

Nancy Childress

# Class Field Theory

类域论

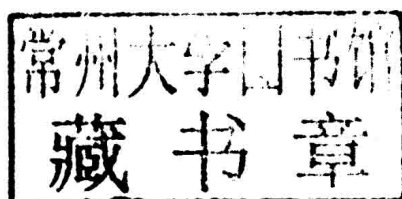


Springer

世界图书出版公司  
[www.wpcbj.com.cn](http://www.wpcbj.com.cn)

Nancy Childress

# Class Field Theory



Nancy Childress  
Department of Mathematics and Statistics  
Arizona State University  
Tempe, AZ, USA  
nc@asu.edu

*Editorial board:*

Sheldon Axler, San Francisco State University  
Vincenzo Capasso, Università degli Studi di Milano  
Carles Casacuberta, Universitat de Barcelona  
Angus MacIntyre, Queen Mary, University of London  
Kenneth Ribet, University of California, Berkeley  
Claude Sabbah, CNRS, École Polytechnique  
Endre Süli, University of Oxford  
Wojbor Woyczynski, Case Western Reserve University

Reprint from English language edition:  
Class Field Theory  
by Nancy Childress

This reprint has been authorized by Springer Science & Business Media for distribution in China Mainland only and not for export therefrom.

ISBN: 978-0-387-72489-8      e-ISBN: 978-0-387-72490-4  
DOI 10.1007/978-0-387-72490-4

Library of Congress Control Number: 2008935390

Mathematics Subject Classification (2000): 11Rxx, 11Sxx, 11-01

© Springer Science+Business Media, LLC 2009

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

## 图书在版编目 (CIP) 数据

类域论 = Class field theory: 英文/(美)奇尔德雷斯 (Childress, N.) 著. —影印本. —北京: 世界图书出版公司北京公司, 2013. 10

ISBN 978 - 7 - 5100 - 7021 - 1

I. ①类… II. ①奇… III. ①类域—理论—英文 IV. ①O156.2

中国版本图书馆 CIP 数据核字 (2013) 第 249232 号

---

书 名: Class Field Theory

作 者: Nancy Childress

中译名: 类域论

责任编辑: 高蓉 刘慧

---

出 版 者: 世界图书出版公司北京公司

印 刷 者: 三河市国英印务有限公司

发 行: 世界图书出版公司北京公司 (北京朝内大街 137 号 100010)

联系电话: 010 - 64021602, 010 - 64015659

电子信箱: kjb@wpcbj.com.cn

---

开 本: 24 开

印 张: 10

版 次: 2014 年 3 月

版权登记: 图字: 01 - 2013 - 5099

---

书 号: 978 - 7 - 5100 - 7021 - 1

定 价: 39.00 元

---

Universitext

For further volumes:  
<http://www.springer.com/series/223>



# Preface

In essence, class field theory is the study of the abelian extensions of arbitrary global or local fields. In particular, one is interested in characterizing the abelian extensions of a given field  $K$  in terms of the arithmetical data for  $K$ . The most basic example of such a characterization is the Kronecker-Weber Theorem, which states that the abelian extensions of the field of rational numbers are subfields of its cyclotomic extensions, so expressible in terms of roots of unity.

Also of interest is to describe how the prime ideals in the ring of integers of a global or local field decompose in its finite abelian extensions. In the case of the quadratic extensions of the field of rational numbers, such a description is obtained through the Law of Quadratic Reciprocity. There are also higher reciprocity laws of course, but all of these are subsumed by what is known as Artin Reciprocity, one of the most powerful results in class field theory.

I have always found class field theory to be a strikingly beautiful topic. As it developed, techniques from many branches of mathematics were adapted (or invented!) for use in class field theory. The interplay between ideas from number theory, algebra and analysis is pervasive in even the earliest work on the subject. And class field theory is still evolving. While it is prerequisite for most any kind of research in algebraic number theory, it also continues to engender active research. It is my hope that this book will serve as a gateway into the subject.

Class field theory has developed through the use of many techniques and points of view. I have endeavored to expose the reader to as many of the different techniques as possible. This means moving between ideal theoretic and *idèle* theoretic approaches, with  $L$ -functions and the Tate cohomology groups thrown in for good measure. I have attempted to include some information about the history of the subject as well. The book progresses from material that is likely more naturally accessible to students, to material that is more challenging.

The global class field theory for number fields is presented in Chapters 2-6, which are intended to be read in sequence. For the most part they are not prerequisite for Chapter 7. (The exceptions to this are in Chapter 6: profinite groups and the theory of infinite Galois extensions in Section 6, and the notion of a ramified prime in an infinite extension from Section 7.) The local material is positioned last primarily because it is somewhat more challenging; for this reason, working through the earlier chapters first may be of benefit.

For students who have completed an introductory course on algebraic number theory, a one-term course on global class field theory might comprise Chapters 2-5 and sections 1-4 of Chapter 6. For more experienced students, some of the material in these chapters may be familiar, e.g., the sections on Dirichlet series and the Theorem on Primes in Arithmetic Progressions. In that case, the remainder of Chapter 6 may be included to produce a course still entirely on global class field theory. For somewhat more sophisticated students, Chapter 7 provides the option of including the local theory.

Facility with abstract algebra and (very) basic topology and complex analysis is assumed. Chapter 1 contains an outline of some of the prerequisite material on number fields and their completions. Nearly all of the results in Chapter 1 appear without proof, but details can be found in Fröhlich and Taylor's *Algebraic Number Theory*, [FT], or (for the global fields) Marcus' *Number Fields*, [Ma].

The level of preparation in abstract algebra that is required increases slightly as one progresses through the book. However, I have included a little background material for certain topics that might not appear in a typical first-year course in abstract algebra. For example there are brief discussions on topological groups, infinite Galois theory, and projective limits. Finite Galois theory is heavily used throughout, and concepts such as modules, exact sequences, the Snake Lemma, etc., play important roles in several places. A small amount of cohomology is introduced, but there is no need for previous experience with cohomology.

The source for the material on Dirichlet characters in Chapter 2 is Washington's *Cyclotomic Fields*, [Wa], while the material on Dirichlet series was adapted primarily from Serre's *A Course in Arithmetic*, [Se1], and the book by Fröhlich and Taylor, [FT]. The section on Dirichlet density is derived mostly from Janusz' *Algebraic Number Fields*, [J], and Lang's *Algebraic Number Theory*, [L1].

I first saw class fields interpreted in terms of Dirichlet density in Sinnott's lectures, [Si], which greatly influenced the organization of the material in Chapters 3 and 4. (This point of view appears also in Marcus' *Number Fields*, [Ma].) Other sources that were particularly valuable in the writing of these two chapters were [J], [L1], and Cassels and Fröhlich's *Algebraic Number Theory*, [CF].

The main source consulted in the preparation of Chapters 5 and 6 is [L1], although [J], [CF], [Si], Neukirch's *Class Field Theory*, [N], and the lecture notes of Artin and Tate, [AT], also were very valuable throughout. For section 7 of Chapter 6, [Wa] is the primary source, and Lang's *Cyclotomic Fields I and II*, [L3], was also consulted.

Other references that proved particularly useful in the preparation of the chapters on global class field theory include Gras' *Class Field Theory*, [G], and Milne's lecture notes, [Mi].

The presentation of local class field theory in Chapter 7 relies mainly on the article by Hazewinkel, [Haz2]. Also very useful were Iwasawa's *Local Class Field Theory*, [I], Neukirch's book, [N], and the seminal article of Lubin and Tate, [LT].

A preliminary version of this book was used by a group of students and faculty at the University of Colorado, Boulder. I am indebted to them for their careful reading of the manuscript, and the many useful comments that resulted. My thanks espe-



cially to David Grant, who led the group and kept detailed notes on these comments, and to the members: Suion Ih, Erika Frugoni, Vinod Radhakrishnan, Zachary Strider McGregor-Dorsey and Jonathan Kish.

Several incarnations of the manuscript for this book have been used for courses in class field theory that I have offered periodically. I am grateful to my class field theory students over the past few years, who have participated in these courses using early versions of the manuscript. Among those who have helped in spotting typographical errors and other oddities are Eric Driver, Ahmed Matar, Chase Franks, Rachel Wallington, Michael McCamy and Shawn Elledge. Special thanks also to John Kerl for advice on creating diagrams in LaTeX and to Linda Arneson for her excellent work in typing the first draft of the course outline, which grew into this book.

In completing this book, I am most fortunate to have worked with Mark Spencer, Frank Ganz and David Hartman at Springer, and to have had valuable input from the reviewers. My sincere thanks to them as well.

Tempe, AZ  
2007



# Contents

<b>1 A Brief Review</b>	1
1 Number Fields	1
2 Completions of Number Fields	8
3 Some General Questions Motivating Class Field Theory	14
<b>2 Dirichlet's Theorem on Primes in Arithmetic Progressions</b>	17
1 Characters of Finite Abelian Groups	17
2 Dirichlet Characters	20
3 Dirichlet Series	30
4 Dirichlet's Theorem on Primes in Arithmetic Progressions	35
5 Dirichlet Density	40
<b>3 Ray Class Groups</b>	45
1 The Approximation Theorem and Infinite Primes	45
2 Ray Class Groups and the Universal Norm Index Inequality	47
3 The Main Theorems of Class Field Theory	60
<b>4 The Idèlic Theory</b>	63
1 Places of a Number Field	64
2 A Little Topology	66
3 The Group of Idèles of a Number Field	68
4 Cohomology of Finite Cyclic Groups and the Herbrand Quotient	75
5 Cyclic Galois Action on Idèles	83
<b>5 Artin Reciprocity</b>	105
1 The Conductor of an Abelian Extension of Number Fields and the Artin Symbol	105
2 Artin Reciprocity	111
3 An Example: Quadratic Reciprocity	128
4 Some Preliminary Results about the Artin Map on Local Fields	130

<b>6</b>	<b>The Existence Theorem, Consequences and Applications</b>	<b>135</b>
1	The Ordering Theorem and the Reduction Lemma	136
2	Kummer $n$ -extensions and the Proof of the Existence Theorem	139
3	The Artin Map on Local Fields	148
4	The Hilbert Class Field	153
5	Arbitrary Finite Extensions of Number Fields	159
6	Infinite Extensions and an Alternate Proof of the Existence Theorem	162
7	An Example: Cyclotomic Fields	168
<b>7</b>	<b>Local Class Field Theory</b>	<b>181</b>
1	Some Preliminary Facts About Local Fields	182
2	A Fundamental Exact Sequence	186
3	Local Units Modulo Norms	191
4	One-Dimensional Formal Group Laws	195
5	The Formal Group Laws of Lubin and Tate	198
6	Lubin–Tate Extensions	201
7	The Local Artin Map	210
	<b>Bibliography</b>	<b>219</b>
	<b>Index</b>	<b>223</b>

# Chapter 1

## A Brief Review

For the convenience of the reader and to fix notation, in this chapter we recall some basic definitions and theorems for extensions of number fields and their completions. Typically the material discussed in this chapter would be presented in detail in an introductory course on algebraic number theory.

We conclude this chapter with a brief discussion of some questions that arise naturally in the study of algebraic number fields. These questions were important to the development of class field theory. In subsequent chapters, we shall explore some of the mathematics they have inspired. Class field theory provides information on the nature of the abelian extensions of number fields, their ramified primes, their primes that split completely, elements that are norms, etc. We also treat the abelian extensions of local fields in a later chapter, where analogous questions may be asked. The present chapter is intended to be used as a quick reference for the notation, terminology and precursory facts relating to these concepts.

We state nearly all of the results in this chapter without proof. For a more thorough treatment of introductory algebraic number theory, see Fröhlich and Taylor's *Algebraic Number Theory*, [FT], (which includes material on completions), or Marcus' *Number Fields*, [Ma], (which does not). Somewhat more advanced books on the subject include Janusz' *Algebraic Number Fields*, [J], and Lang's *Algebraic Number Theory*, [L1].

### 1 Number Fields

A *number field* is a finite extension of the field  $\mathbb{Q}$  of rational numbers. If  $F$  is a number field, denote the ring of algebraic integers in  $F$  by  $\mathcal{O}_F$ . It is well-known that  $\mathcal{O}_F$  is a Dedekind domain, so that any ideal of  $\mathcal{O}_F$  has a unique factorization into a product of prime ideals. A *fractional ideal* of  $F$  is a non-zero finitely generated  $\mathcal{O}_F$ -submodule of  $F$ . The fractional ideals of  $F$  form a group  $\mathcal{I}_F$  under multiplication; the identity in  $\mathcal{I}_F$  is  $\mathcal{O}_F$ , and for a fractional ideal  $\mathfrak{a}$ , we have

$$\mathfrak{a}^{-1} = \{x \in F : x\mathfrak{a} \subseteq \mathcal{O}_F\}.$$

The principal fractional ideals of  $F$  form a (normal) subgroup of  $\mathcal{I}_F$ , denoted  $\mathcal{P}_F$ . The quotient  $\mathcal{C}_F = \mathcal{I}_F / \mathcal{P}_F$  is called the *ideal class group* of  $F$ . A non-trivial theorem in algebraic number theory says that  $\mathcal{C}_F$  is a finite group for any number field  $F$ . Its order is the *class number* of  $F$ , denoted  $h_F$ .

Given a finite extension  $K/F$  of algebraic number fields, consider the ideal  $\mathfrak{p}\mathcal{O}_K$ , where  $\mathfrak{p}$  is a non-zero prime ideal of  $\mathcal{O}_F$ . Using unique factorization of ideals in  $\mathcal{O}_K$ , we have

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

where the  $\mathfrak{P}_j$  are (distinct) prime ideals of  $\mathcal{O}_K$ ,  $g = g(\mathfrak{p})$  is a positive integer and the  $e_j$  are positive integers. We call  $e_j$  the *ramification index* for  $\mathfrak{P}_j/\mathfrak{p}$ , denoted  $e_j = e(\mathfrak{P}_j/\mathfrak{p})$ . If  $K/F$  is a Galois extension, then the Galois group permutes the  $\mathfrak{P}_j$  transitively, so that  $e_1 = \cdots = e_g = e$ , say.

Since every non-zero prime ideal is maximal in a Dedekind domain, the quotients  $\mathcal{O}_K/\mathfrak{P}_j$  and  $\mathcal{O}_F/\mathfrak{p}$  are fields, called *residue fields*. Indeed, they are finite fields of characteristic  $p$ , where  $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ . We may view  $\mathcal{O}_F/\mathfrak{p}$  as a subfield of  $\mathcal{O}_K/\mathfrak{P}_j$ . The *residue field degree* is

$$f(\mathfrak{P}_j/\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{P}_j : \mathcal{O}_F/\mathfrak{p}].$$

If  $K/F$  is Galois, then  $f(\mathfrak{P}_1/\mathfrak{p}) = \cdots = f(\mathfrak{P}_g/\mathfrak{p}) = f$ , say.

In general, we have  $\sum_{j=1}^g e(\mathfrak{P}_j/\mathfrak{p}) f(\mathfrak{P}_j/\mathfrak{p}) = [K : F]$ . When  $K/F$  is Galois, this becomes  $efg = [K : F]$ .

If  $K/F$  is an extension of number fields, we say that the prime  $\mathfrak{p}$  is *unramified* in  $K/F$  if  $e(\mathfrak{P}_j/\mathfrak{p}) = 1$  for all  $j$ ,  $\mathfrak{p}$  is *totally ramified* in  $K/F$  if there is a unique prime  $\mathfrak{P}$  above  $\mathfrak{p}$  with  $e(\mathfrak{P}/\mathfrak{p}) = [K : F]$ ,  $\mathfrak{p}$  *remains inert* in  $K/F$  if  $\mathfrak{p}\mathcal{O}_K$  is prime in  $\mathcal{O}_K$ , and  $\mathfrak{p}$  *splits completely* in  $K/F$  if  $g = [K : F]$ .

Given an extension  $K/F$  of number fields and a prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_F$ , one approach to finding the factorization of  $\mathfrak{p}\mathcal{O}_K$  is the following, sometimes called the *Dedekind-Kummer Theorem*.

**Theorem 1.1.** *Let  $K/F$  be an extension of number fields and suppose  $\mathcal{O}_K = \mathcal{O}_F[\alpha]$ . Let  $f(X) = \text{Irr}_F(\alpha, X)$ , the irreducible polynomial of  $\alpha$  over  $F$ , and let  $\mathfrak{p}$  be a prime ideal in  $\mathcal{O}_F$ . Put  $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p}$ , and denote the image of  $f(X)$  in  $\mathbb{F}_{\mathfrak{p}}[X]$  by  $\overline{f(X)}$ , (reduce the coefficients of  $f$  modulo  $\mathfrak{p}$ ). Suppose in  $\mathbb{F}_{\mathfrak{p}}[X]$ , the factorization of  $\overline{f(X)}$  is given by*

$$\overline{f(X)} = \overline{p_1(X)}^{e_1} \cdots \overline{p_g(X)}^{e_g}$$

where the  $\overline{p_j(X)}$  are distinct monic irreducible polynomials in  $\mathbb{F}_{\mathfrak{p}}[X]$ . For each  $j$ , let  $p_j(X)$  be a monic lift of the corresponding  $\overline{p_j(X)}$  to  $\mathcal{O}_F[X]$ , and let  $\mathfrak{P}_j$  be the ideal of  $\mathcal{O}_K$  generated by  $\mathfrak{p}$  and  $p_j(\alpha)$ . Then

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

with the  $\mathfrak{P}_j$  distinct prime ideals of  $\mathcal{O}_K$ .  $\square$

The discriminant of an extension of number fields will be of use to us. This can be defined in terms of the discriminants of bases for  $K$  as a vector space over  $F$ . Recall that if  $K/F$  is a finite extension of number fields, with  $\{v_1, \dots, v_n\}$  an  $F$ -basis of  $K$ , then we define the *discriminant* of this basis to be

$$d(v_1, \dots, v_n) = \det[\mathrm{Tr}_{K/F}(v_i v_j)] = \det[\sigma_i(v_j)]^2$$

where  $\sigma_1, \dots, \sigma_n : K \hookrightarrow F^{\mathrm{alg}}$  are  $F$ -monomorphisms. The relationship between the discriminants of two different bases for  $K$  over  $F$  can be described in terms of the change of basis matrix between them: If  $A$  is an  $n \times n$  matrix with  $(w_1, \dots, w_n)^t = A(v_1, \dots, v_n)^t$ , then

$$d(w_1, \dots, w_n) = (\det A)^2 d(v_1, \dots, v_n).$$

In the case when  $K = F(\alpha)$  where  $[K : F] = n$ , the matrix  $[\sigma_i(\alpha^{j-1})]$  is Vandermonde, so

$$d(1, \dots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

Specifically, if  $\mathcal{O}_K = \mathcal{O}_F[\alpha]$  and  $f(X)$  is the irreducible polynomial of  $\alpha$  over  $F$ , then  $N_{K/F}(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} d(1, \alpha, \dots, \alpha^{n-1})$ .

Note that different  $F$ -bases for  $K$  need not have the same discriminant. Hence the discriminant of the extension  $K/F$  must be defined in terms of all the possible bases for  $K$ . To do so, we generate a module with all these discriminants.

Suppose  $M$  is a non-zero  $\mathcal{O}_F$ -submodule of  $K$  and  $M$  contains an  $F$ -basis of  $K$ . We let  $d(M)$  be the  $\mathcal{O}_F$ -module generated by all  $d(v_1, \dots, v_n)$  where  $\{v_1, \dots, v_n\} \subset M$  varies through the  $F$ -bases for  $K$  contained in  $M$ . Of course if  $M$  is a fractional ideal of  $K$  then  $d(M)$  is a fractional ideal of  $F$ . Moreover, if  $M$  is a free  $\mathcal{O}_F$ -module, say  $M = \bigoplus_{i=1}^n \mathcal{O}_F w_i$ , then  $d(M) = d(w_1, \dots, w_n) \mathcal{O}_F$ .

The (relative) discriminant of the extension  $K/F$  is  $d_{K/F} = d(\mathcal{O}_K)$ , where  $\mathcal{O}_K$  is considered as a (finitely generated)  $\mathcal{O}_F$ -module. This makes  $d_{K/F}$  an integral ideal of  $\mathcal{O}_F$ . The (absolute) discriminant of  $K$  is  $d_K = d_{K/\mathbb{Q}}$ . Note that  $\mathcal{O}_K$  is a free  $\mathbb{Z}$ -module of rank  $n = [K : \mathbb{Q}]$ , so  $d_K = d_{K/\mathbb{Q}}$  is a (principal) ideal in  $\mathbb{Z}$ , generated by  $d(v_1, \dots, v_n)$  where  $\{v_1, \dots, v_n\}$  is any integral basis for  $\mathcal{O}_K$ , (by *integral basis* we mean a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$ ).

One of the reasons why discriminants will be useful to us is that they carry information about the primes that ramify in an extension. For a non-zero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_F$ , we have that  $\mathfrak{p}$  is ramified in  $K/F$  if and only if  $\mathfrak{p} \mid d_{K/F}$ .

We shall make heavy use of the notion of the norm of a fractional ideal. We record its definition and a few basic facts here. Let  $K/F$  be a finite extension of

number fields. Let  $\mathfrak{p}$  be a non-zero prime ideal of  $\mathcal{O}_F$  and let  $\mathfrak{P}$  be a prime of  $\mathcal{O}_K$  dividing  $\mathfrak{p}\mathcal{O}_K$ . Define the *norm* of  $\mathfrak{P}$  as  $N_{K/F}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$ . Now extend  $N_{K/F}$  to arbitrary fractional ideals of  $K$  by multiplicativity, i.e.,

$$N_{K/F}(\mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_t^{a_t}) = N_{K/F}(\mathfrak{P}_1)^{a_1} \cdots N_{K/F}(\mathfrak{P}_t)^{a_t}.$$

Thus the norm of a fractional ideal of  $K$  is a fractional ideal of  $F$ . Note that if  $K/F$  is Galois, then

$$N_{K/F}(\mathfrak{A})\mathcal{O}_K = \prod_{\sigma \in \text{Gal}(K/F)} \sigma(\mathfrak{A}).$$

If  $\alpha \in K$ , then  $N_{K/F}(\alpha\mathcal{O}_K) = N_{K/F}(\alpha)\mathcal{O}_F$ , where the norm on the right is the usual element norm. Also, if  $F \subseteq E \subseteq K$  are number fields, then

$$N_{K/F} = N_{E/F} \circ N_{K/E}.$$

The specific case when  $F = \mathbb{Q}$  gives  $N_{K/\mathbb{Q}}(\mathfrak{A}) = a\mathbb{Z}$  for some  $a \in \mathbb{Q}$ . We shall sometimes write  $N\mathfrak{A}$  for  $N_{K/\mathbb{Q}}(\mathfrak{A})$ , and frequently in our expressions for Dirichlet series we shall also use  $N\mathfrak{A}$  to represent the non-negative generator  $|a|$  of  $a\mathbb{Z}$ .

Given a Galois extension of number fields  $K/F$  with Galois group  $G$ , a non-zero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_F$  and a prime ideal  $\mathfrak{P}$  of  $\mathcal{O}_K$  with  $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$ , we define the *decomposition group*

$$Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Note that  $Z(\mathfrak{P}/\mathfrak{p})$  acts on the finite field  $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ , fixing the subfield  $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p}$  elementwise, so there is a natural homomorphism of groups

$$Z(\mathfrak{P}/\mathfrak{p}) \rightarrow \text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

From algebraic number theory, we have the following.

**Theorem 1.2.** *Let  $K/F$  be a Galois extension of number fields with Galois group  $G$ . Let  $\mathfrak{p}$  be a non-zero prime ideal of  $\mathcal{O}_F$ .*

- i.  *$G$  acts transitively on the set of prime ideals  $\mathfrak{P}$  of  $\mathcal{O}_K$  that divide  $\mathfrak{p}\mathcal{O}_K$  whence*

$$[G : Z(\mathfrak{P}/\mathfrak{p})] = \#\{\text{primes } \mathfrak{P} \text{ of } \mathcal{O}_K : \mathfrak{P}|\mathfrak{p}\mathcal{O}_K\} = g.$$

*Also, if  $\mathfrak{P}, \mathfrak{P}'$  are prime ideals of  $\mathcal{O}_K$  dividing  $\mathfrak{p}\mathcal{O}_K$ , then  $Z(\mathfrak{P}/\mathfrak{p})$  and  $Z(\mathfrak{P}'/\mathfrak{p})$  are  $G$ -conjugate.*

- ii.  *$N\mathfrak{p} = \#\mathbb{F}_{\mathfrak{p}}$ ,  $N\mathfrak{P} = \#\mathbb{F}_{\mathfrak{P}}$  and  $\text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$  is cyclic, generated by the Frobenius automorphism  $\varphi_{\mathfrak{p}} : x \mapsto x^{N\mathfrak{p}}$ .*



iii. The homomorphism  $Z(\mathfrak{P}/\mathfrak{p}) \rightarrow \text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$  is surjective; its kernel is called the inertia subgroup, denoted  $T(\mathfrak{P}/\mathfrak{p})$ . Note that  $[Z(\mathfrak{P}/\mathfrak{p}) : T(\mathfrak{P}/\mathfrak{p})] = f$  and  $T(\mathfrak{P}/\mathfrak{p})$  has order  $e$ .  $\square$

In the case of a Galois extension  $K/F$  of number fields, the decomposition group and inertia subgroup give rise, via the Galois correspondence, to intermediate fields, called the *decomposition field* and *inertia field*, respectively. Let  $K_Z$  be the fixed field of  $Z(\mathfrak{P}/\mathfrak{p})$  and let  $K_T$  be the fixed field of  $T(\mathfrak{P}/\mathfrak{p})$ . For an abelian extension, the factorization of the ideals generated by  $\mathfrak{p}$  in these intermediate fields is given by the following result from algebraic number theory.

**Theorem 1.3 (Layer Theorem).** Let  $\mathfrak{p}$  be a non-zero prime ideal of  $\mathcal{O}_F$ , where  $K/F$  is an abelian extension of number fields. Then  $\mathfrak{p}$  splits completely in  $K_Z/F$ . The primes above  $\mathfrak{p}$  remain inert in  $K_T/K_Z$  and ramify totally in  $K/K_T$ .  $\square$

If  $e(\mathfrak{P}/\mathfrak{p}) = 1$ , then via the natural homomorphism in (iii) of Theorem 1.2, we have  $Z(\mathfrak{P}/\mathfrak{p}) \cong \text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$  is cyclic of order  $f$ . The Galois group for the residue fields is generated by the Frobenius automorphism  $\varphi_{\mathfrak{p}}$ , whence there is a unique element  $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$  that corresponds to  $\varphi_{\mathfrak{p}}$  under the natural isomorphism. We have  $Z(\mathfrak{P}/\mathfrak{p}) = \langle \sigma \rangle$ . This element  $\sigma$  is called the *Frobenius element* at  $\mathfrak{P}$ . We denote it  $\sigma = \left( \frac{\mathfrak{P}}{K/F} \right) = (\mathfrak{P}, K/F)$ .

**Proposition 1.4.** Let  $K/F$  be a Galois extension of number fields,  $\mathfrak{p}$  a non-zero prime of  $\mathcal{O}_F$  that is unramified in  $K/F$  and  $\mathfrak{P}$  a prime of  $\mathcal{O}_K$  with  $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$ . Then the Frobenius element at  $\mathfrak{P}$  is the unique element  $\sigma \in \text{Gal}(K/F)$  that satisfies  $\sigma(\alpha) \equiv \alpha^{N_{\mathfrak{P}}} \pmod{\mathfrak{P}}$  for every  $\alpha \in \mathcal{O}_K$ .

*Proof.* Say  $\sigma(\alpha) \equiv \alpha^{N_{\mathfrak{P}}} \pmod{\mathfrak{P}}$  for all  $\alpha \in \mathcal{O}_K$ . From this congruence we see that  $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$ , whence  $\sigma(\mathfrak{P}) = \mathfrak{P}$ , i.e.,  $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$ . Clearly, the isomorphism  $Z(\mathfrak{P}/\mathfrak{p}) \cong \text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$  maps  $\sigma$  to  $\varphi_{\mathfrak{p}}$ . Thus  $\sigma = \left( \frac{\mathfrak{P}}{K/F} \right)$ .  $\square$

If we suppose further that  $G$  is abelian, then by (i) of Theorem 1.2 we know that  $Z(\mathfrak{P}/\mathfrak{p})$  depends only on  $\mathfrak{p}$  and we may write  $Z(\mathfrak{p})$ . Also, if  $\mathfrak{p}$  is unramified in  $K/F$ , then we show in Proposition 1.5 below that the Frobenius element at  $\mathfrak{P}$  depends only on  $\mathfrak{p}$ . In this case, we call it the *Artin automorphism* for  $\mathfrak{p}$ , denoted  $\left( \frac{\mathfrak{p}}{K/F} \right) = (\mathfrak{p}, K/F)$ . We may define a map

$$\{\text{primes of } \mathcal{O}_F \text{ that are unramified in } K/F\} \rightarrow G$$

$$\text{given by } \mathfrak{p} \mapsto \sigma_{\mathfrak{p}} = \left( \frac{\mathfrak{p}}{K/F} \right).$$

**Proposition 1.5.** Let  $K/F$  be an abelian extension of number fields,  $\mathfrak{p}$  a non-zero prime of  $\mathcal{O}_F$  that is unramified in  $K/F$  and  $\mathfrak{P}$  a prime of  $\mathcal{O}_K$  with  $\mathfrak{P}|\mathfrak{p}\mathcal{O}_K$ . Then  $\sigma = \left( \frac{\mathfrak{P}}{K/F} \right)$  does not depend on the choice of the prime  $\mathfrak{P}$  above  $\mathfrak{p}$ .