrr(i) \quad (l\_:::j\_:::r, i=l. \ldots\ldots\ldots, n).$$

Now we had $B_k(A,x) = \frac{1}{4}$ *L*�=*l* *Bk(A,xtl,* where Bk(A,_\){[1]l was the coefficient of $u^{n(k-1)+r}(t_1, \ldots$,*t;_1,t,+1,* .. ,,tn)J..-I in the Taylor expansion of the function

$$\prod_{J=I}^{Ur} \frac{\exp(XjULi(f))}{\exp(uL_1(t) - 1)}$$

with $L_1(t) = a_{11}t_1 + \cdots + a_1ntn$, This makes it clear that *Bk(A,x)Ui* lie� in Land that *aBk(A.x)(,)* = *Bk(A,x)i"11ll*_Therefore *Bk(A..t)* b invariant under the action of the Galois group *G(L* IQ), and thus belongs to Q. □

The nature of the special values of L-series at integer points has recently found increasing interest. Like in the class number formula, which expresses the behaviour of the Dedekind zeta function at the point� = 0, the properties of all the 5pecial values indicate a deep arithmetic law which appears to extend to an extremely wide cla::r, of L-scries, the L-series attached to "motives" According to a conjecture of the American mathematician STEPHEN LICHTENBAUM, t l�ig�ificance of these L-values can be explained by a strikingly simple geometric interpretation: they appear according lO the **Lichtenbaum conjecture** as Euler characteristics in etale cohomology (�ee [99], I12J). The proof of this conjecture is a great, if �till remote, goal of number theory. On the way towards it, the inr,ights into the nature of L-series which we have encountered may prove to he important.

Finally we want to mention that the French mathematicians *DANltL BARSKY* and *P11:.Rtfrt Ct.55ou-Noccts* have used *S111,'.TAl\'1's* result to prove the exi�tcnce of *p-adic L-series.* These play a major r61e in *lwasawa theory,* which we have mentioned before. The *p-adic zeta function* of a totally real number field *K* is a continuous function

$$(p : Z'' \text{ "-}\{IJ \to Q''.$$

which is related to the ordinary Dedekind zeta function *(K* (s) by

$$(,(-n) \to (K\{-n) \prod_{pip} (I - \text{'}ll(p)'')$$

for all $n \in \mathbb{N}$ such that $-n \equiv 1 \bmod d$, where $d = [K(\mu_{2p}) : K]$ denotes the degree of the field $K(\mu_{2p})$ of 2p-th roots of unity over K. The p-adic zeta function is uniquely determined by this relation. Its existence hinges on the fact that the rational values $\zeta_K(-n)$ are subjected to severe congruences with respect to p.

§ 10. Artin L-series

So far, all L-series we have considered were associated to an individual number field K. With the *Artin L-series*, a new type of L-series enters the stage; these are derived from representations of the Galois group $G(L|K)$ of a Galois extension $L|K$. This new kind of L-series is intimately related to the old ones via the main theorem of class field theory. In this way they appear as far-reaching generalizations of the old L-series. Let us explain this for the case of a Dirichlet L-series

$$L(\chi,s) = \sum_{n=1} \qquad = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

attached to a Dirichlet character

$$\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow$$

Let $G = G(\mathbb{Q}(\mu_m)|\mathbb{Q})$ be the Galois group of the field $\mathbb{Q}(\mu_m)$ of m-th roots of unity. The main theorem of class field theory in this particular case simply describes the familiar isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^* \cong G,$$

which sends the residue class $p \bmod m$ of a prime number $p \nmid m$ to the *Frobenius automorphism* φ_p, which in turn is defined by

$$\varphi_p \zeta = \zeta^p \quad \text{for} \quad \zeta \in \mu_m .$$

Using this isomorphism we may interpret χ as a character of the Galois group G, or in other words, as a 1-dimensional *representation* of G, i.e., a homomorphism

$$\chi : G \longrightarrow GL_1(\mathbb{C}).$$

This interpretation describes the Dirichlet L-series in a purely Galois-theoretic fashion,

$$L(\chi,s) = \prod_{p \nmid m} \frac{1}{1-\chi(\varphi_p)p^{-s}},$$

and allows us the following generalization.

Let LI K be a Galois extension of finite algebraic number flclds with Galois group G = G(LIK). A representation of G is an action of G on a finite dimensional C-vector space *V,* i.e., a homomorphism

$$p\text{: G --+ } GL(V) = \text{Autr:(V)}.$$

Our shorthand notation for the action of *er* E G on v E V is *av.* instead of the complete expression *p(u)v.* Let p be a prime ideal of *K,* and let $Ill be a prime ideal of L lying above p. Let G<;p be the decomposition group and *1*13the inertia group of ,.P- over p. Then we have a canonical isomorphhm

$$G_{\mathfrak P}/I_{\mathfrak P} \xrightarrow{\sim} G\big(\kappa(\mathfrak P)|\kappa(\mathfrak p)\big)$$

onto the Galois group of the residue field extension K(l,JJ)IK(IJ) (see chap. I, (9.5)). The factor group G'll/ /13 is therefore generated by the Frobenius automorphism lf'll whose image in G(K(l.l})IK(p)) is the q-th power map *x f--+ .-,;11,* where q = '.Jl(p). *'P'+l* is an endomorphism of the module V"ll of invariants. The characteristic polynomial

det(l - (f'qJI; V1':P)

only depends on the prime ideal p, nol on the choice of the prime ideal ? above p. In fact, a different choice ?'lp yields an endomorphism conjugate to ({'<,p, as the decomposition groups G13 and G<,p', the inertia groups lti und f.-:µ,, and the Frobenius automorphisms 'P'+l and 'P'+l' arc :c.imultancous conjugates. We thus arrive at the following

(10.l) Definition. *Let LIK be* a *Galois extension of algebraic* number *fields with* Galois group G, *and lcl (p,* V) be a representation of G. *Then the* Artin L-series *,ittached to p is defined to* be

C(LIK ,p,s) = Q I / det(l - tpii91(p)-s; V1·ʟɪɪ)

where p runs *through all* prime ideals of *K.*

The Arlin L-series converges absolutely and uniformly in the half-plane Rc(5) ? 1 + *0,* for any *ti* > 0. It thus defines an analytic function on the half-plane Re(s) > I. This is shown in the same way as for the Hecke L-series (see (8.1)), observing that the *E",* in the factorization

$$\det\big(1-\varphi_{\mathfrak P}\mathfrak N(\mathfrak p)^{-s};V^{I_{\mathfrak P}}\big) = \prod_{i=1}^{d}\big(1-\varepsilon_i\mathfrak N(\mathfrak p)^{-s}\big)$$

arc roots of unity because the endomorphism 'P'+l of *Vt,,,,,* ha? finite order.

For the trivial representation (p,C), $p(a) = 1$, the Artin L-serics is simply the Dedekind zeta function $f;K(s)$. An additive expression analogous to the expansion

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}$$

does not exist for general Artin L-series. But they exhibit a perfectly regular behaviour under change of extensions LI K and representations p. This allows to deduce many of their excellent properties. As a preparation for this study, we first collect basic facts from representation theory of finite groups. For their proofs we refer to [125].

The degree of a representation *(p,* V) of a finite group G is the dimension of *V*. The representation is called irreducible if the G-module *V* doer, not admit any proper G-invariant r,ubspace. An irreducible representation of an *ahe!ian* group is simply a character

$$p: G - \quad = GL_1(C).$$

Two reprer,entations *(p, V)* and *(p', V')* are called equivalent if the G-modules V and V' are isomorphic. Every representation *(p,* V) factors into a direct sum

$$V = ViEB \cdot\cdot EBV.1$$

of *irreducible* representation1-. If an irreducible representation *(Pa, Va)* is equivalent to precisely *ra* among the represcmations in this decomposition, then *ra* is called the multiplicity of *Po:* in p, and one writes

$$\rho \sim \sum r_\alpha \rho_\alpha,$$

where *Po:* varies over all non-equivalent irreducible representations of G.

The character of a representation *(p,* V) is by dclinition the function

$$Xp: G - \quad C, \qquad Xp(a) = \text{trace } p(u).$$

One has $Xp(l) = \dim V = \text{degree(p)}$, and $Xp(ara^{-1}) = Xp(r)$ for all a, r E G. In general, a function / G -cl- C with the property that $/(aru^{-1}) = .f(r)$ is called a central function (or class function). The special importance of characters comes from the following fact:

Two representations are equivalent if and only if their characters are equal. If $p \sim La\ ro:Pa$, then

$$\chi_\rho = \sum_\alpha r_\alpha \chi_{\rho_\alpha}$$

The character of the *trivial representation* $\rho : G \to GL(V)$, $\dim V = 1$, $\rho(\sigma) = 1$ for all $\sigma \in G$, is the constant function of value 1, and is denoted by 1_G, or simply 1. The *regular representation* is given by the G-module

$$V = \mathbb{C}[G] = \Big\{ \sum_{\tau\in G} x_\tau \tau \;\Big|\; x_\tau \in \mathbb{C} \Big\},$$

on which the $\sigma \in G$ act via multiplication on the left. It decomposes into the direct sum of the trivial representation $V_0 = \mathbb{C}\sum_{\sigma\in G}\sigma$, and the *augmentation representation* $\{\sum_{\sigma\in G} x_\sigma \sigma \mid \sum_\sigma x_\sigma = 0\}$. The character associated with the regular, resp. the augmentation representation, is denoted by r_G, resp. u_G. We thus have $r_G = u_G + 1_G$, and explicitly: $r_G(\sigma) = 0$ for $\sigma \neq 1$, $r_G(1) = g = \#G$.

A character χ is called *irreducible* if it belongs to an irreducible representation. Every central function φ can be written uniquely as a linear combination

$$\varphi = \sum_\chi c_\chi \chi, \quad c_\chi \in \mathbb{C},$$

of irreducible characters. φ is a character of a representation of G if and only if the c_χ are rational integers ≥ 0. For instance, for the character r_G of the regular representation we find

$$r_G = \sum \chi(1)\chi,$$

where χ varies over all irreducible characters of G. Given any two central functions φ and ψ of G, we put

$$(\varphi,\psi) = \frac{1}{g}\sum_{\sigma\in G} \varphi(\sigma)\overline{\psi(\sigma)}, \quad g = \#G,$$

where $\overline{\psi}$ is the function which is the complex conjugate of ψ. For two irreducible characters χ and χ', this gives

$$(\chi,\chi') = \begin{cases} 1 & \text{if } \chi = \chi', \\ 0, & \text{if } \chi \neq \chi'. \end{cases}$$

In other words, (,) is a hermitian scalar product on the space of all central functions on G, and the irreducible characters form an orthonormal basis of this hermitian space.

For the representations itself, this scalar product has the following meaning. Let

$$V = V_1 \oplus \cdots \oplus V_r$$

be the decomposition of a representation V with character χ into the direct sum of irreducible representations V_i. If V' is an irreducible representation with character χ', then (χ, χ') is the number of times that V' occurs among the V_i up to isomorphism. For if χ_i is the character of V_i, then $\chi = \chi_1 + \cdots + \chi_r$, so that

$$(\chi,\chi') = (\chi_1,\chi') + \cdots + (\chi_r,\chi'),$$

and we have $(\chi_i,\chi') = 1$ or 0, depending whether V_i is or is not isomorphic to V'. Applying this to the trivial representation $V' = \mathbb{C}$, we obtain in particular that

$$\dim V^G = \frac{1}{g}\sum_{\sigma\in G}\chi(\sigma), \quad g = \#G.$$

Now let $h : H \to G$ be a homomorphism of finite groups. If φ is a central function on G, then $h^*(\varphi) = \varphi\circ h$ is a central function on H. Conversely, one has the following proposition.

(10.2) Frobenius Reciprocity. *For every central function ψ on H there is one and only one central function $h_*(\psi)$ on G such that one has*

$$(\psi, h^*(\varphi))_H = (h_*(\psi),\varphi)_G$$

for all central functions φ on G.

This will be applied chiefly to the following two special cases.

a) *H is a subgroup of G and h is inclusion.*

In this case we write $\varphi|_H$ or simply φ instead of $h^*(\varphi)$, and ψ^* instead of $h_*(\psi)$ (the **induced function**). If φ is the character of a representation (ρ, V) of G, then $\varphi|_H$ is the character of the representation $(\rho|_H, V)$. If ψ is the character of a representation (ρ, V) of H, then ψ^* is the character of the representation $(\mathrm{ind}(\rho), \mathrm{Ind}_H^G(V))$ given by the **induced** G-module

$$\mathrm{Ind}_H^G(V) = \{\, f : G \to V \mid f(\tau x) = \tau f(x) \ \text{for all } \tau \in H \,\},$$

on which $\sigma \in G$ acts by $(\sigma f)(x) = f(x\sigma)$ (see chap. IV, §7). One has

$$\psi^*(\sigma) = \sum_{\tau}\psi(\tau\sigma\tau^{-1}),$$

where τ varies over a system of representatives on the right of G/H, and we put $\psi(\tau\sigma\tau^{-1}) = 0$ if $\tau\sigma\tau^{-1}\notin H$.

b) *G is a quotient group H/N of H and h is the projection.*

We then write φ instead of $h^*(\varphi)$, and $\psi_\natural$ instead of $h_*(\psi)$. One has

$$\psi_\natural(\sigma) = \frac{1}{\#N}\sum_{h(\tau)=\sigma}\psi(\tau).$$

If φ is the character of a representation (ρ, V) of G, then $h^*(\varphi)$ is the character of the representation $(\rho\circ h, V)$.

The following result is of great importance.

(10.3) Brauer's Theorem. *Every character* χ of *a* finite *group* G *is a* Z-*linear* combination of *characters* $\chi_i{}^*$ *induced* from *charncter� χ_i* of *degree* 1 *,,s�ociatcd to subgroups.* H_i of G.

Note that a character of degree 1 of a group His �imply a homomorphim1 χ: H--+

After this brief survey of representation theory for finite groups., we now return to Artin L-series. Since two representation.s V) and (p', V') are equivalent if and only if their characters χ and coincide, we will henceforth write

$$L(L\ |K,\ \chi,.,)\text{�}\ Q\ \det(I - p(\text{�}\cdot o)91(p)\text{-}\cdot'; viv)$$

instead of £..(L IK, p, s). These L-series exhibit the following functorial behaviour.

(10.4) Proposition. (i) For *the principal character* $\chi = 1$, one *ha�*

$$L(L|K,1..<)\ \text{�}\ (K(S).$$

(ii) *If* χ, χ' are *two characters ofG(L* IK), *then*

$$L(L|K,\chi + \chi',.<)\ \text{�}\ C(L|K, \chi,.,)L(L|K,\chi\ ,.,).$$

(iii) For *a bigger Galois extension* L' IK, $L' \supseteq L \supseteq K$. and *a character* χ *of* G(LIK) one *has*

$$C(L'|K.\chi,.,)\ \text{�}\ C(L|K.\chi,.,).$$

(iv) *If* M *is an imermediate field,* $L \supseteq M \supseteq K$, *and* χ is *a character* ofG(LIM), *then*

$$C(L|M, \chi,.,)\ \text{�}\ L(L|K, \chi,..,).$$

Proof: We have already noted **(i)** earlier. (ii) If *(p,* V), *(p'.* V') are representations of $G(L|K)$ with characters χ, χ', then the direct sum *(p* EB *p', V* EB V') is a representation with character $\chi + \chi'$, and

$$\det(1 - rp,:\mu r; (V \text{ EB } V^1)^{1}\text{'}1l) = \det(1 -rp,;pt; V^{1}\text{'}+')\det(I - (\{),:\mu t;\ V'^{1}\text{'}1l)\_$$

This yields (ii).

(iii) Let 'I3'I'I31P be prime ideals of L' IL IK, each lying above the next. Let χ be the character belonging to the $G(L$ IK)-module V. $G(L'|K)$ acts on V via the projection G(L'IK)--+ G(LIK). It induces surjective homomorphisms

$$G,;p,\text{---}+ G,,p,\ l'+.v\text{---}+ I,:\mu,\ G,p\cdot/fo,\_11\text{---}+ G,,pfl,;p$$

of lhe decomposition and inertia groups. The latter maps the Frobenius automorphism rp13, to the Frobenius automorphism 1/J<.p so that (rprp, $V^{1}\cdot v'$) = (rp'l}, *yl-P)*, i.e.,

$$\det(1-\varphi_{\mathfrak{P}'}t\,;\,V^{I_{\mathfrak{P}'}})=\det(1-\varphi_{\mathfrak{P}}t,V^{I_{\mathfrak{P}}})$$

This yields (iii).

(iv) Let G = *G(LIK)* and *H* = G(LIM). Let p be a prime ideal of *K*, q1, ... q, the various prime ideals of *M* above p, and ,P, a prime ideal of *L* above q,, i = I, , *r.* Let G,, resp. *I;,* be the decomposition, resp. inertia, group of ,P, over p. Then *H, = G1* n *H,* resp. /1' = /1 n *H,* arc the decomposition, resp. inertia, groups of ,P, over q1. The degree of q, over p is_{, =*(C;* :H;/1),i.e.,

$$\mathfrak{N}(\mathfrak{q}_i)=\mathfrak{N}(\mathfrak{p})^{f_i}.$$

We choose elements r1 E *G* such that ,p1 = ,P�'. Then C, = r,-1CI r1, and/, = r,-1/1r1. Let rp E G1 be an element which is mapped to the Frobenius rp,ii1 E C1//1. Then *rp1* = r I11{Jr, EC, is mapped to the Frobenius ifl'lJ, E G1//1, and the image *ofip(* in *H,J!/* is the Frobenius of,P, over q,.

Now let *p* : *H* → *CL(W)* be a representation of *H* with character *X*. Then *X** is the character of the induced representation ind(p) : *C* → *GL(V)*, *V* = lndJ *(W)*. Clearly, what we have to show is that

det(l -*l()t; V*I, = JJdet(l -*l{J* I't J *W* I',).
1

We reduce the problem to the case G1 = G, i.e., *r* = l. Conjugating by r,. we obtain

det(l-ip('r.1 W 1;)=det(l-ipf,r.l (r1W) 11�r,Hr,- 1)

and *.f,* = (C (C n r Hr For every i we choose a system of

representatives on the left, *a; 1,* of GI mod GI n r, *H*r,.-1. One checks immediately that then *{a,Jr,/* is a system of representatives on the left of G mod *fl.* We thus have (see chap. IV, §5, p.297) the decomposition

V=EBrr11r1W.

Putting *V, = EBJ a,J* r, *W,* we obtain a decomposition *V* = EB,- *V1* of *V* as a *C* 1-module. Hence

det(I - *ipl;* V11) = � det(l - *rpt;* V111).
1 1

Itis therefore sufficient *to* prove that det(l-l{Jt; *V,*[11]*)=det(l-l{)f,rl1;* (r,W)^{1} 1nr,Hr,-^{1})_

We simplify the notation by replacing G_1 by G, I_1 by I, $G_1 \cap \tau H \tau^{-1}$ by H, f_τ by $f = (G : IH)$, V_τ by V, and τW by W. Then we have still $V = \operatorname{Ind}_H^G(W)$, i.e., we are reduced to the case $r = 1$, $G_1 = G$.

We may further assume that $I = 1$. For if we put $\bar G = G/I$, $\bar H = HI/I$, then $V^I = \operatorname{Ind}_{\bar H}^{\bar G}(W^{I \cap H})$. Indeed, a function $f : G \to W$ in V is invariant under I if and only if one has $f(x\sigma) = f(x)$ for all $\sigma \in I$, i.e., if and only if it is constant on the right (and therefore also on the left) cosets of G mod I, i.e., if and only if it is a function on $\bar G$. It then automatically takes values in $W^{I \cap H}$, because $\sigma f(x) = f(\sigma x) = f(x)$ for $\sigma \in I \cap H$.

So let $I = 1$. Then G is generated by φ, $f = (G : H)$, and thus

$$V = \bigoplus_{i=0}^{f-1} \varphi^i W .$$

Let A be the matrix of φ^f with respect to a basis $w_1, \dots, w_d$ of W. If E denotes the $(d \times d)$ unit matrix, then

$$\begin{pmatrix} 0 & E & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & E \\ A & 0 & & 0 \end{pmatrix}$$

is the matrix of φ with respect to the basis $\{\varphi^i w_j\}$ of V. This gives

$$\det(1 - \varphi t; V) = \det \begin{pmatrix} E & -tE & & 0 \\ \vdots & & \ddots & \\ & & & -tE \\ -tA & & & E \end{pmatrix} = \det(1 - \varphi^f t^f ; W)$$

as desired. The last identity is obtained by first multiplying the first column by t and adding it to the second, and then multiplying the second column by t and adding it to the third, etc. $\square$

The character 1^* induced from the trivial character 1 of the subgroup $\{1\} \subseteq G(L|K)$ is the character $r_G = \sum_\chi \chi(1)\chi$ of the regular representation of $G(L|K)$. We therefore deduce from (10.4) the

(10.5) Corollary. *One has*

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq 1} \mathcal{L}(L|K, \chi, s)^{\chi(1)},$$

where χ varies over the nontrivial irreducible characters of $G(L|K)$.

The starting point of Artin's investigations on L-series had been the question whether, for a Galois extension *LIK,* thequolient *t;L(s)/t;K(s)* is an entire function, i.e., a holomorphic function on the whole complex plane. Corollary (10.5) shows that this could be deduced from the famous

Artin Conjecture: For every irreducible character *x i-* **1,** the Artin L-series *L(LIK, x*,s) defines an **entire** function.

We will '>CC pre:,,ently that this conjecture holds for *ahelian* extension'>. In general it is not known. In view of its momentous comcquences, it constitutes one of the big challenges in number theory.

We will show ncxl that the Artin L-series in the case of *ahelian* extensions *LIK* coincide with certain Hecke L-series, more prcci:,,ely, with generalized Dirichlet L-series. This means that the propertie5 of Heckc's series, and in particular their functional equation, trarn;fer to Artin series in the abelian case. Via functoriality (10.4) they may lhen be extended to the non-abelian

The link between Artin and Hecke L-series is provided by class field theory. Let LI *K* be an abelian extension, and let f be the **conductor** of LI *K,* i.e., the smallest module

such that *LIK* lies in the ray class field *KIIK* (see chap. VI, (6.2)). The **Artin symbol** (�) then gives us a surjective homomorphbm

$$Jf/P^1 \text{---+} G(LIK), \quad \text{amodPff-------+} \ (L�K),$$

from the ray class **group** .If/Pf. Here *Jl* is the group of fractional ideals prime to f, and p! is the group of principal ideals *(a)* such thal $a =$ I mod *f* and a is positive in $K_{11} =$ IR if p is real.

Now let *x* be an *irreducihle* character of the abelian group G(LIK), i.e., a homomorphism

$$X, \ G(LIK)-$$

Composing with the Artin symbol (!.l!S..), this gives a character of the ray clas:,, group *Jf/Pf,* i.e., a Dirichlet character mod f. It induces a character on *J* f, which we denote by

$$X:.!i\text{--+}$$

By (6.9), this character on ideals is a **GrOBencharacter** mod *f* of type (p, 0), and we have the

(10.6) Theorem. Let $L|K$ *be an abelian extension, let* $\mathfrak{f}$ *be the conductor of* $L|K$, *let* $\chi \neq 1$ *be an irreducible character of* $G(L|K)$, *and* $\tilde{\chi}$ *the associated Größencharakter* mod $\mathfrak{f}$.

Then *the Artin L-series for the character* χ *and the Hecke* L-series *for the Größencharakter* $\tilde{\chi}$ *satisfy the identity*

$$\mathcal{L}(L|K,\chi,s) = \prod_{\mathfrak{p}\in S} \frac{1}{1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}}\, L(\tilde{\chi},s),$$

where $S = \{\mathfrak{p}\mid\mathfrak{f} \mid \chi(I_{\mathfrak{P}}) = 1\}$.

Proof: The representation of $G(L|K)$ associated to the character χ is given by a 1-dimensional vector space $V = \mathbb{C}$ on which $G(L|K)$ acts via multiplication by χ, i.e., $\sigma v = \chi(\sigma)v$. Since $\mathfrak{f}$ is the conductor of $L|K$, we find by chap. VI, (6.6), that

$$\mathfrak{p}\mid\mathfrak{f} \iff \mathfrak{p} \text{ is ramified} \iff I_{\mathfrak{P}} \neq 1.$$

If $\chi(I_{\mathfrak{P}}) \neq 1$, then $V^{I_{\mathfrak{P}}} = \{0\}$, and the corresponding Euler factor does not occur in the Artin L-series. If on the other hand $\chi(I_{\mathfrak{P}}) = 1$, then $V^{I_{\mathfrak{P}}} = \mathbb{C}$, so that

$$\det(1-\varphi_{\mathfrak{P}}\mathfrak{N}(\mathfrak{p})^{-s};\, V^{I_{\mathfrak{P}}}) = 1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}.$$

We thus have

$$\mathcal{L}(L|K,\chi,s) = \prod_{\mathfrak{p}\nmid\mathfrak{f}} \frac{1}{1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}} \prod_{\mathfrak{p}\in S} \frac{1}{1-\chi(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}}$$

and

$$L(\tilde{\chi},s) = \prod_{\mathfrak{p}\nmid\mathfrak{f}} \frac{1}{1-\tilde{\chi}(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}.$$

For $\mathfrak{p}\nmid\mathfrak{f}$, one has $\left(\frac{L|K}{\mathfrak{p}}\right) = \varphi_{\mathfrak{P}}$, and so $\tilde{\chi}(\mathfrak{p}) = \chi(\varphi_{\mathfrak{P}})$. This proves the claim. □

Remark: If the character $\chi : G(L|K) \to \mathbb{C}^*$ is *injective*, then $S = \emptyset$, and one has complete equality

$$\mathcal{L}(L|K,\chi,s) = L(\tilde{\chi},s).$$

In this case $\tilde{\chi}$ is a *primitive Größencharakter* mod $\mathfrak{f}$.

If on the other hand χ is the trivial character 1_G, then $\tilde{\chi}$ is the trivial Dirichlet character mod $\mathfrak{f}$, and we have

$$\zeta_K(s) = \prod_{\mathfrak{p}\mid\mathfrak{f}} \frac{1}{1-\mathfrak{N}(\mathfrak{p})^{-s}}\, L(\tilde{\chi},s).$$

The theorem implies lhat the **Artin conjecture** holds for all Artin L-series .C(L IK, $X.s)$ which correspond to nontrivial irreducible characters X of *ahelian* Galois groups $G(L|K)$. For if Lx is the fixed field of the kernel of x and Xis the *Griij]cncharakter* associated with X : GU-x IK) ' + lhen the above remark shows that $L'.(LIK.x,s) = L'.(LxlK.x,s) =$ Hence $L'.(LIK.x.s)$ is holomorphic on all of C, because the �ame true for $L(X, s)$, as was shown in (R.5). This also scllles the Artin conjecture for every solvable extension LI K.

Our goal now is to prove a functional equation for Arlin L-serie1>. The basis for this will be lhe above theorem and the functional equation we have already e�tablished for Hecke L-series. We however have lo complete the Artin /.-series by the right "Euler factors" at the infinite places. In looking for these Euler factors, the first nalural guideline is provided by the ca1>e of Hecke L-series. But in order to go the whole way, we need an addilional Galois-theoretic complement which will be dealt with in the next section.

§11. The Arlin Conductor

The discriminant()= $Dr.iK$ of a Galois extension L IK of algebraic number fields admits a fine structure based on group theory. It is expressed by a product decomposition

$$) = \prod \mathfrak{f}(\chi)^{\chi(1)},$$

where X varies over the irreducible characters of the Galois group $G = C(LIK)$. The ideals $f(x)$ are given by

$$f(x) = \bigcap_{Pt">:.'} p/p(,()$$

with

$$f_{\mathfrak{p}}(\chi) = \sum_{i\geq 0} \frac{g_i}{g_0} \operatorname{codim} V^{G_i},$$

where V is a representation with character X. G_I is the i-th ramification group of L,i1IKμ, and R, denotes its order. This di<,covery goes back to HMIL i\Rn1v and HcLMUI HA,v The ideals $f(x)$ are called **Arlin conductors.** They play an important r61e in the functional equation of the Artin L-series, which we are going to prove in the next <,cction. Herc we collect the properties needed for thi�, following essentially the treatment given by *J.-P. SrRRt:* in! 1221.

First let u� consider a Galois extension $L|K$ of **local fields,** with Galois group G = *G(LIK).* Let f = *hiK* =IA: K] be the inertia degree of *LIK.* In chap. II*, I0, we defined, for any rr E *G,*

$$ir;(a) = vL(ax - x),$$

where x is an element such that *01.* = *oKlxl,* and l'L i� the normalized valuation of *L.* With thi� notation we can wrile the *i-th* ramification group as

$$G, =/a \quad EC \mid i(;(a) =::: i + 1 j$$

One has ic;(rar ¹) = *ir;(a),* and *iu(a)* = *iu(o)* for every subgroup *H* � *G.* If *LIK* is unramificd, then *iu(o)* = 0 for all *a* E G, *a* -=/=- I. We put

$$a_G(\sigma) = \begin{cases} -f i_G(\sigma) & \text{for } a\text{-=/=- } 1, \\ f \sum_{\tau \neq 1} i_G(\tau) & \text{fora} = 1. \end{cases}$$

*ar;*i� a central function on G, and we have

$$(a_G, 1_G) = \frac{1}{\#G} \sum_{\sigma \in G} a_G(\sigma) = 0$$

We may therefore write

$$ar; � "£fix)x. \quad /lx)EC.$$

with X varying over the irreducible characters of C. Our chief problem i� to prove that the coefficients $j(X)$ are rational =::: 0. Once we have 1,hown this. we may form the ideal fp(X) = which will be the p-component of the global A11in conductor that we want. First we prove that the function *ac* 1>atistie1> the follm\.-ing properties (we use the notation of the preceding 1,ection).

(11.1) Proposition. (i) *If* His a *norm1:d .�ubgroup oJ"G, then*

$$a_{G/H} = (a_G)_{H}.$$

(ii) Jf // is *any* subgroup ofG, *and* if *K' is the fixed* field *with* discriminant *i)K' K* = p''' *lhen*

$$a_G|H = vr_H + f_{K'|K} a_H$$

(iii) Let C, *be rhe 1-1h rnmification group* of C, *u, the ,wgmenlillion charncler* of G_1, *and (u,)� the character* of *G* induced from *u,. Then* one *ha1,*

$$ac = \sum_{,\hat{\ }1}^{I} \frac{1}{(Co: G_{\cdot})} (u, L.$$

Proof: (i) follows immediately from chap. II, (10.5).

(ii) Let $\sigma \in H$, $\sigma \neq 1$. Then

$$a_G(\sigma) = -f_{L|K}\, i_G(\sigma), \quad a_H(\sigma) = -f_{L|K'}\, i_H(\sigma), \quad r_H(\sigma) = 0.$$

Since $i_G(\sigma) = i_H(\sigma)$ and $f_{L|K} = f_{L|K'} f_{K'|K}$, this implies

$$a_G(\sigma) = \lambda r_H(\sigma) + f_{K'|K}\, a_H(\sigma).$$

Now let $\sigma = 1$, and let $\mathfrak{D}_{L|K}$ be the different of $L|K$. Let $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and $g(X)$ be the minimal polynomial of α over K. By chap. III, (2.4), $\mathfrak{D}_{L|K}$ is then generated by $g'(\alpha) = \prod_{\sigma \neq 1}(\alpha - \sigma\alpha)$. Consequently,

$$v_L(\mathfrak{D}_{L|K}) = v_L(g'(\alpha)) = \sum_{\sigma \neq 1} i_G(\sigma) = -\frac{1}{f_{L|K}}\, a_G(1).$$

By chap. III, (2.9), we know, on the other hand, that $\mathfrak{d}_{L|K} = N_{L|K}(\mathfrak{D}_{L|K})$, so $v_K \circ N_{L|K} = f_{L|K} v_L$ gives the identity

$$a_G(1) = f_{L|K}\, v_L(\mathfrak{D}_{L|K}) = v_K(\mathfrak{d}_{L|K}),$$

and in the same way $a_H(1) = v_{K'}(\mathfrak{d}_{L|K'})$. From chap. III, (2.10), we get furthermore that

$$\mathfrak{d}_{L|K} = \mathfrak{d}_{K'|K}^{[L:K']}\, N_{K'|K}(\mathfrak{d}_{L|K'}).$$

Thus $r_H(1) = [L:K']$ and $\lambda = v_K(\mathfrak{d}_{K'|K})$ yields the formula

$$a_G(1) = [L:K']\, v_K(\mathfrak{d}_{K'|K}) + f_{K'|K}\, v_{K'}(\mathfrak{d}_{L|K'}) = \lambda r_H(1) + f_{K'|K}\, a_H(1).$$

(iii) Let $g_i = \#G_i$, $g = \#G$. Since G_i is invariant in G, we have $(u_i)_*(\sigma) = 0$ if $\sigma \notin G_i$, and $(u_i)_*(\sigma) = -g/g_i = -f \cdot g_0/g_i$ if $\sigma \in G_i$, $\sigma \neq 1$, and $\sum_{\sigma \in G}(u_i)_*(\sigma) = 0$. For $\sigma \in G_k \smallsetminus G_{k+1}$, we thus find

$$a_G(\sigma) = -f(k+1) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)}\, (u_i)_*(\sigma).$$

This implies the identity for the case $\sigma = 1$ as well, since both sides are orthogonal to 1_G. □

For the coefficients $f(\chi)$ in the linear combination

$$a_G = \sum_\chi f(\chi)\chi,$$

we have, in view of $a_G(\sigma^{-1}) = \overline{a_G(\sigma)}$, that

$$f(\chi) = (a_G, \chi) = \frac{1}{g}\sum_{\sigma \in G} a_G(\sigma)\chi(\sigma^{-1}) = \frac{1}{g}\sum_{\sigma \in G} a_G(\sigma^{-1})\chi(\sigma) = (\chi, a_G),$$

$g = \#G$. For any central function φ of G, we put

$$f(\varphi) = (\varphi, a_G)$$

and

$$\varphi(G_i) = \frac{1}{g_i}\sum_{\sigma \in G_i} \varphi(\sigma), \quad g_i = \#G_i.$$

(11.2) Proposition. (i) *lfrp is* :1 *central* ftmctio11 *on the quotient group C /JI, and* rp' *i�* the *corresponding central function* 011 G, *then*

$$f(\varphi) = f(\varphi').$$

(ii) Jf rp *is* a *central function on* a . *�uhgroup II* of G, *and* rp. *is lhe central function* induced *by* rp on C, *then*

I(�,) � VK(OK'IK)�(I) + *Jic,K* f(�).

(iii) *For a central function* rp *on* G, *one has*

f(�J � I: "'(o(I) - �(G,)).
,c':0 go

Proof: (i) f(rp) = *(rp,ac;flt)* = (rp,(ac;)q) = (rp',ac) = f"(rp').
(ii) f(rp*) = *(rp.,ac;)* = *(rp,aulH)* = *v(rp.rH)* + *fK*:1*drp,a11)* = *vrp(I)* + *fK'IK f(rp)* with *V* = *v{((i.'JK'!K).*
(iii) We have = (rplG,, *u,)* = rp(l)-rp(G,), -.o the formula follows from (11.1), □

If *x* is the charncler of a representation *(p, V)* of C, then *x* (I) = dim *V* and x(G,) = dim vG,, hence

/(x) = *L*�codim *V(;,.*
1c::ll go

Now consider the function

rJL1d.1) = ! *h* (Go: G1),
D

which was introduced in chap. II, �**10.** For integers *m* 2: -1, it **i�·** given by I/L1K(-l) = -L IJL1d0) = 0, and

IJL1dm) = f,� *form* 2: I.
1=1 go

The theorem of *HAs.11:.-ARF* (sec chap. V, (6.3)) now gives ut-. the following integrality statement for the number *f* (X) in the case of a character *X* of degree I.

(11.3) Proposition. *Let be a character* of *G* of degree **1.** Let *j be* the *biggest* integer *such that* *-1-* *1(,'J* (w/Jen *x* = **I(,'** we *put j* = - I). *Then* we *lrnve*

/'(X) � *ryLIK(}*) +I,

:.md thi� i� a rational integer :=:: 0.

Proof: If $i \leq j$, then $\chi(G_i) = 0$, so that $\chi(1) - \chi(G_i) = 1$. If $i > j$, then $\chi(G_i) = 1$, and so $\chi(1) - \chi(G_i) = 0$. From (11.2), (iii), it thus follows that

$$f(\chi) = \sum_{i=0}^{j} \frac{g_i}{g_0} = \eta_{L|K}(j) + 1,$$

provided $j \geq 0$. If $j = -1$, we have $\chi(1) - \chi(G_i) = 0$ for all $i \geq 0$, and hence by (11.2), $f(\chi) = 0 = \eta_{L|K}(-1) + 1$.

Let H be the kernel of χ and L' the fixed field of H. By Herbrand's theorem (chap. II, (10.7)) one has

$$G_j(L|K)H/H = G_{j'}(L'|K) \quad \text{with} \quad j' = \eta_{L|L'}(j).$$

In terms of the upper numbering of the ramification groups, this translates into

$$G^t(L|K)H/H = G^t(L'|K),$$

where $t = \eta_{L|K}(j) = \eta_{L'|K}(\eta_{L|L'}(j)) = \eta_{L'|K}(j')$ (see chap. II, (10.8)). But $\chi(G_j(L|K)H/H) \neq 1$, and $\chi(G_{j+\varepsilon}(L|K)H/H) = \chi(G_{j+1}(L|K)H/H) = 1$ for all $\varepsilon > 0$, and in particular $G_j(L|K)H/H \neq G_{j+\varepsilon}(L|K)H/H$ for all $\varepsilon > 0$. Since $\eta_{L|K}(s)$ is continuous and strictly increasing, it follows that

$$G^t(L'|K) = G^t(L|K)H/H \neq G^{t+\delta}(L|K)H/H = G^{t+\delta}(L'|K)$$

for all $\delta > 0$, i.e., t is a *jump* in the ramification filtration of $L'|K$. The extension $L'|K$ is abelian and therefore $t = \eta_{L|K}(j)$ is an integer, by the theorem of HASSE-ARF. □

Now let χ be an arbitrary character of the Galois group $G = G(L|K)$. By Brauer's theorem (10.3), we then have

$$\chi = \sum n_i \chi_{i*}, \quad n_i \in \mathbb{Z},$$

where χ_{i*} is the character induced from a character χ_i of degree 1 of a subgroup H_i. By (11.2), (ii), we have

$$f(\chi) = \sum n_i f(\chi_{i*}) = \sum n_i \big(v_K(\mathfrak{d}_{K_i|K}) \chi_i(1) + f_{K_i|K} f(\chi_i) \big),$$

where K_i is the fixed field of H_i. Therefore $f(\chi)$ is a rational integer. On the other hand, (11.1), (iii) shows that $g_0 a_\chi$ is the character of a representation of G, so $g_0 f(\chi) = (\chi, g_0 a_\chi) \geq 0$. We have thus established the

(11.4) Theorem. *If χ is a character of the Galois group $G = G(L|K)$, then $f(\chi)$ is a rational integer ≥ 0.*

(11.5) Definition. *We define the (local)* **Artin conductor** of *the character x* ofG = G(LIK) lo *be the ideal*

fo(X) =p/(Jl_

In chap. V, (1.6), we defined the **conductor** of an *ahclian* exten<,ion *L* IK of local tield.., to he the smallest power of p, f = p", such that the 11-th higher unit group *utl* is contained in the norm group *NLIKL*.* The latter is the kernel of the norm residue :-ymhol

$$(\ ,L|K):K^*\longrightarrow G(L|K),$$

which map� v¼J to the higher ramification group *G'* (LIK) = *G₁(L* IK) with i = *1/f.'K<i)* - see Y. (6.2). The conductor f = p" is therefore given by the smallest integer *n* 2: 0 such that G"(LIK) =I.Prom (11.3) we thus ohtain the following remit.

(11.6) Proposition. *Let* LI *K be a Galois extension* of *local fields,* and *let x be* a *cluiracter* of *G* (*L* I*K)* of degree I. *Let L_I be the fixed field* of *the* kernel of *x, ;Jnd* f *the conductor* of *Lx* I*K. Then one has*

Proof: By (I 1.3), we have *f"(x)* = + I, where *j* i� the largest integer mch that G₁(LIK) *i_ G(LIlx)* =: Let *t* = *1/LiK (}).* Then one has

G'(L,IK) � *G'(LIK)H/H* �*G,(LIK)H/H.*

and G¹¹c(Lx1K) i; *G₁+₁(LIK)H/H* = **1** for all£> 0. Hence *r* i-; the largest number such that *C¹([,₁1K)* #-I.By the theorem *ofll11.11F-AR1•,* tis an integer, and we conclude that *f(x)* =*t* +I is the smallest integer >ouch tha1ct¹11(LxlK)= l.i.e.,f(x)=n. D

We now leave the local situation. and suppose 1hat *LIK* is a Galois extcmion of **global** fields. Let p be a prime ideal of *K,* \.PIP a prime ideal of *L* lying above 1-J. Let L,:plK₁₁ be the completion of *LIK,* and G,:p = G(L,:vlKp) the decomposition group of l1J over *K.* We denolc the function *ac,ll* on G'+J by a,:p, and extend it to *G* = G(I.IK) by zero. The central function

immediately tum5 out to be the function (a,:µ)* induced by a13IG,,p. It is therefore the character of a representation of C. If now *X* is a character of *G,* then we put

/(x.pl � (x.ap) � /(xIG,µ).

Then fr(X) = p/i,,: pl j._ the Artin conductor of the rc�triction of *X* to G,p = G(L:plKr)- In particular, we have fr(X) = I if pi� unramified. We define the (global) **Artin conductor** of *X* to he the product

fix)� TT fp(XJ-
P]�

Whenever preci�ion i:-. called for, we write *f(LIK.x)* in�tead of f(x). The propcrtie� (11.2) of the numbers *f(x,* p) transfer immediately to the Arlin conductor *f(x),* and we obtain the

(11.7) Proposition. (i) fix+ *x')* � f(xlf(x'), f(l) � (I).

(ii) *If l,'IK* i.\ ,1 *Galois subextemion* of *LIK, and x is a* charncter *o(* G(L'[K), *then*

f(LIK.x) � f(L'IK.x).

(iii) *If His a subgroup* ofG *with fixed field K'* and if *xis a character* of *H, then*

$$\mathfrak{f}(L|K,\chi_*) = \mathfrak{d}_{K'|K}^{\chi(1)} N_{K'|K}\big(\mathfrak{f}(L|K',\chi)\big)$$

Proof: (i) and (ii) are trivial. To prove (iii). we choose a fixed prime ideal \.ll of *L,* put

$$G = G(L|K),\quad H = G(L|K'),\quad G_{\mathfrak{P}} = G(L_{\mathfrak{P}}|K_{\mathfrak{p}}),$$

with p = llJ n *K.* and con\kler the decomposition

$$G = \bigcup G_{\mathfrak{P}}\tau H$$

into double coset�. Then representation theory yield� the following formula for the character *X* of *H:*

$$\chi_*|G_{\mathfrak{P}} = \sum_\tau \chi_*^\tau,$$

where *x'* i� the character *x'* **(a)**= **x(r-¹ar)** of G,:p nr //r-¹, and *x:* i'> the character of G13 induced by *X'* (see [119], chap. 7, prop. 22). Furthermore ll]� = \.ll' n *K'* are the different prime idcab of *K'* ahove p (see chap. **L** *9, p. .55). and we have

G-:µ, = r-1G,:pr = G(Lpr IKp). H,:µr = G,;pr n *H* = G(Lw IK�l�)-

Now !el il<;p' = p 11 'L-� be the discriminant ideal of K�. IK p, and let f''lJ' be the degree of;� over K. Thu� NK'IK('-13�) = pf,v,. Sin�c '

fp(LIK, X*) = pf(x,IG,lll and t'lJ;(LIK', x) = -,p'!(xlH-i_.,i,

we have lo show that

/(x,IG,,) �� v,,,;x(IJ + h,; /(xlH'lJ,),

or, in view of (11.2), (ii), that

$$f(\chi_*|G_{\mathfrak{P}}) = \sum f((\chi|H_{\mathfrak{P}^\tau})_*).$$

Bul H-+Jr = r ¹(G<;pn rHr-¹)r, and xiii<,μ,, resp.$(\chi|H_{\mathfrak{P}^\tau})_*$, arises by conjugation a � ra r-¹ from xr, resp. x:. Therefore $f((\chi|H_{\mathfrak{P}^\tau})_*) =$ l(x;), and(**) follows from(*). □

We apply (iii) to the case X = lH, and denote the induced character X* by sc;H• Since t(x) =I.we obtain the

(ll.8) Corollary. i)K'IK = t(LIK, �·u;fl).

If in particular H = I I}, then sc;;11 is the character re; of the regular represenlation. Its decomposition into irreducible characters X is given by

cc; � LX(l)x.
l

Thbyields the

(11.9) Conductor-Discriminant-Formula. *For an arhitra,y* Galois *extension* LI K of *global fields,* one *has*

i)LIK = nf(X)x(I)•
l

where X varies over *the irreducible* characters ofG(LIK).

For an *ahelian* extension LI K of global field�, we defined the conductor tin VI. (6.4). By chap. VI, (6.5), it is the product

1�n1,
p

of the conductors fp of the local exten�ion:-. L.plKμ. (I 1.6) now gives rise to the following

(11.10) Proposition. *Let $L|K$ be a Galois extension of global fields, χ a character of $G(L|K)$ of degree 1, L_χ the fixed field of the kernel of χ, and $\mathfrak{f}$ the conductor of $L_\chi|K$. Then one has*

$$\mathfrak{f} = \mathfrak{f}(\chi).$$

Now let $L|K$ be a Galois extension of algebraic number fields. We form the ideal

$$\mathfrak{c}(L|K,\chi) = \mathfrak{d}_K^{\chi(1)} N_{K|\mathbb{Q}}(\mathfrak{f}(L|K,\chi))$$

of $\mathbb{Z}$. The positive generator of this ideal is the integer

$$c(L|K,\chi) = |d_K|^{\chi(1)}\mathfrak{N}(\mathfrak{f}(L|K,\chi)).$$

Applying (11.7) and observing the transitivity of the discriminant (chap. III, (2.10)), we get the

(11.11) Proposition. (i) $c(L|K,\chi+\chi') = c(L|K,\chi)c(L|K,\chi')$, $c(L|K,1) = |d_K|$,

(ii) $c(L|K,\chi) = c(L'|K,\chi)$,

(iii) $c(L|K,\chi_*) = c(L|K',\chi)$.

Here the notation is that of (11.7).

§ 12. The Functional Equation of Artin L-series

The first task is to complete the Artin L-series

$$\mathcal{L}(L|K,\chi,s) = \prod_{\mathfrak{p}\nmid\infty} \frac{1}{\det(1-\varphi_{\mathfrak{P}}\mathfrak{N}(\mathfrak{p})^{-s};V^{I_{\mathfrak{P}}})}$$

for the character χ of $G = G(L|K)$, by the appropriate gamma factors. For every infinite place $\mathfrak{p}$ of K we put

$$\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s) = \begin{cases} L_{\mathbb{C}}(s)^{\chi(1)} & \text{if } \mathfrak{p} \text{ is complex},\\ L_{\mathbb{R}}(s)^{n_+}L_{\mathbb{R}}(s+1)^{n_-} & \text{if } \mathfrak{p} \text{ is real},\end{cases}$$

with the exponents $n_+ = \frac{\chi(1)+\chi(\varphi_{\mathfrak{P}})}{2}$, $n_- = \frac{\chi(1)-\chi(\varphi_{\mathfrak{P}})}{2}$. Here $\varphi_{\mathfrak{P}}$ is the distinguished generator of $G(L_{\mathfrak{P}}|K_{\mathfrak{p}})$, and

$$L_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \quad L_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$$

(see §4). For $\mathfrak{p}$ real, the exponents n_+, n_- in $\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s)$ have the following meaning.

The involution tpq:; on V induces an eigen-;pace decomposition V = V-'-- EB V-, where

$$v+ � \{x \in V \,|\, ��x � , \backslash, \quad v- � \{ , \in V| �\cdot ax� -x \backslash .$$

and it follow1> from the remark in S 10, p.521, that

dimV' ��(x(ll+x(�•oJ), dimv-��(xilJ-x(�,,,J)

The functions *Lp(L* IK, *X,s)* exhibit the same behaviour under change of fields and character1, as the L-serie1, and the Artin conductor.

(12.l) Proposition. (i) .Cp(L IK, $X + X'$,s) = *.Cµ(L* IK, *X*,.\).Cp(L IK, *X* ,_1).

(ii) *lfL'IK isaGaloi.�1,ubextensionofLIK andx aclwr.:ic1crof"G(/,* IK). *then*

L,(LIK.x ..,) � Cp(L'IK.x ..,).

(iii) *IfK' i1,an* intermediate *fieldofLIK :md x acharacterofG(LIK'), then*

C,(LIK, *x,..,)* � [1Cq(LIK', *X,* ,).
q,P

where q *varie1>* over *1he place,;* of *K' lying* above p.

Proof: (i) i1> trivial.

(ii) If i;plq:.J'lp arc place-; of *L* 2 *L'* 2 *K,* each lying above the next. then 'P'll is mapped under the projection *G(LIK)* ---+ G(L'IK) to <P'll'· So = x('f1-r).

(iii) Ifp complex, then there are precisely *m* = *\K':* KIplace� q above p. They are abo complex, and the claim follows from xAIJ = mx(l).

Suppo-;e pi� real. Let *G* = *G(LIK), II=* G(LIK'), and let *H\GJG,"11* be the set of double cosets HrG,"+3 with a fixed place i;p of *L* above p. Then v...c have a bijection

H\G/Gii--+ {q place of *K'* above p), HrGq.1 ,----:,. q, = ri;pJK,

(sec chap. I, §9, p.55). q, is real if and only if 'Pr"'.+J = *T<iJ,".+JT* I E *H,* i.e., = rGq:;r-1 <; *II.* The latter inclusion holds if and only if the double 1/rG,J,J comists of only one co1>et mod H:

HrGw, = (HrGri.ir -I)r =Hr.

We thus obtain the real places among the q, by letting r run through a system of representatives of the cosets 1/r of 1/\G such that Ttpq:;r-1 EH. But, for .'>uch a :-.yqem. one ha1i

x*(tp,p) = Lx(rtp1-ir-1) = Lx('Pr'll).

Putting $\mathfrak{Q} = \mathfrak{P}|L$, makes $\mathfrak{q} = \mathfrak{Q}|K'$ run through the real places of K' above $\mathfrak{p}$, i.e.,

$$\chi_*(\varphi_{\mathfrak{P}}) = \sum_{\substack{\mathfrak{q}|\mathfrak{p} \\ \mathfrak{q} \text{ real}}} \chi(\varphi_{\mathfrak{Q}}).$$

On the other hand we have

$$\chi_*(1) = \sum_{\mathfrak{q} \text{ complex}} 2\chi(1) + \sum_{\mathfrak{q} \text{ real}} \chi(1).$$

Legendre's duplication formula $L_{\mathbb{R}}(s)L_{\mathbb{R}}(s+1) = L_{\mathbb{C}}(s)$ (see (4.3)) turns this into

$$\begin{aligned} L_{\mathfrak{p}}(L|K,\chi_*,s) &= \prod_{\mathfrak{q} \text{ compl}} L_{\mathbb{C}}(s)^{\chi(1)} \prod_{\mathfrak{q} \text{ real}} L_{\mathbb{R}}(s)^{\frac{\chi(1)+\chi(\varphi_{\mathfrak{Q}})}{2}} \prod_{\mathfrak{q} \text{ real}} L_{\mathbb{R}}(s+1)^{\frac{\chi(1)-\chi(\varphi_{\mathfrak{Q}})}{2}} = \\ &= \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}(L|K',\chi,s). \end{aligned}$$ □

We finally put

$$L_\infty(L|K,\chi,s) = \prod_{\mathfrak{p}|\infty} L_{\mathfrak{p}}(L|K,\chi,s),$$

and obtain immediately from the above proposition the equations

$$\begin{aligned} L_\infty(L|K,\chi+\chi',s) &= L_\infty(L|K,\chi,s)\,L_\infty(L|K,\chi',s), \\ L_\infty(L|K,\chi,s) &= L_\infty(L'|K,\chi,s), \\ L_\infty(L|K,\chi_*,s) &= L_\infty(L|K',\chi,s). \end{aligned}$$

(12.2) **Definition.** *The* **completed Artin** *L-series for the character χ of $G(L|K)$ is defined to be*

$$\Lambda(L|K,\chi,s) = c(L|K,\chi)^{s/2} L_\infty(L|K,\chi,s)\,L(L|K,\chi,s),$$

where

$$c(L|K,\chi) = |d_K|^{\chi(1)}\,\mathfrak{N}\big(\mathfrak{f}(L|K,\chi)\big).$$

The behaviour of the factors $c(L|K,\chi)$, $L_\infty(L|K,\chi,s)$, $L(L|K,\chi,s)$ on the right-hand side, which we studied in (10.4), (11.11), and above, carries over to the function $\Lambda(L|K,\chi,s)$, i.e., we have the

(12.3) Proposition. (i) $\Lambda(L|K,\chi+\chi',s) = \Lambda(L|K,\chi,s)\Lambda(L|K,\chi',s)$.

(ii) *If $L'|K$ is a Galois subextension of $L|K$ and χ a character of $G(L'|K)$, then*

$$\Lambda(L|K,\chi,s) = \Lambda(L'|K,\chi,s).$$

(iii) *If K' is an intermediate field of $L|K$ and χ a character of $G(L|K')$, then*

$$\Lambda(L|K,\chi_*,s) = \Lambda(L|K',\chi,s).$$

For a character χ of degree 1, the completed Artin L-series $\Lambda(L|K,\chi,s)$ coincides with a completed Hecke L-series. To see this, let $L_\chi|K$ be the fixed field of the kernel of χ, and let $\mathfrak f = \prod_{\mathfrak p} \mathfrak p^{n_\mathfrak p}$ be the conductor of $L_\chi|K$. By (11.10), we then have

$$\mathfrak f = \mathfrak f(\chi).$$

Via the Artin symbol

$$J^{\mathfrak f}/P^{\mathfrak f} \longrightarrow G(L_\chi|K), \qquad \mathfrak a \longmapsto \left(\frac{L_\chi|K}{\mathfrak a}\right),$$

χ becomes a Dirichlet character of conductor $\mathfrak f$, i.e., by (6.9), a primitive *Größencharakter* mod $\mathfrak f$ with exponent $p = \prod_\tau p_\tau$ so that $p_\tau = 0$ if τ is complex. This Größencharakter will be denoted $\tilde\chi$.

We put $p_\mathfrak p = p_\tau$ if $\mathfrak p$ is the place corresponding to the embedding $\tau : K \to \mathbb C$. The numbers $p_\mathfrak p$ have the following Galois-theoretical meaning.

(12.4) Lemma. *For every real place $\mathfrak p$ of K one has*

$$p_\mathfrak p = [L_{\chi\mathfrak P} : K_\mathfrak p] - 1.$$

Proof: We consider the isomorphism

$$I/I^{\mathfrak f}K^* \xrightarrow{\ \sim\ } J^{\mathfrak f}/P^{\mathfrak f},$$

where $I^{\mathfrak f} = \prod_\mathfrak p U_\mathfrak p^{(n_\mathfrak p)}$ is the congruence subgroup mod $\mathfrak f$ of the idele group $I = \prod K_\mathfrak p^*$ (see chap. VI, (1.9)), and consider the composite map

$$I/I^{\mathfrak f}K^* \longrightarrow J^{\mathfrak f}/P^{\mathfrak f} \longrightarrow G(L_\chi|K) \xrightarrow{\ \chi\ } \mathbb C^*.$$

Let $\mathfrak p$ be a real place of K, and let $a \in I$ be the idele with components $a_\mathfrak p = -1$ and $a_\mathfrak q = 1$ for all places $\mathfrak q$ different from $\mathfrak p$. By chap. VI, (5.6), the image $\tilde a_\mathfrak p = (a, L_\chi|K) = (-1, L_{\chi\mathfrak P}|K_\mathfrak p)$ in $G(L_\chi|K)$ is a generator of the decomposition group Gp= *G(LxidKp)-* By Lhe approximation theorem, we may choose an *a* EK* rnch that *a*= I mod f, *a*< 0 in *Kp,* and *a*> 0 in *K* q, for all real places q *-1-* p. Then

$$fi = \text{r.rn E } JO) = \{XE" \cdot \text{'PE } ui"p) \text{ for Plfxi}). \quad \text{if } f = \text{np p"P.}$$

Ai, explained in the proof of chap. VI, (1.9), the image of *a* mod *nK•* in *Jljp!* is the clas� of (/J) = *(a),* which therefore maps to 'P'-J.l· Consequently,

$$x((a)) = x1(a)x\text{-}x,(a) = \text{x(t/-h.p)}.$$

Since *a*= I mod f, we have Xr(a) = I and *x..,_,(a)* = N((�}") = (�:P)P" = (-1)1'1>, i.e., x(<p<:p) = (-I)"P, so that *'P'-J.l* = I for /Jp = 0, ,1 and (f-l<p *-f.* I for /Jp = I. But this b the i,tatement of the lemma. D

(12.5) **Proposition.** *The completed Artin 1.-scrie.\ for the characier x* of *degree I and the completed Hecke L-series for the Grij_/iewharakre, X coincide:*

$$A(LIK,x,,<J \text{ � } A(x,,,),$$

Proof: The completed Hecke L-series is given, according to §8, by

$$A(x,,,) \text{ � } (\text{ldKl91(f(x)J)}'^{12}L\%(x,,)L(x,,,)$$

with

$$L,)X,s) = Lx(s).$$

ands= sl + *p,* where

$$Lx(s) = \prod_{,,}\text{�} Lp(Sp)$$

is the L-function of the G(Clil{)-i,ct *X* = Hom(K,C) defined in §4. The factors Lp(sp) are given explicitly by

$$\text{(*)} \qquad Lp(Sp) = [\; \begin{matrix} Lc(s), & \text{if p complex,} \\ l."J,.(S+ \; pp), & \text{ifp real,} \end{matrix}$$

(i,ee p.454). On lhe other hand we have

$$A(LIK, X,,,,) \text{ � } c(LIK, x)'^{12}C\text{�}(LIK, X, ,)C(LIK, X, <)$$

with

$$c(L|K,\chi) = |d_K|\mathfrak{N}\big(\mathfrak{f}(L|K,\chi)\big)$$

and

$$C,\%(LIK,x,<I\text{�} \prod_{Pl\text{�}} C,(LIK,x,,J,$$

Let *Lx* be the fixed field of the kernel of *x*. By (I I. 11). (ii), and the remark preceding lemma (12.4). one has

,(LIK, *x)* � *c(L,* IK, xl � *ldK* l'll(f(x))'

and by (10.4), (ii), and (10.6), and the subse4uent remark, one ha�

L(LIK, X..<J � C(L, IK, *X,,,)* � *LC/ ..n.*

We arc thu� reduced to proving

L'.p(LIK' *X.* �) = Lµ(Sp)

for Ploo ands= .11 + *p.* Firstly. we have L'.p(LIK, *x,s)* = *L'.11(Lx* IK. *x,s)* (�cc p. 537). Let <P<p he the generator of G(Lx,:plK$_{11}$). Since *X* is injective on *G(Lx* IK), we get x(<P,v) = -1 if <P'll *i*- I. and x(rp,:p) = I if <P'-P = I. Using (12.4) this gives

L'.$_{11}$(Lx1K,x,s)= Le(�). for p complex,
LJR(,1), forprealandl.'preal,i.e.,p$_{11}$=0,
L.k(s + I). for p real and l.'p complex. i.e.. f)p = I .

Hence (*) shows that indeed L'.$_{11}$(L IK, *x.* j) = Lp(Sp)- LJ

In view of the two results (12.3) and (12.5), the functional equation for A11in L-series now follow� from Brauer\ theorem (10.3) in a purely formal fa�hion, a� a com,cqucncc of the functional equation for Hecke L-�eries, which we have already established.

(12.6) Theorem. *Tile* Artin *L-series A(LIK,x,1)* admit,; a meromorp/Jic *co11ti11u:1tio11* to C ,md .�alis/ie� */he functional* equation

$$\Lambda(L|K,\chi,s) = W(\chi)\Lambda(L|K,\overline{\chi},1-s)$$

with a comtant W(x) ofab.mlute value *1.*

Proof: By Brauer·s theorem. the character *xi*� an integral linemcumbina1ion

x=Ln,xn,

where the *X,** arc induced from characters xi of degree I on subgroup� *H$_1$ = GU,IK,).* From propositions (12.3) and (12.5), it follow� that

A(LIK.x. '1�$\prod$ *A(LIK,x,,.* ,)"'

$$= \prod_i \Lambda(L|K_i,\chi_i,s)^{n_i}$$

$$= \prod \Lambda(\widetilde{\chi}_i,s)^{n_i}\,.$$

where 7, is the *Crfdlem hara/.:ter* of K_1 as!-.ociated to X,. By (8.6), the Hecke L-series A(;(1.. 1) admit meromorphic continuation1-, to C and 1-,atisfy the functional equation

$$\Lambda(\widetilde{\chi}_i, s) = W(\widetilde{\chi}_i)\Lambda(\overline{\widetilde{\chi}}_i, 1-s).$$

Therefore _;\(L IK, X,s) satistie!-. the functional equation

A(LIK, x. ,) � W(x) TT *ACx,.* I - ,) � *W(x)A(LIK. X,* I - .,) .

where *W(x)* = n, *W(X1)* **i"** of absolute value J.

The functional e4uation for the Artin L-series may be given the following explicit form, which i1-, easily deduced from (12.6) and (4.3):

$$\mathcal{L}(L|K,\chi,1-s) = A(\chi,s)\mathcal{L}(L|K,\overline{\chi},s),$$

with the factor

Alx ..,) � W(xl[ldKl""l'llf(LIK.xJJ]' *!*

x (COSJr1/2)"+(sin;rs/2)[11] n,(.1)"y(I)

and the exponents

$$n^+ = \frac{n}{2}\chi(1) + \sum_{\mathfrak{p}} \frac{1}{2}\chi(\varphi_{\mathfrak{P}}), \quad n = \frac{n}{2}\chi(1) - \sum_{\mathfrak{p}} \frac{1}{2}\chi(\varphi_{\mathfrak{P}}).$$

Here the summations arc over the real place5 p of *K.* This gives immediately the zeroe� of the function *L(LIK ,x,s)* in the half-plane Re(.1) -S 0. If *xi!-.* not the principal character, they arc the following:

ats = 0. - 2. -4. . .t:eroes of order �x(I) + *L* prec1I

at *s* = -1, - 3, -5, .. zoe!-. of order �x(l) - *L* p·�-11

Remark: For the proof of the functional equation of the completed Arlin L-serie5, we have made essential use of 1he fact that "Euler factors" *Lp(L* I *K, X,*s) at the infinite place� p, which are made up out of gamma function�. behave under change of fields and character� in exactly the ..,ame way as the Euler factors

$$\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s) = \det(1-\varphi_{\mathfrak{P}}\mathfrak{N}(\mathfrak{P})^{-s};V^{I_{\mathfrak{P}}})^{-1}$$

at the finite places. This uniform behaviour is in striking contrast to the great difference in the procedures that lead to the definitions of the Euler factors for and $\mathfrak{p} \mid \infty$. It is in this context that the mathematician C11rmTOPHU1 recently made a very interesting discovery (see [26], [27]). He shows that the Euler factors for all places $\mathfrak{p}$ can all be written in the same way:

$$\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s) = \det{}_{\infty}\Big(\frac{\log \mathfrak{N}(\mathfrak{p})}{2\pi i}(s\,\mathrm{id} - \Theta_{\mathfrak{p}});\ H(X_{\mathfrak{p}}/\mathbb{L}_{\mathfrak{p}})\Big)^{-1}.$$

Here $H(X_{\mathfrak{p}}/\mathbb{L}_{\mathfrak{p}})$ is an *infinite dimensional* $\mathbb{C}$-vector space which can be canonically constructed, $\Theta_{\mathfrak{p}}$ is a certain linear "Frobenius" operator on it, and $\det_{\infty}$ is a "regularized determinant" which generalizes the ordinary notion of determinant for finite dimensional vector spaces to the infinite dimensional case. The theory based on this observation is of the utmost generality, and reaches far beyond Artin L-series. It suggests a complete analogy for the theory of L-series of algebraic varieties over finite fields. The striking success which the geometric interpretation and treatment of the L-series has enjoyed in this analogous situation adds to the relevance of DE11'f,\•GER\ theory for present-day research.

§ 13. Density Theorems

Dirichlet's prime number theorem (5.14) says that in every *arithmetic progression*

$$a,\ a\pm m,\ a\pm 2m,\ a\pm 3m, \dots$$

$a, m \in \mathbb{N}$, $(a,m) = 1$, there occur infinitely many prime numbers. Using L-series, we will now deduce a far-reaching generalization and sharpening of this theorem.

(13.1) Definition. *Let M be a set of prime ideals of K. The limit*

$$d(M) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{p} \in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s}},$$

provided it exists, is called the Dirichlet density *of M.*

From the product expansion

$$\zeta_K(s) = \prod_{\mathfrak p} \frac{1}{1-\mathfrak N(\mathfrak p)^{-s}}, \quad \mathrm{Re}(s) > 1,$$

we obtain as in § 8, p. 494,

$$\log \zeta_K(s) = \sum_{\mathfrak p, m} \frac{1}{m\,\mathfrak N(\mathfrak p)^{ms}} = \sum_{\mathfrak p} \frac{1}{\mathfrak N(\mathfrak p)^{s}} + \sum_{\mathfrak p, m \ge 2} \frac{1}{m\,\mathfrak N(\mathfrak p)^{ms}}.$$

The latter sum obviously defines an analytic function at $s = 1$. We write $f(s) \sim g(s)$ if $f(s) - g(s)$ is an analytic function at $s = 1$. Then we have

$$\log \zeta_K(s) \sim \sum_{\mathfrak p} \frac{1}{\mathfrak N(\mathfrak p)^{s}} \sim \sum_{\deg(\mathfrak p) = 1} \frac{1}{\mathfrak N(\mathfrak p)^{s}},$$

because the sum $\sum_{\deg(\mathfrak p) \ge 2} \mathfrak N(\mathfrak p)^{-s}$ taken over **all** $\mathfrak p$ of degree ≥ 2 is analytic at $s = 1$. Furthermore, by (5.11), (ii), we have $\zeta_K(s) \sim \frac{1}{s-1}$, and so

$$\sum_{\mathfrak p} \frac{1}{\mathfrak N(\mathfrak p)^{s}} \sim \log \frac{1}{s-1}.$$

So we may also write the Dirichlet density as

$$d(M) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak p \in M} \mathfrak N(\mathfrak p)^{-s}}{\log \frac{1}{s-1}}.$$

Since the sum $\sum \mathfrak N(\mathfrak p)^{-s}$ over all prime ideals of degree > 1 converges, the definition of Dirichlet density only depends on the prime ideals of degree 1 in M. Adding or omitting finitely many prime ideals also does not change anything as far as existence or value of the Dirichlet density is concerned. One frequently also considers the **natural density**

$$\delta(M) = \lim_{x \to \infty} \frac{\#\{\mathfrak p \in M \mid \mathfrak N(\mathfrak p) \le x\}}{\#\{\mathfrak p \mid \mathfrak N(\mathfrak p) \le x\}}.$$

It is not difficult to show that the existence of $\delta(M)$ implies the existence of $d(M)$, and that one has $\delta(M) = d(M)$. The converse is not always true (see [123], p. 26). In the notation of chap. VI, §1 and §7, we prove the generalized **Dirichlet density theorem.**

(13.2) Theorem. *Let* $\mathfrak m$ *be a module of* K *and* $H^{\mathfrak m}$ *an ideal group such that* $J^{\mathfrak m} \supseteq H^{\mathfrak m} \supseteq P^{\mathfrak m}$ *with index* $h^{\mathfrak m} = (J^{\mathfrak m} : H^{\mathfrak m})$.

For every class $\mathfrak K \in J^{\mathfrak m}/H^{\mathfrak m}$*, the set* $P(\mathfrak K)$ *of prime ideals in* $\mathfrak K$ *has density*

$$d(P(\mathfrak K)) = \frac{1}{h^{\mathfrak m}}.$$

For the proof we need the following

(13.3) Lemma. *Let* X *be* a *nontrivial* (irredU1.:iblc) *character* of J^{111}/ *pm* (i.e., *a* character of degree /). *Then the* Hecke *L-scrics*

$$\mathbf{L(x,.,)} \quad Q \; 1- \frac{\mathrm{I}}{x(p)91(pJ-\bullet}$$

(x (p) = 0 for plm) *s<1li fics*

Proof: By (8.5) and the remark following (5.10) (in the ca e m = I), *L(x,)* doe-; not have a pole al s = I. Let *LIK* be the ray clas<s field mod m. 1,0 *G(LIK)* r^{1}/P^{111}. Interpreting x as a character of the Galois group G(LIK), the function *L(x,s)* agree.1, with the Artin L-series *L([,IK,x,s)* up to finitely many Euler factors - ee (10.6). Like *L(x,s)*, this Artin L-serie doe not have a pole at ., = 1. So all we have to show is thal L(LIK, *X*, I) *-1-* 0. According to (10.5), we have

$$(L(,l)=(K(s) \; \bigcap_{Jr'} \; L\{LIK,x,.1Y(lJ\_$$

where X rum through the nontrivial irreducible character.'. of G(LIK). By (5.11), both *(K(s)* and *(L(s)* have .1,imple poles at s = I, i.e., the product i.1, nonzero at s = I, Since none of the factors ha.1, a pole, we tinuL(LIK,x.1)#0. lJ

Proof of (13.2): Exactly as for the Dedekind Leta function above, we obtain for the Dirichlet /.-series

$$\log L(x..,)\sim \mathrm{I:}_{p} \frac{}{91(pJ'} \qquad \chi(\mathfrak{K}') \sum_{\mathfrak{p}\in\mathfrak{K}'} \frac{1}{\mathfrak{N}(\mathfrak{p})^s}.$$

Multiplying this by x(- -^{1}) and wmming over all (irreducible) X yields

$$\log(KC.'1+ \sum_{x7''1} x(Jl-')\log L(x..,) \sim \quad ') \; \mathrm{I:}_{pec\bullet l.'} \frac{\_I}{IJ1(p)'}$$

Since *L(x,* 1) *-1-* 0, logL(x--1) is analytic at s =I.But

$$L_{1} \; x\,(Jt'Jl'\,') \quad \begin{cases} 0, & \text{ifJl'} \# - ' \\ \text{hm}, & \text{if .it'} = \text{fl.} \end{cases}$$

Hence \\--e get

$$\log \frac{\_I\_}{s-1} \sim \log(K(s) \sim \mathrm{hm} \; L_{pec IJ1(p)'} \; I\_,$$

and the theorem i.1, proved. □

The theorem shows in particular that the density of the prime ideals in a class of $J^{\mathfrak m}/H^{\mathfrak m}$ is the same for every class, i.e., the prime ideals are **equidistributed** among the classes. In the case $K = \mathbb{Q}$, $\mathfrak m = (m)$, and $H^{\mathfrak m} = P^{\mathfrak m}$, we have $J^{\mathfrak m}/P^{\mathfrak m} \cong (\mathbb{Z}/m\mathbb{Z})^*$ (see chap. VI, (1.10)), and we recover the classical Dirichlet prime number theorem recalled at the beginning, in the stronger form which says that the prime numbers in an arithmetic: i.e., in a class a mod m, $(a,m) = 1$, have density $\varphi(m) =$

Relating the prime ideals $\mathfrak p$ of a class of $J^{\mathfrak m}/P^{\mathfrak m}$, via the class field theory isomorphism $J^{\mathfrak m}/P^{\mathfrak m} \cong G(L|K)$, to the Frobenius automorphisms $\varphi_{\mathfrak p} = \left(\frac{L|K}{\mathfrak p}\right)$, gives us a Galois-theoretic interpretation of the Dirichlet density theorem. We now deduce a more general density theorem which is particularly important in that it concerns arbitrary Galois extensions (not necessarily abelian). For every $\sigma \in G(L|K)$, let us consider the set

of all unramified prime ideals $\mathfrak p$ of K such that there exists a prime ideal $\mathfrak P$ of L satisfying

$$\sigma = \left(\frac{L|K}{\mathfrak P}\right),$$

where $\left(\frac{L|K}{\mathfrak P}\right)$ is the Frobenius automorphism $\varphi_{\mathfrak P}$ of $\mathfrak P$ over K. It is clear that this set depends only on the conjugacy class

$$\langle\sigma\rangle = \{\tau\sigma\tau^{-1} \mid \tau \in G(L|K)\}$$

of σ and that one has $P_{L|K}(\sigma) \cap P_{L|K}(\tau) = \emptyset$ if $\langle\sigma\rangle \neq \langle\tau\rangle$. What is the density of the set $P_{L|K}(\sigma)$? The answer to this question is given by the **Cebotarev density theorem.**

(13.4) Theorem. Let $L|K$ *be a Galois extension with group* G. *Then* for every $\sigma \in G$, *the set* $P_{L|K}(\sigma)$ *has a density, and it is given by*

$$d(P_{L|K}(\sigma)) = \frac{\#\langle\sigma\rangle}{\#G}.$$

Proof: We first assume that G is generated by σ. Let $\mathfrak m$ be the conductor of $L|K$. Then $L|K$ is the class field of an ideal group $H^{\mathfrak m}$, $J^{\mathfrak m} \supseteq H^{\mathfrak m} \supseteq P^{\mathfrak m}$. Let $\mathfrak K \in J^{\mathfrak m}/H^{\mathfrak m}$ be the class corresponding to the element σ under the isomorphism

$$J^{\mathfrak m}/H^{\mathfrak m} \xrightarrow{\sim} G, \quad \mathfrak p \longmapsto \left(\frac{L|K}{\mathfrak p}\right).$$

Then *PL1K(u)* consists precisely of the prime ideals p which lie in the class .it. By the Dirichlet dem,ity theorem (13.2), we conclude that *P1.w(a)* has density

d(PL1drr)) = I/hm = I/#G = #(a)/#G•

In the general case, let *E* he the fixed field of *a*. If *.f* is the order of *a*, then, as we just saw, d(P11r(a)) = f- Let *P(a)* be the set of prime ideals 13 of *L* wch that 131P E *Pt* K(a) and (�) =a.Then *P(a)* corresponds bijectively to the set P{1r(a) of thO'-C prime ideals q in *PL1r(a)* �uch that Eq = Kp, qlp. Since the remaining prime ideals in PL1r(rr) are either ramified or have degree > I over Q, we may omit them and obtain

d(PL' 1r(a)) = d(PL1r(a)) = yl ·

Now we consider the surjective map

P: P;.IL(a)-----;, *PL1K(a).* qi---+ q n *K*

As *P{1r(a)* � P(u), we get, for every p E *P1.1K(a),*

p-1(p) "/'|| E P(rr)I 'JIlp} "Z(rr)/(a).

where Z(a) = {r E GI ra = ar) is the ccntra[i7er of *a.* So we get

d(PL Kia)) � I/(Z(rr)' (a)), *d(P,* 1c:(a)) � j/#Z(a) *f* � I#(a)/#G. □

The Cebotarev density theorem has quite a number of surprising consequence�, which we will now deduce, If *S* and *T* are ,my two "cts of primes, then let us write

Sr:;T

to indicate that *S* is contained in *T* up to tinitely many exceptional elements. Furthermore, let us write S = *T* if *Sr:;_ r* and *Tr:;_ S,*

Let LI *K* be a finite extension of algebraic number fields. We denote by *P(LIK)* the set of all unramified prime ideals p of *K* which admit in La prime divisor 13 of degree I over *K.* So. if *LIK* i5 Galois, then *P(LIK)* i» just the �et of all prime ideals of *K* which 5plit completely in *L.*

(13.5) Lemma. Let *NIK be* a Galois *extension conwining L.* ;.md let *G* = G(NIK), *H* = G(NIL). *Then one has*

P(LIK)= PN1K(a) (di8jointunion).

Proof: A prime ideal $\mathfrak{p}$ of K which is unramified in N lies in $P(L|K)$ if and only if the conjugacy class $\langle\sigma\rangle$ of $\sigma = \left(\frac{N|K}{\mathfrak{P}}\right)$, for some prime ideal $\mathfrak{P}|\mathfrak{p}$ of N, contains an element of H, i.e., if and only if $\mathfrak{p} \in P_{N|K}(\sigma)$ for some $\sigma \in G$ such that $\langle\sigma\rangle \cap H \neq \emptyset$. □

(13.6) Corollary. *If $L|K$ is an extension of degree n, then the set $P(L|K)$ has density $d(P(L|K)) \geq \frac{1}{n}$. Furthermore, one has*

$$d(P(L|K)) = \frac{1}{n} \iff L|K \text{ is Galois.}$$

Proof: Let $N|K$ be a Galois extension containing L, and let $G = G(N|K)$ and $H = G(N|L)$. By (13.5), we have

$$P(L|K) \doteq \bigcup_{\langle\sigma\rangle \cap H \neq \emptyset} P_{N|K}(\sigma).$$

The Čebotarev density theorem (13.4) then yields

$$d(P(L|K)) = \sum_{\langle\sigma\rangle \cap H \neq \emptyset} \frac{\#\langle\sigma\rangle}{\#G} = \frac{1}{\#G}\,\#\Big(\bigcup_{\langle\sigma\rangle \cap H \neq \emptyset} \langle\sigma\rangle\Big).$$

Since $H \subseteq \bigcup_{\langle\sigma\rangle \cap H \neq \emptyset} \langle\sigma\rangle$, it follows that

$$d(P(L|K)) \geq \frac{\#H}{\#G} = \frac{1}{n}.$$

$L|K$ is Galois if and only if H is a normal subgroup of G, and this is the case if and only if $\langle\sigma\rangle \subseteq H$ whenever $\langle\sigma\rangle \cap H \neq \emptyset$, and so this holds if and only if $H = \bigcup_{\langle\sigma\rangle \cap H \neq \emptyset} \langle\sigma\rangle$. This implies the second claim. □

(13.7) Corollary. *If almost all prime ideals split completely in the finite extension $L|K$, then $L = K$.*

Proof: Let $N|K$ be the normal closure of $L|K$, i.e., the smallest Galois extension containing L. A prime ideal $\mathfrak{p}$ of K splits completely in L if and only if it splits completely in $N|K$ (see chap. I, §9, exercise 4). Under the hypothesis of the corollary, we therefore have

$$1 = d(P(L|K)) = d(P(N|K)) = \frac{1}{[N:K]},$$

so that $[N:K] = 1$ and $N = L = K$. □

(13.8) Corollary. *An* exten.,;ion L IK is *Galois* if and *only* if every *prime ideal* in *P*(LI K) split.,; *completely in L.*

Proof: Let again *NIK* he the normal closure of *LIK.* Then *P(NIK)* consists preci,;cly of those prime ideals which t-.plit completely in *L*. Hence if P(NIK) � P(LIK), then by (13.6),

$$\frac{1}{[N:K]} = d(P(NIK)) \geq d(P(LIKJ)e>\_ \frac{1}{[L:K]}$$

i.e., *[N:* Kl.::: IL: *K],* so $L = N$ is Galois. The convcr,;;e is trivial. D

(13.9) Proposition *(M.BA/Jf.H). If LIK* is *Galoi.,;* and *MIK* is *an arbitrary finite* extension. *1hen*

$$P(LIK)2P(M[K) \iff Lr;;M,$$

Proof: L <; M lrivially implies that *P(MIK)* C; *P(LIK).* So at-.wme convert-.ely that *P(LIK)2P(MIK).* Let *NIK* be a Galois extension containing Land *M,* and let G = G(NIK), *H = G(NIL), If'= C(NIM).* Then we have

$$P(MIK)� \qquad P,vlK(a) <; P(LIK)= \bigcup_{-r,),llirvl} P,1i,\bullet1drr).$$

Let *a* E *//¹*. Since P.v1K(a) **i,;** infinite by (13.4), there mw,t exist some p E P,v1K(a) such that p E PNIK(r) for a '>uitahle r E *G* wch that (r) n *fl* *i-* 0. But then *rr* i,; conjugate to r, and since // i!'. a normal subgroup of *G,* we find {rr) = \r) C; *Il.* We therefore have *f/¹* <; *H,* and henceL<;M. D

(13.10) Corollary. *A* G;.J/ois *extension I,IK is uniquely determined by rhc :set P(L* IK) of *prime* idea/,; *which ,;plit completely in ii.*

Thi,; beautiful result is the beginning of an answer to the programme formulated by *lt.OPow KHOMCKf:.H* (1821-1891), of characterizing the extensions of *K,* with all their algebraic and arithmetic properties, solely in term'> of sets of prime ideab, *"in a similar way as Cauchy"s theorem determines a.function hy its houndarv rn/ue�"* The re...ult raises the quct-.tion of how to characterize the sets *P(I,* IK) of prime ideals solely in tcnw, of the ba�c Held *K.* For abelian extensions, c\ast-. Held theory gives, a concise an<,wcr lo !hit-., **in** that it recognize� P (LI K) as the set of prime ideals lying in the ideal group H''' for any module of definition m (see chap. VI. (7.3)). If for instance LIK is the Hilbert class Held. then P(LIK) consists precisely of the prime ideals which are principal ideals. If on the other hand $K = \mathbb{Q}$ and $L =$ Ql(/L$_{111}$), then $P(L$ IK) comist" of all prime numbers $p ==$ **1** mod m.

In the case of nonabelian extension� LI K, a characterization of the �eb $P(LIK)$ is e%cntialty not known. However. this problem is part of a much more general and far-reaching programme known as "Langlands philo�ophf", which it-. undergoing a rapid development at the moment. For an introduction to this circle of ideas, we refer the interested reader to [106].

Bibliography

Adleman, LM., Heath-Rrown. D.R.

11] The fir;,t case of Fermat's la�t theorem. Invent. math. 79 (1985) 409-416

Ahlfors,LV.

[21 Complex Analy�i;,. McUraw-Hill, New York 1966

Apostol, TM.

131 Introduction to Analytic Number Theory. Springer, New York Hc1dclherg Berlin 1976

Artm, E.

[4] Bewei;, de;, allgemeinen Rcziproz1tabgc;,ctzcs. Collected Papers, Nr. 5. Addi-;,on-Wesley 1965

[5] Collected Papers. Addi;,on-Wesley 1965

[6] D1e gruppcntheoreti�chc Struktur der D1;,kriminanten algcbrai;,cher Zahlki)rper. Collected Papers, Nr. 9. Addi;,on-We�ley 1965

[7] ldealklas.�en in Oherki:irpem und allgemeincs Rez1pnv:iliilsgcset7. In: Colledcd Paper�, Nr. 7. Add1son-We;,lcy 1965

181 Uber cine neue Art von L-Reihen. In: Collected Paper�, Nr. 3. Adlfaon-We�ley 1965

Anm, .I::., Ha��e. H.

[9] Die beiden Ergrin7ung��iilzc 7um Re;;iprozitiitsgesetz der ,n-ten Potenae�te im Kiirper der '" -ten Einheitswur7eln. Co\leetcd Paper�, Nr. 6. Addison- Wesley 1965

Artin, E., Talc, J.

1101 Class Field Theory. Benjamin, New York Am�ten.lam 1967

Artrn, E., Whap!es, G.

111] Axiomatic characterization of fields hy the product torrnula for valuation� Bull. Amer. Math. Soc 51 (1945) 469-492

Bayer, P., Neukm.:h,J.

[!21 On value� of zeta functions and '-adic Euler characterist1e�. Invent. math. 50 (1978) 35-64

Bloch, S.

[13] Algebraic cycles and higher K-theory. Ad�. Math. 61 (1986) 267-304

Bornio, S.1., SafareviC, I.R.

[14) Number Theory. Academic Press. New York 1966

Bourhak1, N

{151 AlgCbrc. Hermann, Pari� 1970

116] AlgCbre commutative. Hermann, Pari� 1965

117] Espaecs vectorieh topo!og1que�. Hermann. Pari� 1966

118] Tupologie generale. Hermann, Pari� 1961

Bri.iekner, II

[19] line expl17ite Funnel ,.um Re7ipnllitUbge�el/ fi.ir Primzahlcxponenten p. In: Hasse, Ruquette, Algebra1�che Zahlentheorie. Rericht einer Tagung de\ Math. ln�l. Oherwolfm.:h 1%4. Bib!iographisches; lns;titut, Mannheim 1966

[20] Expli1,ite� Rcnpr07itht�gcset1 und Anwendungcn. Vorle�ungcn au� dcm Fachbere1eh M<1thematik der Univer�il,it fa�cn, Heft 2, 1979

I2 l] Hilbertsymbole 7Um Exponcntcn p'' und Pl'affsche 1-"ormen. Manu�cript Ham- burg 1979

Brumer, A

[22] On the units; of algebraic number tield�. Mathematika 14 (1967) 121-124

Cartan, H., Eilenberg, S.

[23] Homological Algebra. Princeton U1mer�11y Press, Princeton. N.J. 1956

Cassel�. J.W.S., Fr0hlich, A.

[24] Algebraic Number Theory. Thomp\011, Wa�hington, D.C 1967

Field Theory. Univer.\1(Ut Nagoya 1954

Deninger, C

[26] Moti,ie !,-functions; and regulari7cd determinant� In: Jann�en, Klcimann, Serre Seattle conference on motives. Proc. Symp. Pure Math. AMS 55 1, 707-743

\271 Mot1vic L-runetions and regulanLed determinants II. In. F. Catane¾e (ed.): Arithmetic Geometry, 138-156, Cambridge Uni,. Pres� 1997

Deuring,M.

[281 Algehraische Regn.indung der komplexen Mu!t1phkation. Abh. Math. Sem. Univ. Hamburg 16 {1949) 32--47

129] Die Kla¾\enkiirper der komplexen Mulliplikation. En,. Math. Wi\�. Band 1_2, Heft 10, Tei! Jl

[301 Uber den T�chehotarcff�chen DJChtigkeib�atL. Math. Ann. 110 (1935) 414-415

Dieudonne. J

[311 Ge�chichtc der Mathematik 1700-1900. Vieweg. Braun�ehwetg Wie�baden 1985

Dress, A.

[321 Cuntrihut1on� to the theory of mduced rcpre\entation�. Lecture Note� in Mathematics, vol. 342. Springer, Berlin Heidelberg New York 1973

Dwnrk, l3.

[33] Norm re\iduc �ymhol in locctl numhcr !ield�. Abh. Math. Si:m. Univ. Humburg 22 (1958) 180-190

l.:.rdclyi, A (Editor)

1341 H1ghcr Transcendental Function\, vol. I. Mc(iraw-Hill, New York Toronto London 1953

Fa!tmg�. G

135] Endlichkeit��atzc fiir ahehchc Varietatcn iiber Zahlhirpern. Invent. math. 73 (1983) 349-366

Fesenko, I.

[361 Ahellan exten,\ions of complete discrete valuation field\. In: Number Theory Pari� 1993/94, Camhndge Univ. Pre��- Cambridge 1996, pp. 47-74

[37] On class field theory of mult1d1mensional local fields of po�ilive characten\tic Adv<1nc:cs in S0\-1et Math. 4 (1991) pp. 103-127

[38] Cla�� field theory of multidimen\10nal local fields of characte1i�tic: 0, with the re�iduc field of po�it1ve characlcri�tic Ru��ian) Algebra i Ana117 3 i��c 3 (1991), pp. 165-196 [Engli�h St. Pctmburg Math. J. 3 (1992) pp. 649-678]

Fontaine, J.M.

[39] II n"y a pa� de variclC abe!1enne �ur Z. Invent. math. 81 (1985) 515-538

For\ter, 0.

1401 R1emann�chc Fliichen. Springer. Berlm Heidelberg Ne½ York 1977

Freitag, E

[411 Siegelsc:hc Modulfunktionen. Springer. Berlin Heidelberg Ne½ York 1983

foihlich, A. (Editor)

[42] Algebraic Number Fields (L-function� and Galois prnpertic�). Academic Pre�\, London Ne½ York San Franc1srn 1977

Frohlich, A.

[43] Formal Group�. Lecture Note� in Mathematic¾. vol. 74. Springer, Berlin Heidelberg New York 1968

Furtwangler, Ph.

[44] Allgcmciner Exi.\1en,.bcwcis fur den Kl<1¾�enkilrpcr emes heliebigcn algcbrai�chen Zah!kUrpcrs. Math. Ann. 63 (1907) l-37

145] Bcwci� des Hauptide.iba(Lc� ftir die Kla\\enkorpcr algebraischer Z<1hlkiirper. Hamh. Ahh. 7 (1930) 14-36

[46] Punktgittcr und ldeahheoric. Math. Ann. 82 (]921) 256-279

Gold�tem. L.J.

[47] Analytic Number Theory. Prentice-Hall Inc., New Jersey 1971

Golod, E.S., Šafarevič, LR.

[48] On Class Field Tower� (rn RU¾¾ianJ. l,v. Akad. Nau\.... SSSR 28 (1964) 261-272. [English tran�lation 111: AMS Translation\ (2) 48, 91-l021

Grothcndieek. A. et al.

1491 Thforie de�intersections et ThCOrCme de Riemann-Roch. SC.A 6, Lecture Notes in Mathematics, vol 225. Springer. Berlin Heidelberg New York 1971

HaherlanJ, K.

[50) Galo1� C'ohomology of Number Field� Deut�c:hcr Verlag der Wi\\Cn�chaftcn, Berlin

Hartshorne, R

[51] Algebraic Geometry. Springer, New York Heidelberg Berlin 1977

Has�e, H.

1521 Allgerneinc Theonc der G<1ufhchcn Summen in Zahlki)rpern Abh. d. Akad. W1�\. Math.-Natur½i4s. Kla\\e l

[53] Beneht Uber ncucre Unter�uchungen und Prohlerne au� dcr Theone der algehrdi�chcn Zahlkorper. Phy�ica. Wi.ir7hurg Wien 1970

[54] Die Struktur der R. Brauerschcn Algebrcnkla��cngruppe i.ihcr emem algebra1�chcn Zahlki.irper. Math. Ann. 107 (1933) 731-760

155 j Fuhrer, Di�kriminante und Ver7wcigun!,!".�kiirpcr abel"chcr Zahlki.irper. J. Reine Angew. Math. **162** (1930) 169-184

[561 H1�tory of Cla�� Field Theory. In: Ca��els-Fri.ihlich, Algebraic Nurnher Theory. Thomp�on, Washington, D.C. 1967

157] Mathemat1�che Abhand!ungen. De Gruytcr, Berlin New York 1975

[58] Uber die Kla��ennhl abel�chcr Zahlk6rper. Akadcmie-Verlag, Berlin 1952

[591 Vorlesungcn tiher Zahlenthcorie. Spnngcr, Berlin Heidelberg New York 1964

160] Zahlcntheone. Akademic-Yerlag, Berlin 1963

161] Zur Arbe1t von LR. SafareviC iibcr das allgcrneine Rc.liprozitiitsgeset7. Math. Nachr. 5 (1951) 301-327

lfat.ewinkcl, M

[62] Formal groups and applications. Academic Pre��- New York San Pranc1�co London 1978

163] Local cla"s field theory i� ea"Y· Adv. Math. **18** (!975) 1"1-8-181

Hecke, E

!641 Eme neue Art von Zctafunktioncn und ihrc Bezichung.en 1.ur Verteilung dcr Primzahlen. Er�te Mitteilung. Mathemat1"chc Werke Nr. ! 2, 215-234 Vandcnhoeck & Ruprecht, Gi:ittingcn 1970.

[65] Einc neue Art von Zetafunktionen und 1hre Bezichungcn *wr* der Primt.ahlen. Zwene Mitte1lung. Mathemati�che Wcrke Nr. 14, Vandenhocck & Ruprecht, Giiuingen 1970

[66] Mathemali�che Wcrke. Vandt:nhoeck & Ruprecht, G0ttingcn 1970

[671 Uber die Zetafunktion hclicbiger algebrai�chcr Zah!kiirper. Mathcmati,.chc Wcrke Nr. 7, 159-171. Vandenhoeck & Ruprecht, Gi.ittingen 1970

[68] Vorle�ungcn tiber die Theoric der algcbraischcn Zahlen. Second edition. Chel"ca, New York 1970

Henniart,G

[69] Loi� de rCCiprocitC cxphcitc� S6minairc de Thforie de� Nombre�, Pam 1979-80. B1rkhiiu�cr, Bo�ton Ba�el Stullgart 1981, pp. 115-149

Hen�cl, K.

[70] Thcorie der algehraischcn Zahlcn. Teuhncr. Leip7ig Berlin 1908

Hcrrmann,O.

\71] Uber Hilhertsche Modull"unktionen und die Dinchlcl�chen Rcihen rmt Euler-�cher Produktentwicklung. Math. Ann. **127** (1954) 357--400

Hilbert D.

(721 The Thcor) of algebraic Number Field� ("ZahlbcrichC), tran-,1. hy I. Adam-�on. with an mlroduction b) F. Lcmmermeycr and N. Schappachcr. Springer Verlag, Berlin etc. I998

HolLer, L.

[73] Kla��enkorpcrtheorie. Tcubner, Lcip71g 1966

Hi.ibschke, L

[74] Arakelovthcorie fur Zahlkl'irper. Rcgen�hurgcr Tnchtcr 20, Fakull11t flir MH1hemat1k dcr Univcr�1tiit Regcn�burg 1987

Huppert. 8.

[751 Endliche Gruppen I. Springer, Berlin Heidelberg New York 1967

Ireland, K., Ro\en, M

[76] A Cla�sical lntroduet1un tu Modern Number Theur}. Springer, New York Heidelberg Berlin 1981

lwa�awa, K.

[77] A chi\� number formula for cyclotomic field� Ann. Math. 76 (!962) 171-179

178] Lecture\ on p-adic L-Function�. Ann. Math. Studic� 74, Prmceton Univer�1ty Pre�� 1972

[79] Local Cla\� Field Theory. Oxford Univer�ity Pre�\, New York; Clarendon Press, Oxford 1986

[80] On explicit formulas tor the norm 1esiduc �ymbol. J. Math. Soc. Japan 20 (1968)

Janu�L. G.J

181] Algebrdic Number Fields. Academic Press, Nev.. York London 1973

Kaplansky, I.

[82] Commutative Ring�. The University of Chicago Pres� 1970

Kato, K

[83] A generalization ot local cla�� field theory hy u�ing K-group� I. J. Fae. Sci Univ. of Tokyo, Sec. IA 26 (1979) 103-376

Kawada, Y.

184) Class formations. Proc. Symp. Pure Mdth. 20 (1969) 96-114

Klingen, H

[85] Ober die Werte der Dedekindschen Zetafunkt1on. Mach. Ann. **145** (1962) 265-272

Koch, H

[86] Galm�sche Theorie Jer p-Erwe1lcrungcn. Deutscher Verlag der Wisscnschaften, Herlm 1970

Koch, H., Pieper, H.

[87] Zahlentheorie (Au�gewiihlte Methodcn und Ergebni��e). Deut�chcr Verlag der Wi��en�chaften, Berlin 1976

KOkLc,{, ¢

[881 � ; em Anulogon 7Um Hilbert\ymbol fi.ir algebra1�che Funktionen und Witt-Vektoren \Olcher Funktionen. D1plomarbeit, Regcn�hurg 1990

Krull, W.

189] Galoisst:hc Thcorie der unendlichen algcbraischen Erweiterungen. Math. Ann. **l00** (1928) 687-698

Kunz, E.

[90] Introduction to Commutative Algebra and Algebraic Geometry. B1rkhamer, Hoston Ba�el Stuttgart 1985

J91 I K.ihler D1ffcrcntiab. Vieweg Advanced Lecture� m Math., Braunschweig Wiesbaden 1986

Landau. I:..

192] Einfi.ihrung in die elementare und Theorie der algebrai�chcn Z.ihlen und dcr ldeale, C'hehea, New 1949

Lang, S.
1931 Algebra. Add1son-We�lcy 1971
(941 Algebrnil: Number Theory. Addi�nn-We�lcy 1970
[95] Cyclotomil: Field�. Springer, Berlin Heidelberg New York 1978
[96] Elliptic Funetiom (Second Ed11ion). Springer. Ne\\- York 1987
1971 Introduction to Modular Form\. Springer, Berlin Heidelberg New York 1976
[98] Real Analri�. Addison-Wc�lcy 1968

Lichtenbaum. S.
[99] Value� of Leta-funct10ns at non-negative Lecture Note� in Mathematic�. vol. 1068. Springer, 13er!in Heidelberg York 1984, pp.127-138

Lubin, J., Tate, J
[1001 Formal Complex Multiplicat1on m Local Field�. Ann. Math. 81 (1965) 380-387

Matsumura, H.
[101] Commutative 1ing theory. Cambridge Univer�1ty Pre�� 1980

Me�chkow�ki. H.
I 1021 Mathematiker-Lcxikon. B1bliographiM.:he� ln¾t!lut, Mimnheim 1968

M1lne,J.S.
[103] .Eta!e Cohomolog). Princeton Univcr�ity Pre��. Princeton. New Jer\ey 1980

Mumford.0
1104] The Red Book of Varietie¾ and Scheme�. Lecture Note� 111 Mathematics. vol 1358. Springer, Berlin Heidelberg New York 1988

Narkiew1cz, W.
[105] Elementary and Analytic Theory or Algebraic Number.\. Pofoh Scientific Publbhers. Warszawa 1974

Neukirch. J
[106] Algebrai¾che Zahlcntheorie. In: Em Jahrhundert Mathematik. re�lsl:hrift ,um Jubi!iium der OMV. Vieweg, Braun�chweig 1990
[107] Cla�� Field Thwry. Sprmger, Bcrlm Heidelberg New York Tokyo 1986
1108] Klassenkcirpcrtheorie. Bibl1ographischc� In�titut Mannheim 1969
11091 On Solvable Number F1dd\. Invent. math. 53 (!979) 135-164
[1101 The Beilinson Conjecture for Algebraic Number Fields. In: Beilinson's Conjectures on Special Values of L-Functions. M. Rapoport, N. Schappacher, P. Schneider (Editors). Perspectives in Mathematics, vol. 4. Academic Press, Boston 1987

Odly7ko, A.M
[I11] On Conductors and O1�criminants. In: A. Fr0hlith, Number Fickb. Academit Pre\�, London New York San Franci�co

Ogg. A
1112] Modular Forms and Dirichlet Serie�. lknjamin, New York Am�ten.him 1969

O'Mear<1, Q.T.
[I IJI Introduction to quadralil: l'orm� Springer, Berlin G0ttmgen Heidelberg 1963

Pattcr\on. SJ.
11141 EN!Clf Hro:1; und die Rolle der L-Rcihen in der Zahlentheoric. In: Ein

Jahrhun<lert Mathematik. Fc\t�chrift rnm Jubiliium der OMV. Vieweg, Braun-�chwc1g Wie¾baden 1990, pp. 629-655

Poilou. G.

11151 Cohomologie Galoi�ienne de, Module� F1111s. Dunod, Pan� 1967

Rapoport, M

11161 Comparison of the Regulators of Beilimon and of Borel. In: Bell111�on'4 Conjectures on Special Values of L-Functions (Rapoport, Schappacher, Schneider (Editors)). Perspectives in Mathematics, vol. 4. Academic Press, Boston 1987

Rapoport, M., Schappacher, N.. Schneider. P. (Editors)

[117] Beilin�on's Conjecture� on Values of L-Functmn\, Per,pective� in Mathematic\, vol. 4 Pre,,. Bo�ton I987

Ribenboim, P.

1118) 13 Lectures on Fermat\ La�t Theorem. Springer, Berlin Heidelberg New York 1979

S(;harlau, W.. Opolka, H

1119] Prom Fermat to Minkow,ki. Springer, Bcrlm llciddbcrg New York Tokyo 1984

Sch1!1111g, O.F.G

11201 The Theory ot Valuation,. Am. M.ith. Soc.. Providence, Rhode Island 1950

Sc1Te, J.-P.

[121J Cohomolog1e Galrnsienne. Lecture]\;ote, 111 Mathematic�. vol. 5. Springer. Berlin Heidelberg New York 1964

[1221 Corps locaux. Hermann, Pan� 1968

[1211 Cours d'arithm€tique. Pre,,e, univer�llairc� de France, Dunod, Pari� 1967

1124] Groupe� alg€brique� el corp� de classes. Hermann. Paris 1959

[125] ReprC�cntalion� linCaircs; des; groupe, fi111�, 2nd ed. Herm,mn, Pari� 1971

Shimura. G

[126] A reciprocity !aw in non-solvable exten�ion,. J. Rcmc Angcw. Math. **221** (1966) 209–220

Shintani, T

[127] A remark on zeta func1ion� ot number tield,. In: Automorph1c Forms, Repre,entation Theory Bombay Colloqrnurn 1979 Springer. Berlin Heidelberg New York !981

[1281 On c\aluation of zeta tunct1ons of totally re.ii algebraic number field� al integers. J. of rac. of Sc. Univ. Tokyo S.IA. '.ol. 23, 393--417,

C.L

Benxhnung von Zctafunktioncn an gannahligen Stellen. Nachr Akad ¥li,� G0ttingen 1969. pp.87-102

T.tkagi, T

I!30] Uber da, Rc1iprn1itiit�geset1 in cincm hclich1gcn algchrai�ehen Zahlk0rper J. Coll. Sci. Univ. Tok)o 44. 5 (1922) 1-50

I13I] Ubct cine Thcoric de� rclativ-ahchchcn Zahlkiirpcr�. J. Coll. Sci. Urnv. Tokyo 41,9(1920) 1-33

Tamme, G.
[132] Einfiihrung 111 die €talc Kohomologie. Regensburger Trichter 17, Fakultiit fi.ir Mathematik der Univer"itiit Regensburg 1979. [Eng!i�h tran�lation: Introduction to Etale Cohomology. Sprmger, Berlin Heidelberg New York 19941
I 1:"\JJ The Theorem of Riemann-Roch. In: Rapoport, Schappachcr, Schneider, Be1hn"on's on Special Value� of L-Functions. Perspectives in Mathematic\, 4. Academic Press, Bo�ton 1988

Tate,J.
[134) Fourier analysi" in number field� and Hecke\ Leta-function"· Thesi'-, Princeton 1950 (rcprmted in Ca""els. J.W.S., Frohlich, A. [24])

Vostokov. S.
[135] torm of the reciprocity law. ILv. Akad. Nauk. SSSR. Ser. Math. 42 [English tran�lation in: Math. USSR lzvc�tija 13 (1979)]

Wa�hington, L.C.
[136] Introduction to Cyclotomic f-iclds. Springer, Berlin Heidelberg New York 1982

Weil,A
11371 Ba�ic Number Theory. Springer, Berhn Heidelberg New York 1967
[138] Sur l'analogie entre le" corps de nombrc� alg€brique� et le\ corps de functions algCbri4ues. (Euvre� Scientitiques. \-ol. I, 1939a. Springer, Berlin Heidelberg New York 1979

Weiss,E.
[139] Algebraic Number Theory. McGraw-Hill, New York 1963

Weyl,H.
[140] Algebrai"che Zahlentheorie. Bib!iograph1�chc� In�titut, Mannheun
1966 Will,E.
[141] Verlagerung von Gruppcn uml Haupti<lealsat7. Proc. Int. Congr. of Math Am�ler<lam 1954. Ser. II, vol. 2. 71-73

D.
Die er\ten 50 Millionen Primtahlcn. In: Mathcrnati�che Miniaturen I. Birkhiiu�cr, Ba�d Boston Stuttgart 1981

Zari�ki. 0., Samuel, P.
[143] Commutative Algebra I. II. Van Nostnrnd, Princeton, New Jersey 1960

Cornell, G., Silverman. J.H., Steven�, G. (Editor�)
1144] Modular Forms and Fcrm<1t\ Last Theorem. Sprmger Verlag, Berlm clc. 1997

Neuk1rch. J., Schmidt, A., Wmgbcrg, K.
11451 Cohomology of Number Field". Sprmger Verlug, Berlin etc. 1999

Index

Printing (computer to plate): Mercedes Druck, Berlin
Binding: Buchbinderei Lüderitz & Bauer, Berlin

Grundlehren der mathematischen Wissenschaften

A Serie.1 (�/" Cmnprehrnsive Stu(lie.1 in Mathematics

A .Selection

217. Stenström: Rings of Quotients
218. Gihman/Skorohod: The Theory of Stochastic Processes II
219. Duvaut/Lions: Inequalities in Mechanics and Physics
220. Kirillov: Elements of the Theory of Representations
221. Mumford: Algebraic Geometry I: Complex Projective Varieties
222. Lang: Introduction to Modular Forms
223. Bergh/Löfström: Interpolation Spaces. An Introduction
224. Gilbarg/Trudinger: Elliptic Partial Differential Equations of Second Order
225. Schütte: Proof Theory
226. Karoubi: K-Theory. An Introduction
227. Grauert/Remmert: Theorie der Steinschen Räume
228. Segal/Kunze: Integrals and Operators
229. Hasse: Number Theory
230. Klingenberg: Lectures on Closed Geodesics
231. Lang: Elliptic Curves. Diophantine Analysis
232. Gihman/Skorohod: The Theory of Stochastic Processes III
233. Stroock/Varadhan: Multidimensional Diffusion Processes
234. Aigner: Combinatorial Theory
235. Dynkin/Yushkevich: Controlled Markov Processes
236. Grauert/Remmert: Theory of Stein Spaces
237. Köthe: Topological Vector Spaces II
238. Graham/McGehee: Essays in Commutative Harmonic Analysis
239. Elliott: Probabilistic Number Theory I
240. Elliott: Probabilistic Number Theory II
241. Rudin: Function Theory in the Unit Ball of C^n
242. Huppert/Blackburn: Finite Groups II
243. Huppert/Blackburn: Finite Groups III
244. Kubert/Lang: Modular Units
245. Cornfeld/Fomin/Sinai: Ergodic Theory
246. Naimark/Stern: Theory of Group Representations
247. Suzuki: Group Theory I
248. Suzuki: Group Theory II
249. Chung: Lectures from Markov Processes to Brownian Motion
250. Arnold: Geometrical Methods in the Theory of Ordinary Differential Equation
251. Chow/Hale: Methods of Bifurcation Theory
252. Aubin: Nonlinear Analysis on Manifolds. Monge-Ampère Equations
253. Dwork: Lectures on p-adic Differential Equations
254. Freitag: Siegelsche Modulfunktionen
255. Lang: Complex Multiplication
256. Hörmander: The Analysis of Linear Partial Differential Operators I
257. Hörmander: The Analysis of Linear Partial Differential Operators II
258. Smoller: Shock Waves and Reaction-Diffusion Equations
259. Duren: Univalent Functions
260. Freidlin/Wentzell: Random Perturbations of Dynamical Systems
261. Bosch/Güntzer/Remmert: Non Archimedian Analysis – A System Approach to Rigid Analytic Geometry
262. Doob: Classical Potential Theory and Its Probabilistic Counterpart
263. Krasnosel'skiĭ/Zabreĭko: Geometrical Methods of Nonlinear Analysis
264. Aubin/Cellina: Differential Inclusions
265. Grauert/Remmert: Coherent Analytic Sheaves
266. de Rham: Differentiable Manifolds

267. Arbarello/Cornalba/Griffith�Hams: Geometry of Algebraic Curves, Vol. I
268. Arbarello/Cornalba/Griffiths/Harris: Gcornclr) of Algebraic Curve�. Vol. II
269 Schapira· M1cmdifterent1al Sy�tern, m the Complex Domam
270. Scharlau: Quadratic anJ Hermitian Form�
271. Elhs: Entropy. Large Deviations, and Statistical Mechanics
272. Elhott: Arllhmctic functions and Integer Products
273 N1kol'�ki'i: Treat1,e on the Shifl Operator
274. H6rmander The Analysi, of Linear Partial Differential Operator, Ill
275. Hormander The Analysis of Linear Partial Differential Operators JV
276 Liggett· lntcractmg Particle Sy�tem,
277. rullon/Lang. Riemann-Roch Algebra
278. Barr/Wells: Topo�es, Triples and Theories
279. 81,hop/Bndge,· Comtruct1ve Analy,1,,
280. Neukirch: Clas, Field Theory
281. Chandrasekharan. Elliptic Function�
282 Lclong/Gruman- Entire Functmn, ot Several Complex Vanabks
283. Kodaira: Complex Manifold� and Deformation of Complex Structure,
284. Finn: Eqmlibrium Capillary Su1faces
285. Rurago/7.algallcr: Geometric lncqualit1c�
286. AnJriammv: Quadratic Form, and Hecke Operator,
287. Ma,kit: Kleini,m Group,
288. Jacod/Sh1ryacv: Limit Theorem� for Stochastic Procc,�c,
289. Mamn: Gauge Field Theory and Complex Geometry
290. Conway/Sloane. Sphere Packing�, Lallices and Group,
291. Hahn/O'Meara: The Cla�s1cal Groups and K-Theory
292. Ka,h1wara/Schap1ra: Sheave, on Mamfold,
293. Revul/Yor: Continuous Maningale, and Brownian Motion
294. Knus: Quadratic and Hermitian Form, over Rings
29':i. Die1kesJHilJeh1andt/Ktbler/Wohlrah: Mmimal Surface, I
296. Dierkes/Hildebrandt/Ku,ter/Wohlrab: Mmimal Surfaces II
297. Pastur/rigotin: Spectra of Random and Almost-Periodic Opcrah.1r,
298. Rcrhne/Gcl1.le1/Vergne: Heat Kernel, and D1ra!; Operator,
299. Pornrnerenke: Boundary Behaviour of Confom1al M..ip,
300. Orlik/ferao: Arrangements of Hyperplanes
301. Loday: Cyclic Homology
302. Lmge/Birkenhake: Complex Abehan Va11et1e,
303. DeYore/Lorenll: Con,tructive Approximation
304 Lorentz/v. Golmchek/Makovoz: Construcitve Approximation. Advanced Problem\
305. lliriart-Urruty/Lemarfrhal· Con�cx i\naly�i, and Mmimimtion Algonthm.,I
FunJamentdls
306. Hiriart-Urrnty/LcmarCchal: Convex Analy�is and Mrnimirntion Algorithm� II
Adv.meed Therny and Bundle Method,
307 Schwarz: Quantum Field Theory and Topology
308. Schwarr Topology for Phy\icl�h
109. Adem/Milgram: ('ohomology of F1mte Group�
310 Giaquint,t/Hildebrandt: Calculu, of Yanahon� I: The Lagrangian Formalism
311. Giaquinta/Hildebrandt: Calculu� of V:mat1ons II: The Hamiltonian Formali,m
312. Chung/Zhao: From Browman Motion lo Schriidinger·, Equ,llmn
'Ill \1allic1vm: StochasticAnalvsis
314. Adams/Hedberg· Funchon·Spaces and Potential Theory
315. Burg1\.,cr/Clau.,cn/Shokrollah1: Algebraic Cornplexit) Theory
316. Satlffot1k· l.oga11thmic Polentiab with External Fields
'.\17. Rockdfellar/Weh: Variational Analy�is
318. Kobaya.\hi: Hyperbolic Complex Space,
319 Bri(hon/llacfl1gcr Metric Space, ot Non-Posil1H: Curvature
320. K1pni.,/Land1m- Scaling Limits of Interacting Particle System�
321.Grimmctt.Pcrcolation
122. Neuk1rch. Algehra1c Numher Theory