Class Field Theory

J.S. Milne

Version 4.03
August 6, 2020

Class field theory describes the abelian extensions of a local or global field in terms of the arithmetic of the field itself. These notes contain an exposition of abelian class field theory using the algebraic/cohomological approach of Chevalley and Artin and Tate. The explicit approach of Lubin and Tate in the local case and the analytic approach in the global case are also explained. The original version of the notes was distributed during the teaching of an advanced graduate course.

BibTeX information

```
@misc{milneCFT,
  author={J.S. Milne},
  title={Class Field Theory (v4.03)},
  year={2020},
  note={Available at www.jmilne.org/math/},
  pages={287+viii}
}
```

v2.01 (August 14, 1996). First version on the web.
v3.10 (May 6, 1997). Substantially revised and expanded; 222 pages.
v4.00 (March 2, 2008). Corrected, revised, and expanded; 287 pages.
v4.01 (May 30, 2011). Many minor fixes; 287 pages.
v4.02 (March 23, 2013). Minor fixes and improvements; 289 pages.
v4.03 (August 6, 2020). Minor fixes and improvements; 294 pages.
Available at www.jmilne.org/math/
Please send comments and corrections to me at jmilne at umich dot edu.

The photograph is of Mt Christina from the McKellar Saddle, New Zealand.

Contents

Notation.

We use the standard (Bourbaki) notation:

$$\begin{array}{ll} \mathbb{N} & = \{0, 1, 2, \ldots\}, \\ \mathbb{Z} & = \text{ring of integers}, \\ \mathbb{Q} & = \text{field of rational numbers}, \\ \mathbb{R} & = \text{field of real numbers}, \\ \mathbb{C} & = \text{field of complex numbers}, \\ \mathbb{F}_p & = \mathbb{Z}/p\mathbb{Z} = \text{field with } p \text{ elements}, \ p \text{ a prime number}. \end{array}$$

For integers m and n, $m|n$ means that m divides n, i.e., $n \in m\mathbb{Z}$. Throughout the notes, p is a prime number, i.e., $p = 2, 3, 5, \ldots$.

Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$. The empty set is denoted by $\emptyset$. The cardinality of a set S is denoted by $|S|$ (so $|S|$ is the number of elements in S when S is finite). Let I and A be sets; a family of elements of A indexed by I, denoted $(a_i)_{i\in I}$, is a function $i \mapsto a_i : I \to A$.

$X \subset Y$	X is a subset of Y (not necessarily proper);
$X \stackrel{\text{def}}{=} Y$	X is defined to be Y, or equals Y by definition;
$X \approx Y$	X is isomorphic to Y;
$X \simeq Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism);
$\hookrightarrow$	denotes an injective map;
$\twoheadrightarrow$	denotes a surjective map.

It is standard to use Gothic (fraktur) letters for ideals:

$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{m}$	$\mathfrak{n}$	$\mathfrak{p}$	$\mathfrak{q}$	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$	$\mathfrak{M}$	$\mathfrak{N}$	$\mathfrak{P}$	$\mathfrak{Q}$
a	b	c	m	n	p	q	A	B	C	M	N	P	Q

Prerequisites

The algebra usually covered in first-year graduate courses and a course in algebraic number theory, for example, my course notes listed below.

References

In addition to the references listed at the end (and in footnotes), I shall refer to the following of my course notes:

GT Group Theory (v3.16, 2020)

FT Fields and Galois Theory (v4.61, 2020)

ANT Algebraic Number Theory (v3.08, 2020).

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of these notes: Vincenzo Acciaro; Raúl Alonso Rodríguez; Tom Bachmann; Oliver Braeunling; Chen, Bingxu; Kwangho Choiy; Brian Conrad; Keith Conrad; Giuseppe Canuto; Philip Dittmann; Ross Griffiths; Darij Grinberg; Florian Herzig; Chong Hui; Hervé Jacquet; Kiran Kedlaya; Timo Keller; Keenan Kidwell; Andrew Kirk; Michiel Kosters; Tyler Lawson; Jungin Lee; Franz Lemmermeyer; Yogesh More; Kim Nguyen; Jianing Li; Catherine

O'Neil; Jack Petok; Kartik Prasanna; Nandini Ranganathan; Peter Roquette; Joshua Seaton; Corinne Sheridan; Jonah Sinick; Daniel Sparks; Jamie Tappenden; Wojtek Wawrów; Yu Zhao; and others. Also I thank the contributors to math.stackexchange.com and mathoverflow.net, especially those who asked or answered questions on my notes.

I have been reading Chevalley's new book on class field theory; I am not really doing research, just trying to cultivate myself.
Grothendieck, 1956.

DRAMATIS PERSONÆ

FERMAT (1601–1665). Stated his last "theorem", and proved it for $m = 4$. He also posed the problem of finding integer solutions to the equation,

$$X^2 - AY^2 = 1, \quad A \in \mathbb{Z}, \tag{1}$$

which is essentially the problem[1] of finding the units in $\mathbb{Z}[\sqrt{A}]$. Brouncker found an algorithm for solving the problem, but neglected to prove that the algorithm always works.

EULER (1707–1783). He introduced analysis into the study of the prime numbers, and he discovered an early version of the quadratic reciprocity law.[2]

LAGRANGE (1736–1813). He proved that the algorithm for solving (1) always leads to a solution, and he proved that every positive integer is a sum of four squares.

LEGENDRE (1752–1833). He introduced the "Legendre symbol" $\left(\frac{m}{p}\right)$, and he found the complete form of the quadratic reciprocity law,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \quad p, q \text{ odd primes.}$$

He proved a result that implies the following local-global principle for quadratic forms in three variables over $\mathbb{Q}$: such a form $Q(X, Y, Z)$ has a nontrivial zero in $\mathbb{Q}$ if and only if it has one in $\mathbb{R}$ and the congruence $Q \equiv 0 \bmod p^n$ has a nontrivial solution for all p and n.

GAUSS (1777–1855). He found the first complete proofs of the quadratic reciprocity law. He studied the Gaussian integers $\mathbb{Z}[i]$ in order to find a quartic reciprocity law. He studied the classification of binary quadratic forms over $\mathbb{Z}$, which is closely related to the problem of finding the class numbers of quadratic fields.

DIRICHLET (1805–1859). He introduced L-series, and used them to prove an analytic formula for the class number and a density theorem for the primes in an arithmetic progression. He proved the following "unit theorem": let α be a root of a monic irreducible polynomial $f(X)$ with integer coefficients; suppose that $f(X)$ has r real roots and $2s$ complex roots; then $\mathbb{Z}[\alpha]^\times$ is a finitely generated group of rank $r + s - 1$.

KUMMER (1810–1893). He made a deep study of the arithmetic of cyclotomic fields, motivated by a search for higher reciprocity laws, and showed that unique factorization could be recovered by the introduction of "ideal numbers". He proved that Fermat's last theorem holds for regular primes.

HERMITE (1822–1901). He made important contributions to quadratic forms, and he showed that the roots of a polynomial of degree 5 can be expressed in terms of elliptic functions.

EISENSTEIN (1823–1852). He published the first complete proofs for the cubic and quartic reciprocity laws.

KRONECKER (1823–1891). He developed an alternative to Dedekind's ideals. He also had one of the most beautiful ideas in mathematics for generating abelian extensions of number fields (the Kronecker liebster Jugendtraum).

[1] The Indian mathematician Bhaskara (12th century) knew general rules for finding solutions to the equation.

[2] Euler discovered [the quadratic reciprocity law] and, apparently, it is possible to construct a proof of the theorem using different fragments that can be found in Euler's Opera omnia or his Nachless. It was Gauss who gave the first complete proof.... (Michael Berg, MR2131680).

RIEMANN (1826–1866). Studied the Riemann zeta function, and made the Riemann hypothesis.

DEDEKIND (1831–1916). He laid the modern foundations of algebraic number theory by finding the correct definition of the ring of integers in a number field, by proving that ideals factor uniquely into products of prime ideals in such rings, and by showing that, modulo principal ideals, they fall into finitely many classes. Defined the zeta function of a number field.

WEBER (1842–1913). He found the correct generalization of "class group" to allow for ramification. Made important progress in class field theory and the Kronecker Jugendtraum.

HENSEL (1861–1941). He gave the first definition of the field of p-adic numbers (as the set of infinite sums $\sum_{n=-k}^{\infty} a_n p^n$, $a_n \in \{0, 1, \dots, p-1\}$) in the 1890s.[3]

HILBERT (1862–1943). He wrote a very influential book on algebraic number theory in 1897, which gave the first systematic account of the theory. Some of his famous problems were on number theory, and have also been influential.

TAKAGI (1875–1960). He proved the fundamental theorems of abelian class field theory, as conjectured by Weber and Hilbert.

NOETHER (1882–1935). Together with Artin, she laid the foundations of modern algebra in which axioms and conceptual arguments are emphasized, and she contributed to the classification of central simple algebras over number fields.

HECKE (1887–1947). Introduced Hecke L-series generalizing both Dirichlet's L-series and Dedekind's zeta functions.

ARTIN (1898–1962). He found the "Artin reciprocity law", which is the main theorem of class field theory (improvement of Takagi's results). Introduced the Artin L-series.

HASSE (1898–1979). He gave the first proof of local class field theory, proved the Hasse (local-global) principle for all quadratic forms over number fields, and contributed to the classification of central simple algebras over number fields.

BRAUER (1901–1977). Defined the Brauer group, and contributed to the classification of central simple algebras over number fields.

WEIL (1906–1998). Showed how to interpret Hecke characters in terms of idèles. Defined the Weil group, which enabled him to give a common generalization of Artin L-series and Hecke L-series.

CHEVALLEY (1909–84). The main statements of class field theory are purely algebraic, but all the earlier proofs used analysis; Chevalley gave a purely algebraic proof. With his introduction of idèles he was able to give a natural formulation of class field theory for infinite abelian extensions.

IWASAWA (1917–1998). He introduced an important new approach into algebraic number theory which was suggested by the theory of curves over finite fields.

TATE (1925–2019). He proved new results in group cohomology, which allowed him to give an elegant reformulation of class field theory. With Lubin he found an explicit way of generating abelian extensions of local fields.

LANGLANDS (1936–). The Langlands program[4] is a vast series of conjectures that, among other things, contains a *nonabelian* class field theory.

[3] The theory of valuations was founded by the Hungarian mathematician Kürschák in 1912.

[4] Not to be confused with its geometric analogue, sometimes referred to as the geometric Langlands program, which appears to lack arithmetic and analytic significance.

Introduction

L'objet de la théorie du corps de classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques K peuvent être déterminées par des éléments tirés de la connaissance de K lui-même; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement.
Chevalley 1940.[5]

The goal of class field theory is to describe the Galois extensions of a local or global field in terms of the arithmetic of the field itself. For abelian extensions, the theory was developed between roughly 1850 and 1930 by Kronecker, Weber, Hilbert, Takagi, Artin, Hasse, and others. For nonabelian extensions, the first indication of the shape the theory should take is in a letter from Langlands to Weil in 1967. In recent years there has been much progress in the nonabelian local and function field cases, but less in the number field case. Beginning about 1980, abelian class field theory has been succesfully extended to higher dimensional fields.

Apart from a few remarks about the more general cases, these notes will concentrate on the case of abelian extensions of local and number fields, which is the basic case.

In the remainder of the introduction, I give a brief historical outline of abelian class field theory. Throughout, by an extension L of a number field K, I mean an extension field contained in some fixed algebraically closed field containing K. For example, if K is a number field contained in $\mathbb{C}$, then we can consider the extensions of K contained in $\mathbb{C}$.

Classification of extensions by the prime ideals that split

Recall (ANT, 3.34) that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ factors (decomposes) in an extension L of K as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{2}$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are the prime ideals of $\mathcal{O}_L$ such that $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$ and $e_i \geq 1$. Moreover,

$$n = e_1 f_1 + \cdots + e_g f_g, \tag{3}$$

where n is the degree of L over K and f_i is the degree of the residue field extension $\mathcal{O}_L/\mathfrak{P}_i \supset \mathcal{O}_K/\mathfrak{p}$. When $e_i > 1$ for some i, the prime $\mathfrak{p}$ is said to ramify in L, and when

[5]The object of class field theory is to show how the abelian extensions of an algebraic number field K can be determined by elements drawn from a knowledge of K itself; or, if one prefers to present things in dialectical terms, how a field contains within itself the elements of its own transcending.

all $e_i > 1$, it is said to be totally ramified in L. When $e_i = 1 = f_i$ for all i, so that $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$, the prime $\mathfrak{p}$ is said to split in L (or, for emphasis, split completely). Choose a primitive element α for L/K with $\alpha \in \mathcal{O}_L$. Then

$$L = K[\alpha] \simeq K[X]/(f(X)), \quad (f \text{ monic irreducible}),$$

and the primes that ramify divide the discriminant of f (so there can only be finitely many of them).[6] Moreover, a prime ideal not dividing the discriminant of f splits in L if and only if f splits completely modulo $\mathfrak{p}$. For example, if (p) ramifies in $\mathbb{Q}[\sqrt{m}] \simeq \mathbb{Q}[X]/(X^2-m)$, then p divides $4m$, and a prime ideal (p) not dividing $4m$ splits in $\mathbb{Q}[\sqrt{m}]$ if and only if m becomes a square modulo p.

When L/K is Galois, $e_1 = e_2 = \cdots = e$ and $f_1 = f_2 = \cdots = f$, and so these equations simplify to

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e, \quad n = efg. \tag{4}$$

Let $\mathrm{Spl}(L/K)$ denote the set of prime ideals of $\mathcal{O}_K$ splitting in L. Towards the end of the nineteenth century, Frobenius used analytic methods to prove the following statement.

THEOREM 0.1 (FROBENIUS) *When L/K is Galois, the set $\mathrm{Spl}(L/K)$ has density $1/[L\colon K]$ in the set of all prime ideals in $\mathcal{O}_K$.*

From this it follows that the set $\mathrm{Spl}(L/K)$ determines L: if the same primes split in L and L', then it follows that

$$\mathrm{Spl}(L/K) = \mathrm{Spl}(LL'/K) = \mathrm{Spl}(L'/K)$$

(ANT, proof of 8.38), and so

$$[L\colon K] = [LL'\colon K] = [L'\colon K].$$

Thus the Galois extensions of K are classified by the sets $\mathrm{Spl}(L/K)$. Two fundamental problems remain.

0.2 Determine the sets $\mathrm{Spl}(L/K)$ as L runs over the finite Galois extensions of K.

0.3 Describe the extension L/K in terms of the set $\mathrm{Spl}(L/K)$.

We shall see that 0.2 has a precise answer when L runs over the *abelian* extensions of K. In this case, the sets $\mathrm{Spl}(L/K)$ are characterized by certain congruence conditions. However, for nonabelian Galois extensions, the sets are *not* characterized by congruence conditions, and the best one can hope for is some analytic description.

Regarding 0.3, note that the density of $\mathrm{Spl}(L/K)$ determines the degree of L/K. We would like to be able to determine the full Galois group of L/K. Moreover, we would like to determine how each prime of K decomposes in L. For example, we would like to determine the set of prime ideals that ramify in L, and for those that don't ramify we

[6] We have

$$\mathrm{disc}(f) = \mathrm{disc}(\mathcal{O}_K[\alpha]/\mathcal{O}_K) = (\mathcal{O}_L\colon \mathcal{O}_K[\alpha])^2 \cdot \mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$$

(see ANT, 2.25). Therefore, if a prime ramifies in L, then it divides $\mathrm{disc}(f)$, but there may be primes dividing $\mathrm{disc}(f)$ that are not ramified in L. For example, let L be the the quadratic field generated by a square root of m. If m is congruent to 1 mod 4, then 2 divides the discriminant of f but is not ramified in L.

would like to determine the residue class degree $f(\mathfrak{p})$ of the primes dividing $\mathfrak{p}$. For abelian extensions, from the description of $\mathrm{Spl}(L/K)$ given by 0.2, we shall be able to do this.

Before continuing I make one observation: in the above discussion, we may ignore a finite number of primes of K. For example, if S is a fixed finite set of prime ideals of $\mathcal{O}_K$, then, in the above discussion, we may replace $\mathrm{Spl}(L/K)$ with the set $\mathrm{Spl}_S(L/K)$ of prime ideals not in S that split in L.

NOTES For a Galois extension L/K of number fields, Frobenius attached a conjugacy class $(\mathfrak{p}, L/K)$ of elements in $G = \mathrm{Gal}(L/K)$ to each prime ideal $\mathfrak{p}$ of K unramified in L, and he conjectured that the density of the primes giving a fixed conjugacy class C is $|C|/|G|$. By construction, the elements in $(\mathfrak{p}, L/K)$ have order $f(\mathfrak{p})$ in G, and so this statement applied to the trivial conjugacy class gives Theorem 0.1. Frobenius was able to prove only a weaker statement than his conjecture (sufficient for 0.1), in which certain conjugacy classes are grouped together[7], and the full conjecture was proved by Chebotarev only in 1926.

Quadratic extensions of $\mathbb{Q}$

For quadratic extensions of $\mathbb{Q}$, the answer to 0.2 is provided by the quadratic reciprocity law. For example, let p be an odd prime number, and let $p^* = (-1)^{\frac{p-1}{2}} p$, so that $p^* \equiv 1 \bmod 4$. Then $\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q}$ is ramified only at p. A prime number $q \neq p$ splits in $\mathbb{Q}[\sqrt{p^*}]$ if and only if p^* is a square modulo q, i.e., $\left(\frac{p^*}{q}\right) = 1$. But if q is odd, then the quadratic reciprocity law says that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$, and so q splits in $\mathbb{Q}[\sqrt{p^*}]$ if and only if q is a square modulo p. Let $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$ be the set of squares. Then $\mathrm{Spl}(\mathbb{Q}\sqrt{p^*}]/\mathbb{Q})$ consists of the primes q such $q \bmod p$ lies in H. Recall that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of even order $p-1$, and so H is the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 2. Thus

$$(\mathbb{Z}/p\mathbb{Z})^\times/H \simeq \mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q}).$$

More generally, let S be a finite set of prime numbers. Let m be a positive integer divisible only by primes in S and assume that m is either odd or divisible by 4. For a subgroup H of $(\mathbb{Z}/m\mathbb{Z})^\times$ of index 2, let

$$p(H) = \{(p) \mid p \text{ a prime number, } p \notin S \text{ , } p \bmod m \text{ lies in } H\}.$$

Then the sets $\mathrm{Spl}_S(L/\mathbb{Q})$ for L running over the quadratic extensions of $\mathbb{Q}$ unramified outside S are exactly the sets $p(H)$ (for varying m). In particular, we see that each such set $\mathrm{Spl}_S(L/\mathbb{Q})$ is determined by a congruence condition modulo m for some m.

NOTES In elementary number theory courses, the quadratic reciprocity often appears as a curiosity, no more profound than many other curiosities. In fact, as the above discussion illustrates, it should be considered the first result in class field theory, which helps explain why Euler, Lagrange, Legendre, and Gauss devoted so much attention to it.

Unramified abelian extensions

Let I be the group of fractional ideals of K, i.e., the free abelian group generated by the prime ideals of $\mathcal{O}_K$, and let $i\colon K^\times \to I$ be the map sending $a \in K^\times$ to the principal ideal

[7] Frobenius, G., 1896, Die Beziehungen Zwischen den Primidealen eines Algebraischen Körpers und den Substitutionen einer Gruppe, Berlin Akad.-Ber.. For a statement of Frobenius's theorem, see Exercise A-10, p. 268.

(a). The class group C of K is $I/i(K^\times)$. To give a subgroup H of C is the same as giving a subgroup $\tilde{H}$ of I containing $i(K^\times)$.

By a "prime" of K, I mean an equivalence class of nontrivial valuations on K.[8] Thus there is exactly one prime for each nonzero prime ideal in $\mathcal{O}_K$, for each embedding $K \hookrightarrow \mathbb{R}$, and for each conjugate pair of nonreal embeddings $K \hookrightarrow \mathbb{C}$. The corresponding primes are called finite, real, and complex respectively. An element of K is said to be positive at the real prime corresponding to an embedding $K \hookrightarrow \mathbb{R}$ if it maps to a positive element of $\mathbb{R}$. A real prime of K is said to split in an extension L/K if every prime lying over it is real; otherwise it is said to ramify in L. For example, $\mathbb{Q}[\sqrt{-5}]$ is ramified over $\mathbb{Q}$ exactly at the primes (2), (5), and ∞.

We say that a finite extension L/K is unramified if it is unramified at all the primes of K. This means that each prime ideal in $\mathcal{O}_K$ is unramified in L and each real prime of K remains real (i.e., every real embedding of K extends to a real embedding of L).

Let H be a subgroup of the class group C of K. A finite unramified abelian extension L of K is said to be a ***class field*** for H if the primes ideals of $\mathcal{O}_K$ splitting in L are exactly those in $\tilde{H}$. The next theorem provides an answer to both 0.2 and 0.3 for the unramified abelian extensions of K.

THEOREM 0.4 (FURTWÄNGLER 1907) *A class field exists for each subgroup of C; it is unique, and every finite unramified abelian extension of K arises as the class field of some subgroup of C. If L is the class field of H, then $\mathrm{Gal}(L/K) \approx C/H$, and for every prime ideal $\mathfrak{p}$ of K, $f(\mathfrak{p})$ is the order of the image of $\mathfrak{p}$ in the group C/H.*

The subgroup H of C corresponding to a finite unramified abelian extension L of K is that generated by the primes that split in L. The uniqueness of the class field follows from (0.1).

The class field of the trivial subgroup of C is called the Hilbert class field of K. It is the largest abelian extension L of K unramified at all primes of K (including the infinite primes). The prime ideals that split in it are exactly the principal ones, and $\mathrm{Gal}(L/K) \approx C$. For example, the class number of $K = \mathbb{Q}[\sqrt{-5}]$ is 2, and its Hilbert class field is $K[\sqrt{-1}]$ (ANT, 4.11).

NOTES Theorem 0.4 was conjectured by Hilbert in 1897, and proved by his student Furtwängler in 1907.

Ramified abelian extensions

To generalize Theorem 0.4 to ramified extensions, we need to generalize our notion of an ideal class group. To see how to do this, we should look first at the abelian extensions we do understand, namely, the cyclotomic extensions of $\mathbb{Q}$. Let m be a positive integer that is either odd or divisible by 4, and let ζ_m be a primitive mth root of 1. Recall (ANT, Chapter 6) that $\mathbb{Q}[\zeta_m]$ is an extension of $\mathbb{Q}$ whose Galois group is $(\mathbb{Z}/m\mathbb{Z})^\times$ with $[n]$ acting as $\zeta_m \mapsto \zeta_m^n$. Moreover, with our condition on m, the primes ramifying in $\mathbb{Q}[\zeta_m]$ are exactly the ideals (p) such that $p|m$ and ∞. How can we realize $(\mathbb{Z}/m\mathbb{Z})^\times$ as an ideal class group? We can try mapping an ideal (p) to the class of $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, but this is only possible if $(p, m) = 1$. Thus, let S be the set of prime ideals (p) such that $p|m$, and let I^S be the group of fractional ideals of $\mathbb{Q}$ generated by the prime ideals *not* in S. Each element of I^S can be represented as $(\frac{r}{s})$ with r and s positive integers relatively prime to m, and we map

[8] "place" is more common than "prime". Sometime I'll switch. "spot" is also used.

$(\frac{r}{s})$ to $[r][s]^{-1}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. This gives us a surjective homomorphism $I^S \to (\mathbb{Z}/m\mathbb{Z})^\times$ whose kernel we now describe. Let $m = \prod p^{\mathrm{ord}_p(m)}$, so that

$$\mathbb{Z}/m\mathbb{Z} \simeq \prod_{p|m} \mathbb{Z}/p^{\mathrm{ord}_p(m)} \quad \text{(Chinese remainder theorem)}$$
$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq \prod_{p|m} \left(\mathbb{Z}/p^{\mathrm{ord}_p(m)}\right)^\times.$$

An ideal $(\frac{r}{s})$ with $(r,m) = 1 = (s,m)$ maps to 1 if and only if r and s have the same sign and r and s map to the same element in $\left(\mathbb{Z}/p^{\mathrm{ord}_p(m)}\right)^\times$ for all p dividing m. Note that the condition at ∞ is that $\frac{r}{s} > 0$ and the condition at p is that $\mathrm{ord}_p(\frac{r}{s} - 1) \geq \mathrm{ord}_p(m)$.

To generalize this, define a ***modulus*** of a number field K to be the (formal) product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of an integral ideal $\mathfrak{m}_0$ of $\mathcal{O}_K$ with the product $\mathfrak{m}_\infty$ of certain of the real primes of K. Let $S(\mathfrak{m})$ be the set of primes dividing $\mathfrak{m}$, and define $I^{S(\mathfrak{m})}$ to be the group of fractional ideals generated the prime ideals of $\mathcal{O}_K$ not in $S(\mathfrak{m})$. The ***ray class group*** $C_\mathfrak{m}$ ***with modulus*** $\mathfrak{m}$ is defined to be the quotient of $I^{S(\mathfrak{m})}$ by the subgroup of ideals in $I^{S(\mathfrak{m})}$ generated by an element a such that $a > 0$ at all real primes dividing $\mathfrak{m}_\infty$ and $\mathrm{ord}_\mathfrak{p}(a-1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{m}_0$ (here $\mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)$ is the exponent of $\mathfrak{p}$ in $\mathfrak{m}_0$).

For example, if $\mathfrak{m} = 1$, then $C_\mathfrak{m} = C$, the usual class group. If $\mathfrak{m}$ is the product of the real primes of K (so $\mathfrak{m}_0 = 1$), then $C_\mathfrak{m}$ is the quotient of I by the principal ideals generated by totally positive[9] elements of K, which is the narrow-class[10] group. If $K = \mathbb{Q}$ and $\mathfrak{m} = (m)\infty$, then $C_\mathfrak{m} \simeq (\mathbb{Z}/m\mathbb{Z})^\times$, as in the first paragraph.

Let H be a subgroup of $C_\mathfrak{m}$ for some modulus $\mathfrak{m}$, and let $\tilde{H}$ be its inverse image in $I^{S(\mathfrak{m})}$. An abelian extension L of K, unramified at the primes dividing $\mathfrak{m}$, is said to be a ***class field*** for H if the prime ideals of $\mathcal{O}_K$ not dividing $\mathfrak{m}_0$ that split in L are exactly those in $\tilde{H}$. The following theorem extends Theorem 0.4 to all abelian extensions of K.

THEOREM 0.5 (TAKAGI) *A class field exists for each subgroup of a ray class group $C_\mathfrak{m}$; it is unique, and every finite abelian extension of K arises as the class field of some subgroup of a ray class group. If L is the class field of $H \subset C_\mathfrak{m}$, then $\mathrm{Gal}(L/K) \approx C_\mathfrak{m}/H$ and the prime ideals $\mathfrak{p}$ of K not dividing $\mathfrak{m}$ are unramified in L with residue class degree $f(\mathfrak{p})$ equal to the order of the image of $\mathfrak{p}$ in the group $C_\mathfrak{m}/H$.*

For any finite set S of primes of K, Theorem 0.5 completely solves the problem of determining the sets $\mathrm{Spl}_S(L/K)$ for abelian Galois extensions L/K ramified only at primes in S.

The theorem can be made more precise. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be moduli for K. If $\mathfrak{m}'|\mathfrak{m}$, then the inclusion $I^{S(\mathfrak{m})} \hookrightarrow I^{S(\mathfrak{m}')}$ defines a surjective homomorphism $C_\mathfrak{m} \twoheadrightarrow C_{\mathfrak{m}'}$; if $H \subset C_\mathfrak{m}$ is the inverse image of a subgroup H' of $C_{\mathfrak{m}'}$, then every class field for H' will also be a class field for H. If L is a class field for $H \subset C_\mathfrak{m}$ and H does not arise in this way from a modulus properly dividing $\mathfrak{m}$, then $S(\mathfrak{m})$ consists exactly of the prime ideals ramifying in L. This smallest possible modulus is called the conductor of L/K.

[9] An element a of K is ***totally positive*** if $\sigma(a) > 0$ for every real embedding $\sigma\colon K \to \mathbb{R}$ of K. For example, -5 is totally positive in $\mathbb{Q}[i]$ but not in $\mathbb{Q}$. This seems odd, but the definition is standard according to the books on my bookshelf. It would be better to say that the element "is positive at all real primes" except when the field is totally real.

[10] The hyphen indicates that it is the classes that are narrow, not the group.

Let L be an abelian extension of K. Then, for every sufficiently large modulus $\mathfrak{m}$ divisible only by the primes ramifying in L, L is the class field for the subgroup H of $C_{\mathfrak{m}}$ generated by the classes of primes splitting in L.

For $K = \mathbb{Q}$, the theorem follows from the results proved in ANT, Chapter 6, except for the assertion that every abelian extension of $\mathbb{Q}$ arises as a class field, which is essentially the Kronecker-Weber theorem: every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

EXAMPLE 0.6 The field $\mathbb{Q}[\sqrt{6}]$ has class number 1, and so equals its Hilbert class field. However, its narrow-class group has order 2, and indeed $\mathbb{Q}[\sqrt{6}]$ does possess a quadratic extension, namely, $\mathbb{Q}[\sqrt{-2}, \sqrt{-3}]$, that is unramified over $\mathbb{Q}[\sqrt{6}]$ at all finite primes (but is ramified at both infinite primes).

When Takagi proved Theorem 0.5, he showed only that the groups $C_{\mathfrak{m}}/H$ and $\mathrm{Gal}(L/K)$ are isomorphic — he didn't construct a specific isomorphism. There is an obvious map $I^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$, namely, that send a prime ideal $\mathfrak{p}$ in $S(\mathfrak{m})$ to the corresponding Frobenius element in $\mathrm{Gal}(L/K)$. The theorem of Frobenius shows that this is surjective, and the problem is to show that it factors through $C_{\mathfrak{m}}$ for some $\mathfrak{m}$, i.e., that the map admits a modulus. Artin conjectured this is 1923, and succeeded in proving it in 1927 (see below).

EXAMPLE 0.7 Let $d = p_1^* \cdots p_t^*$, where the p_i are distinct odd primes and $p_i^* = (-1)^{\frac{p-1}{2}} p_i$, as before. The field $K = \mathbb{Q}[\sqrt{d}]$ is ramified exactly at the prime ideals $(p_1), \dots, (p_t)$. Consider $K[\sqrt{p_i^*}]$. It contains $\mathbb{Q}[\sqrt{p_1^* \cdots p_{i-1}^* p_{i+1}^* \cdots p_t^*}]$, which is unramified over (p_i), and so (p_i) cannot be totally ramified in $K[\sqrt{p_i^*}]$. As p_i ramifies in $K/\mathbb{Q}$, it follows that the prime above (p_i) in K does not ramify in $K[\sqrt{p_i^*}]$. No other prime ramifies, and so $K[\sqrt{p_i^*}]$ is unramified over K. From Kummer theory (FT 5.29), we find that

$$L \stackrel{\text{def}}{=} K[\sqrt{p_1^*}, \sqrt{p_2^*}, \dots, \sqrt{p_{t-1}^*}]$$

has degree 2^{t-1} over K, and $\mathrm{Gal}(L/K) \approx (\mathbb{Z}/2\mathbb{Z})^{t-1}$. Let C_∞ be the narrow class group of K. The above construction shows that $(C_\infty : C_\infty^2) \geq 2^{t-1}$. In fact, with only a little more effort, one can prove the following statement:

> Let K be a quadratic extension of $\mathbb{Q}$ in which t finite primes ramify. Then $(C_\infty : C_\infty^2) = 2^{t-1}$ (Koch 1992, Theorem 2.114).

This result was known to Gauss (by different methods, and in a different language). In particular, we see that by using class field theory, it is easy to construct quadratic extensions of $\mathbb{Q}$ such that $(C : C^2)$ is very large. By contrast, as of 1991, no quadratic field was known with $(C : C^3) > 3^6$. All methods of constructing elements of order 3 in the class groups of quadratic number fields seem to involve elliptic curves.

NOTES The ray class groups $C_{\mathfrak{m}}$ were introduced by Weber in 1897. Theorem 0.5 was conjectured by Hilbert and Weber, and proved by Takagi in a series of papers published between 1915 and 1922 — see especially his talk[11] at the 1920 International Congress, where he states his results almost exactly as we have.

[11] Available in his collected works.

Density theorems

Let m be an integer ≥ 2. Let a be an integer prime to m, and consider the sequence

$$\ldots, a-m, a, a+m, a+2m, a+3m, \ldots, a+km, \ldots. \tag{5}$$

This sequence depends only on a mod m, and so there are $\varphi(m) \overset{\text{def}}{=} |(\mathbb{Z}/m\mathbb{Z})^\times|$ distinct sequences. Dirichlet showed that the prime numbers are equidistributed among these sequences, i.e., the set of prime numbers in each sequence has density $1/\varphi(m)$ in the set of all prime numbers.

We want to interpret this in terms of Galois groups. Let L/K be a finite extension of number fields with Galois group G. Recall (ANT, Chapter 8) that for every prime ideal $\mathfrak{P}$ in $\mathcal{O}_L$, there exists a Frobenius element σ of G such that

- $\sigma\mathfrak{P} = \mathfrak{P}$, and
- for all $\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^q \bmod \mathfrak{P}$, where q is the number of elements in the residue class field $\mathcal{O}_K/\mathfrak{p}$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

When $\mathfrak{P}$ is unramified over $\mathfrak{p}$, the element σ is uniquely determined by these conditions — it is then denoted $(\mathfrak{P}, L/K)$. If $\mathfrak{P}'$ second prime ideal of $\mathcal{O}_L$ dividing $\mathfrak{p}$, then $\mathfrak{P}' = \tau\mathfrak{P}$ for some $\tau \in G$, and

$$(\mathfrak{P}', L/K) = (\tau\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}.$$

Therefore, for every prime ideal $\mathfrak{p}$ of K unramified in L,

$$\{(\mathfrak{P}, L/K) \mid \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}\}$$

is a full conjugacy class in G — we denote it by $(\mathfrak{p}, L/K)$. When G is commutative, the conjugacy classes consist of a single element, and so $(\mathfrak{p}, L/K)$ can be regarded as an element of G.

Now consider $\mathbb{Q}[\zeta_m]/\mathbb{Q}$, where m is either an odd integer > 1 or a positive integer divisible by 4. Recall that $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ with $[n]$ acting as $\zeta \mapsto \zeta^n$. A prime (p) not dividing m is unramified in $\mathbb{Q}[\zeta_m]$, and $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q}) = [p]$ (as one would expect). Now let $\tau = [a] \in \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$. Then $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q}) = \tau$ if and only if p lies in the sequence (5), and so Dirichlet's theorem says that

$$\{p \mid (p, \mathbb{Q}[\zeta_m]/\mathbb{Q}) = \tau\}$$

has density $1/\varphi(m)$ in the set of all prime numbers. For cyclotomic extensions of $\mathbb{Q}$, this proves the conjecture of Frobenius (p. 3) .

In order to prove his theorem on primes in arithmetic progressions, Dirichlet introduced what are now called Dirichlet L-series. Let $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ (i.e., a homomorphism). Then the Dirichlet L-series attached to χ is

$$L(s,\chi) = \prod_{(p,m)=1,\ p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}} = \sum_{(n,m)=1,\ n>0} \chi(n)n^{-s}.$$

When χ is the trivial (principal) character, this becomes the Riemann zeta function except that finitely many factors are missing. Dedekind extended the notion of a zeta function to every number field,

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}} = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \mathbb{N}\mathfrak{a}^{-s}, \quad \mathbb{N}\mathfrak{a} = (\mathcal{O}_K\colon\mathfrak{a}),$$

and Weber extended the notion of an L-series to a character χ of any ray class group $C_{\mathfrak{m}}$,

$$L(s,\chi) = \prod_{(\mathfrak{p},\mathfrak{m})=\mathcal{O}_K} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}} = \sum_{(\mathfrak{a},\mathfrak{m})=1} \chi(\mathfrak{a})\mathbb{N}\mathfrak{a}^{-s}.$$

Weber showed that $L(s,\chi)$ can be analytically continued to a meromorphic function on the whole complex plane, and is even holomorphic when χ is not the trivial character.

The function on whole complex plane is still denoted $L(s,\chi)$, and is called a Dirichlet or Weber L-function.

Artin L-functions

Let L/K be a finite Galois extension with Galois group G, and let S be a finite set of finite prime ideals of $\mathcal{O}_K$ including those that ramify in L. Let

$$\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$$

be a representation of G (i.e., a homomorphism of groups). From each prime ideal not in S, we obtain a conjugacy class $(\mathfrak{p}, L/\mathbb{Q})$ of Frobenius elements of G, which ρ maps into a conjugacy class $\Phi_{\mathfrak{p}}(\rho)$ in $\mathrm{GL}_n(\mathbb{C})$. The elements of $\Phi_{\mathfrak{p}}(\rho)$ are diagonalizable (Maschke's theorem, GT 7.5), and $\Phi_{\mathfrak{p}}(\rho)$ is determined by the common characteristic polynomial $\det(I - \Phi_{\mathfrak{p}}(\rho)T)$ of its elements. Artin defined

$$L_S(s,\rho) = \prod_{\mathfrak{p}\notin S} \frac{1}{\det(I-\Phi_{\mathfrak{p}}(\rho)\,(\mathbb{N}\mathfrak{p})^{-s})}, \quad s\in\mathbb{C}.$$

This product converges to a holomorphic function in some right half plane in $\mathbb{C}$. Such functions are called ***Artin L-functions.***

Note that a 1-dimensional representation of G is just a character $\chi\colon G\to\mathbb{C}^\times$, and that

$$L_S(s,\chi) = \prod_{\mathfrak{p}\notin S} \frac{1}{1-\chi(\mathfrak{p})\,(\mathbb{N}\mathfrak{p})^{-s}}.$$

An elementary lemma on Dirichlet series implies that the factors $\frac{1}{\det(I-\Phi_{\mathfrak{p}}(\rho)(\mathbb{N}\mathfrak{p})^{-s})}$ are uniquely determined by the holomorphic function $L_S(s,\rho)$. If ρ is injective, then

$$\mathrm{Spl}_S(L/K) = \{\mathfrak{p} \mid \Phi_{\mathfrak{p}}(\rho) = \{I\}\},$$

and so the function $L_S(s,\rho)$ determines $\mathrm{Spl}_S(L/K)$. For nonabelian extensions, rather than studying $\mathrm{Spl}_S(L/K)$ directly, it is more useful to study the Artin L-function $L_S(s,\rho)$.

NOTES For a historical introduction to L-series, especially Artin L-series, see Noah Snyder, Artin's L-functions: A Historical Approach, 2002, here.

The Artin map

Recall that, for a cyclotomic extension $\mathbb{Q}[\zeta_m]$ of $\mathbb{Q}$, there is an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q}).$$

sending $[p]$ to $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q})$. A character χ of $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ defines by composition a character χ' of $(\mathbb{Z}/m\mathbb{Z})^\times$. Since

$$\chi'(p) = \chi\left((p, \mathbb{Q}[\zeta_m]/\mathbb{Q})\right),$$

we have

$$L_S(s, \chi) = L_S(s, \chi').$$

Thus, in this case, the Artin L-series $L_S(s, \chi)$ is a Dirichlet L-series.

Could something similar be true more generally? For example, is the Artin L-series defined by a one-dimensional representation a Weber L-series? Let L/K be an abelian extension with Galois group G, and let S be a finite set of primes of K including those that ramify in L. Let I^S be the group of fractional ideals of K generated by the prime ideals not in S. Then I^S is the free group, and so the map $\mathfrak{p} \mapsto (\mathfrak{p}, L/K)$ extends uniquely to a homomorphism

$$I^S \to \mathrm{Gal}(L/K), \tag{6}$$

which is surjective by the Frobenius density theorem 0.1. If there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ such that this homomorphism factors through $C_\mathfrak{m}$, then a character χ of $\mathrm{Gal}(L/K)$ will define a character χ' of $C_\mathfrak{m}$ by composition, and

$$L_S(s, \chi) = L_S(s, \chi'),$$

i.e., the Artin L-series $L_S(s, \chi)$ will be a Weber L-series.

Artin, of course, conjectured that there does exist such a modulus, but he was unable to prove it until he had seen Chebotarev's proof of his density theorem, at which time he obtained the following more complete theorem. Before stating it, we need some notation. For a modulus $\mathfrak{m}$, let $P_\mathfrak{m}$ be the kernel of $I^{S(\mathfrak{m})} \to C_\mathfrak{m}$, so that $P_\mathfrak{m}$ consists of the principal ideals defined by elements satisfying certain positivity and congruence conditions depending on $\mathfrak{m}$. For an extension L of K, let $S'(\mathfrak{m})$ denote the primes of L lying over the primes in $S(\mathfrak{m})$. There is a norm map $\mathrm{Nm}\colon I^{S'(\mathfrak{m})} \to I^{S(\mathfrak{m})}$ (ANT, p. 68) such that $\mathrm{Nm}(\mathfrak{P}) = \mathfrak{p}^f$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ and f is the residue class degree. Note that

$$(\mathrm{Nm}(\mathfrak{P}), L/K) = (\mathfrak{p}^f, L/K) \overset{\text{def}}{=} (\mathfrak{p}, L/K)^f = 1,$$

and so $\mathrm{Nm}(I^{S'(\mathfrak{m})})$ is contained in the kernel of $I^{S(\mathfrak{m})} \to C_\mathfrak{m}$.

THEOREM 0.8 (ARTIN 1927) *Let L be an abelian extension of K, and let S be the set of primes that ramify in L. Then, for some modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, the homomorphism*

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K)\colon I^S \to \mathrm{Gal}(L/K)$$

factors through $C_\mathfrak{m} \overset{\text{def}}{=} I^{S(\mathfrak{m})}/P_\mathfrak{m}$, and defines an isomorphism

$$I^{S(\mathfrak{m})}/P_\mathfrak{m} \cdot \mathrm{Nm}(I^{S'(\mathfrak{m})}) \to \mathrm{Gal}(L/K).$$

In particular, the prime ideals splitting in L are exactly those in the subgroup

$$\tilde{H} = P_\mathfrak{m} \cdot \mathrm{Nm}(I^{S'(\mathfrak{m})})$$

of I^S.

The homomorphism $\psi_{L/K}\colon C_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ in the theorem is called the ***Artin map (or reciprocity) map***. As Artin noted, the theorem includes all known reciprocity laws (see Chapter VIII), and should be seen as the correct generalization of these laws to a field K without roots of 1.

Note that if the Artin map were not surjective, then there would be a proper extension of K in which every prime of K outside S splits. Analytic methods, specifically, the density theorem of Frobenius, show that no such extension exists, but it is difficult to prove this algebraically (see Chapter VII).

Since the Artin L-functions of one-dimensional representations are Weber L-series, they can be extended to meromorphic functions on the entire complex plane. Artin conjectured that every character of a finite group is a $\mathbb{Z}$-linear combination of characters that are close to being abelian, and showed that this conjecture implies that all Artin L-series extend to meromorphic functions on the entire complex plane. This was proved by Brauer in 1946.

Artin conjectured that, if ρ is a nontrivial irreducible representations, then $L(s,\rho)$ is holomorphic on the entire complex plane. He remarked that the proof of this conjecture will require entirely new methods. The conjecture, now known as the ***Artin conjecture***, is one of the most important in number theory. After Theorem 1.8, the Artin L-functions of one-dimensional representations are Weber L-functions, and so the Artin conjecture follows from Weber's results. In general, as Langlands explained, the Artin L-functions of irreducible representations should be cuspidal automorphic L-functions, which are known to be holomorphic. For two-dimensional representations, the Artin conjecture has mostly been proved (Artin, Langlands, Tunnell, Taylor,...). See Taylor, Richard, Pacific J. Math. 181, 1997, 337–347, and subsequent papers.

For function fields, Weil proved Artin's conjecture at the same time as he proved the Riemann hypothesis for curves over finite fields, and he considered it the more important result.

Local class field theory and infinite extensions

An abelian extension L of K defines an abelian extension L^v/K_v of the completion K_v of K at a prime v. Conversely, every finite extension of K_v comes from an extension of the same degree of K (ANT, 7.62). Thus, it should not be surprising that the classification of the abelian extensions of a number field contains within it a classification of the abelian extensions of a local field. Hasse (1930)[12] made this explicit.

THEOREM 0.9 *Let K be a finite extension of $\mathbb{Q}_p$. For every finite abelian extension L of K, $\mathrm{Nm}(L^\times)$ is a subgroup of finite index in $K^\times$, and the map $L \mapsto \mathrm{Nm}(L^\times)$ is an order-reversing bijection from the set of finite abelian extensions of K to the set of subgroups of $K^\times$ of finite index.*

Thus, by 1930, the abelian extensions of both number fields and local fields had been classified. However, there were three aspects of the theory that were considered unsatisfactory.

- ◇ As local fields are simpler than global fields, one expects to prove first a statement locally and then deduce it globally, not the reverse. At the very least, there should be a purely local proof of local class field theory.

[12] H. Hasse, Die Normenresttheorie relative-Abelscher Zahlkörper als Klassenkörper im Kleinen, J. für Mathematik (Crelle) 162 (1930), 145–154.

- ◇ The main statements of class field theory are algebraic, and so they should admit a purely algebraic proof.
- ◇ Theorem 0.8 classifies the abelian extensions of a number field K whose conductor divides a fixed modulus. To include other abelian extensions, one will have to keep enlarging the conductor. So this raises the question of giving a uniform description of all abelian extensions simultaneously or, in other words, a class field theory for infinite abelian extensions.

Chevalley solved all three problems. Let K^{ab} denote the composite of all finite abelian extensions of K. The full statement of local class field theory is that, for every p-adic field K, there exists a well-defined homomorphism $\phi\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ (now called the ***local Artin map***) that induces an isomorphism

$$K^\times/\mathrm{Nm}(L^\times) \to \mathrm{Gal}(L/K)$$

for every finite abelian extension L of K; moreover, all (open) subgroups of finite index are norm groups. This suggests that it might be possible to define a global Artin map whose components are the local Artin maps in the sense that the following diagram commutes for all primes v of K:

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ \prod_v K_v^\times & \xrightarrow{??\phi??} & \mathrm{Gal}(K^{\mathrm{ab}}/K). \end{array}$$

One problem with this is that $\prod_v K_v^\times$ is not locally compact. A product of compact groups is compact, but that the similar statement is false for locally compact groups, and the groups $K_v^\times$ are only locally compact. In fact $\prod_v K_v^\times$ is too big for there exist a ϕ. Chevalley solved this problem by defining the group $\mathbb{I}_K$ of idèles of K to be the subgroup of $\prod_v K_v^\times$ consisting of families (a_v) such that $a_v \in \mathcal{O}_v^\times$ for almost all nonarchimedean primes. When endowed with the topology for which $\prod_{v|\infty} K_v^\times \times \prod_{v \text{ finite}} \mathcal{O}_v^\times$ is an open subgroup, $\mathbb{I}_K$ becomes a locally compact group. Embed $K^\times$ in $\mathbb{I}_K$ as the diagonal subgroup.

In the Chevalley approach to class field theory, one first proves local class field theory directly. Then one defines a global Artin map $\phi_K\colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ whose components are the local Artin maps, and shows that $K^\times$ is contained in the kernel of ϕ_K and that the homomorphism

$$\mathbb{I}_K/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

induced by ϕ is surjective with kernel equal to the identity connected component of the group $\mathbb{I}_K/i(K^\times)$. In other words, the homomorphism ϕ_K fits into a commutative diagram

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

for all primes v of K, and ϕ_K induces an isomorphism

$$\boldsymbol{C}_K/\boldsymbol{C}_K^\circ \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K), \quad \boldsymbol{C}_K \overset{\text{def}}{=} \mathbb{I}_K/K^\times.$$

This statement relates to Theorem 0.9 in the following way: there is a canonical isomorphism $\boldsymbol{C}/\boldsymbol{C}^\circ \simeq \varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$, and for every finite abelian extension L of K and sufficiently large modulus $\mathfrak{m}$, there is a commutative diagram

$$\begin{array}{ccc} \boldsymbol{C} & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow{\scriptstyle \tau\mapsto\tau|L} \\ C_{\mathfrak{m}} & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

By 1950 the local Artin map could be characterized locally, or it could be described as the local component of the global Artin map, but it was not until 1965 that Lubin and Tate found an explicit local description of it.

NOTES In the number field case, the Artin map $C \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is surjective with kernel the identity component of C. In the function field case, it is injective but not surjective. Weil has suggested that interpreting the entire idèle class group of a number field as a Galois group may be the key to proving the Riemann hypothesis (see p. 180).

Central simple algebras

A central algebra over a field K is an algebra A whose centre is K and has finite dimension over K; the algebra is simple if it has no nonzero proper two-sided ideals. For example, the matrix algebra $M_n(K)$ is a central simple algebra over K. The first interesting example of a central simple algebra, namely, the quaternion algebra over $\mathbb{R}$, was found by Hamilton in 1843. It is spanned by $1, i, j, ij$ over $\mathbb{R}$, and its multiplication is determined by

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji.$$

Let K be a field. In 1906, Dickson showed how to attach a central simple algebra $(L/K, \sigma, a)$ over K to a cyclic extension[13] L/K of K, a generator σ for $\mathrm{Gal}(L/K)$, and a nonzero element a of K. As an L-vector space, the algebra is spanned by elements $1, \alpha, \dots, \alpha^{n-1}$, where $n = [L\colon K]$, and its multiplication is determined by

$$\alpha^n = a, \quad \alpha c = (\sigma c)\alpha \text{ for } c \in L.$$

Thus, $(L/K, \sigma, a)$ is a central simple algebra containing L as a maximal subfield in which the action of σ on L is induced by an inner automorphism.

Brauer and Noether showed how to describe central simple algebras by factor systems, which, once group cohomology had been defined, were recognized to be 2-cocycles.

In 1907, Wedderburn showed that every central simple algebra over k is isomorphic to a matrix algebra over a central division algebra. Brauer defined two central simple algebras over K to be similar if they were isomorphic to matrix algebras over the same division algebra, and he showed that the similarity classes form a group under tensor product (now called the ***Brauer group*** of K). Thus, the problem of classifying the central simple algebras over a field K became that of determining the Brauer group $\mathrm{Br}(K)$ of the field.

Results of Frobenius determine the Brauer group of $\mathbb{R}$, and Hasse determined the Brauer group of a nonarchimedean local field. In 1932 Albert, Brauer, Hasse, and Noether showed that every division algebra over a number field is cyclic, and determined the Brauer group

[13] That is, a Galois extension with cyclic Galois group.

of such a field. This is a fundamental theorem of the same depth as the main theorems of class field theory, and, in these notes, will be proved simultaneously with them.

Brauer groups have many applications, for example, to the representation theory of finite groups, which is what interested Brauer, and to the classification of semisimple algebraic groups over number fields.

NOTES The story of the determination of the Brauer group of a number field is well told in Fenster and Schwermer 2005 and Roquette 2005. I quote from the MR review of the first of these:

> In February, 1931, Hasse began a joint effort with Richard Brauer and Emmy Noether to classify all division algebras over algebraic number fields. They achieved this in a paper that was published in early 1932. The young A. A. Albert was also working on the problem at the same time. He had been in correspondence with Hasse during 1930–1931 and he had come close to resolving the problem. Some of his remarks to Hasse had been helpful in the Brauer-Hasse-Noether solution. Within weeks of that event, Albert found an alternate proof, which utilized a suggestion from Hasse.

Cohomology

For a group G and a G-module M, there are homology groups $H_r(G,M)$, $r \geq 0$, and cohomology groups $H^r(G,M)$, $r \geq 0$. Short exact sequences of G-modules give long exact sequences of homology and cohomology groups. Tate showed that, when G is finite, these long exact sequences can be spliced together to give a very long sequence. More precisely, the groups

$$H_T^r(G,M) \stackrel{\text{def}}{=} \begin{cases} H^r(G,M) & r > 0 \\ M^G/\operatorname{Nm}(M) & r = 0 \\ \operatorname{Ker}(\operatorname{Nm})/I_G M & r = -1 \\ H_{-r-1}(G,M) & r < -1, \end{cases}$$

defined for all $r \in \mathbb{Z}$, have this property. In particular,

$$H_T^{-2}(G,\mathbb{Z}) \stackrel{\text{def}}{=} H_1(G,\mathbb{Z}) \simeq G^{\text{ab}} \text{ (largest abelian quotient of } G).$$

Let C be a G-module such that $H^2(H,C)$ is cyclic of order $|H|$ for all subgroups H of G. If $H^1(G,C) = 0$, then Tate showed that the choice of a generator for $H^2(G,C)$ determines a family of isomorphisms

$$H_T^r(G,M) \to H_T^{r+2}(G, M \otimes C), \quad \text{all } r \in \mathbb{Z}.$$

For a Galois extension L/K of local fields with Galois group G, the calculation of the Brauer group of K shows that $H^2(G,L^\times)$ is cyclic of order $|G|$ and that it has a canonical generator. Since Hilbert's Theorem 90 shows that $H^1(G,L^\times) = 0$, Tate's theorem provides us with canonical isomorphisms

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G,L^\times)$$

for all $r \in \mathbb{Z}$. When $r = -2$, this becomes an isomorphism

$$G^{\text{ab}} \xrightarrow{\simeq} K^\times/\operatorname{Nm}(L^\times)$$

whose inverse is the local Artin map. A similar argument applies for global fields with the group of idèles modulo principal idèles playing the role of the multiplicative group of the field.

NOTES I quote from Mac Lane 1978, p. 17:

> Mac Lane recalls that Artin (about 1948) pointed out in conversations that the cohomology of groups should have use in class field theory. Hochschild (1950) and Hochschild and Nakayama (1952) showed how the Brauer group arguments of class field theory could be replaced by cohomological arguments. In 1952, Tate proved that the homology and cohomology groups for a finite group G could be suitably combined in a single long exact sequence. He used this sequence, together with properties of transfer and restriction, to give an elegant reformulation of class field theory.

Explicit construction of class fields (Hilbert's 12th problem)

The Kronecker-Weber theorem shows that every abelian extension of $\mathbb{Q}$ is contained in the field generated by a special value $\zeta = e^{2\pi i/m}$ of the exponential function. A later theorem (the Kronecker Jugentraum) shows that every abelian extension of an imaginary quadratic number field is contained in the field generated by certain special values of the elliptic modular functions. In the 12th of his famous problems, Hilbert asked if the abelian extensions of other number fields can be generated by the special values of explicit holomorphic functions.

The functions that generalize elliptic modular functions are well understood, as are the arithmetic properties of their special values — this is the theory of complex multiplication and of Shimura varieties — but they are useful only for constructing abelian extension of CM fields, and even for these fields they only give the abelian extensions that (roughly speaking) don't come from an abelian extension of the totally real subfield (except $\mathbb{Q}$). On the other hand, conjectures of Stark provide candidates for generators of abelian extensions of totally real fields.

Explicit class field theory

The proofs of the theorems in class field theory are elegant but abstract. For example, the original local proofs of local class field theory show only that there exists a unique Artin map $\phi\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with certain properties, but leave open the question of an explicit description of the map and of K^{ab}. Fortunately, in this case the theory of Lubin and Tate, which we explain in Chapter I, gives an elegant answer to this question.

Much work has been devoted to finding explicit descriptions of the other maps and objects of class field theory. This topic is largely ignored in the current version of the notes.

Computational class field theory.

Beyond finding explicit descriptions of the maps and objects of class field theory, one can ask for algorithms to compute them. For this topic, I can only refer the reader to Cohen 2000.

Nonabelian class field theory

In the same talk at the ICM 1920 in which he announced his proof of the main theorems of abelian class field theory to the world, Takagi raised the question of a nonabelian class field theory:

> En m'arrêtant ici, je me permets d'attirer votre attention sur un problème important de la théorie des nombres algébriques: à savoir, rechercher s'il est possible de définir la classe d'idéaux d'un corps algébrique de telle manière que les corps supérieur relativement normal mais non abélian puisse être caractérisé par le groupe correspondant de classes d'idéaux du corps de fond.[14]

The norm limitation theorem shows that the subgroups of the (ray) class groups do not distinguish between an extension field and its largest abelian subextension.

For several decades it was unclear what form a nonabelian class field theory should take, or even whether it existed. In 1946, Artin speculated that finding the correct statements was the *only* problem: once we knew what they were, it would be possible to deduce them from abelian class field theory (A Century of Mathematics in America, Part II, (Peter Duren, ed.), 1989, p. 312). Weil relates that, a year later, Artin said that he had lost faith in the existence of a nonabelian class field theory (Weil, A., Œuvres, Vol. III, p. 457.)

Instead of studying the set $\mathrm{Spl}_S(L/K)$, we should study the Artin L-series $L(s,\rho)$ of a representation ρ of $\mathrm{Gal}(L/K)$. The problem of describing the sets $\mathrm{Spl}_S(L/\mathbb{Q})$ then becomes that of describing the set of analytic functions that arise in this fashion. Langlands has constructed a class of L-series, called ***automorphic L-series,*** and conjectures[15] that each $L_S(s,\rho)$ is automorphic, and specifies which automorphic L-series arise in this fashion. Thus, the conjecture answers the original question for all finite Galois extensions of $\mathbb{Q}$. For $n = 1$ (so G is abelian) and all K, Artin proved all Artin L-series are automorphic—this was his motivation for proving Theorem 0.8. As noted earlier, for $n = 2$, the conjecture has been proved in most cases.

In 1967 Langlands stated his conjectural[16] functoriality principle, which includes a nonabelian class field theory as a special case. For a local field K, this can be stated as follows. The Weil group W_K of K is defined to be the subgroup of $\mathrm{Gal}(K^{\mathrm{al}}/K)$ consisting of the elements that act on the residue field as an integer power of the Frobenius element. The local Artin map in abelian local class field theory can be regarded as an isomorphism ϕ_K from $K^\times$ onto the largest abelian quotient W_K^{ab} of W_K. Langlands conjectures that the homomorphisms from W_K into $\mathrm{GL}_n(\mathbb{C})$ correspond to certain representations of $\mathrm{GL}_n(K)$. For $n = 1$, the representations of $\mathrm{GL}_1(K) = K^\times$ are just characters, and the correspondence is given by composition with ϕ_K. For $n > 1$ the representations of $\mathrm{GL}_n(K)$ are typically infinite dimensional.

On the automorphic side, let $\mathcal{A}_n(K)$ be the set of equivalence classes of irreducible representations of $\mathrm{GL}_n(K)$ on complex vector spaces for which the stabilizer of each vector is open. On the Galois side, let $\mathcal{G}_n(K)$ be the set of equivalence classes of pairs (r, N) where r is a semisimple representation of W_K on an n-dimensional complex vector space V, trivial on an open subgroup, and N is a nilpotent endomorphism of V such that conjugating N by $r(\sigma)$ ($\sigma \in W_K$) multiplies it by the absolute value of $\varphi_K^{-1}(\sigma)$. The local Langlands

[14] In stopping here, I allow myself to draw your attention to an important problem in the theory of algebraic numbers, namely, whether it is possible to define the ideal classes of an algebraic number field in such a way that the nonabelian normal extension fields can be characterized by the corresponding group of ideal classes of the base field.

[15] Note the similarity to the Taniyama conjecture—in fact, both are special cases of a much more general conjecture.

[16] In a letter to Weil, and later (to the rest of us) in *Problems in the theory of automorphic forms* (1970). For an engaging introduction to these works, see Casselman 2001. TEXed versions of Langlands's works, including the above two, can be found at `http://publications.ias.edu/rpl/`.

conjecture for K asserts that there is a family of bijections $(\sigma_n)_{n\geq 1}$,

$$\pi \mapsto \sigma_n(\pi)\colon \mathcal{A}_n(K) \to \mathcal{G}_n(K),$$

such that

(a) the determinant of $\sigma_n(\pi)$, viewed as a character of W_K, corresponds under φ_K to the central character of π;

(b) the map σ_n preserves L-factors and ε-factors of pairs of π's (as defined by Jacquet, Piatetskii-Shapiro, and Shalika on the automorphic side, and by Langlands and Deligne on the Galois side);

(c) for $\chi \in \mathcal{A}_1(K)$, $\sigma_n(\pi \otimes (\chi \circ \det)) = \sigma_n(\pi) \otimes \sigma_1(\chi)$;

(d) σ_n commutes with passage to the contragredient, $\pi \mapsto \pi^\vee$.

For each K, Henniart showed there exists at most one such family. The conjecture itself was proved by Harris and Taylor (2001). Several months later, Henniart (2000) found a simpler proof.

A final remark

Recall the following theorem of Dedekind (ANT, 3.41).

THEOREM 0.10 *Let A be a Dedekind domain with field of fractions K, and let B be the integral closure of A in a finite separable extension L of K. Let $L = K[\alpha]$ with $\alpha \in B$, and let $f(X)$ be the minimal polynomial of α over K. The following conditions on a prime ideal $\mathfrak{p}$ of A are equivalent:*

(a) *$\mathfrak{p}$ does not divide $\operatorname{disc}(f(X))$;*

(b) *$\mathfrak{p}$ does not ramify in B and $A_{\mathfrak{p}}[\alpha]$ is the integral closure of $A_{\mathfrak{p}}$ in L (here $A_{\mathfrak{p}} = \{a/b \mid b \notin \mathfrak{p}\}$);*

(c) *there is a factorization*

$$f(X) \equiv f_1(X)\cdots f_g(X) \mod \mathfrak{p}$$

with the f_i distinct, monic, and irreducible modulo $\mathfrak{p}$.

When these conditions hold, the factorization of $\mathfrak{p}$ into prime ideals in L is

$$\mathfrak{p}B = (\mathfrak{p}, f_1(\alpha))\cdots(\mathfrak{p}, f_g(\alpha)).$$

Thus class field theory is really about polynomials in one variable with coefficients in a number field and their roots: abelian extensions of K correspond to monic irreducible polynomials $f(X) \in K[X]$ such that the permutations of the roots of $f(X)$ giving field automorphisms commute; Dedekind's theorem shows that the factorization of all but finitely many prime ideals of K in an abelian extension L corresponds to the factorization of a polynomial over a finite field.

The approach taken in these notes

In these notes we prove the main theorems of local and global class field theory following the algebraic/cohomological approach of Chevalley (1940, 1954), Artin and Tate (1961), and Tate (1952, 1967). The cohomological approach makes plain the relation between the fundamental theorems of class field theory and the calculation of the Brauer group. With hindsight, one can see that cohomological calculations have been implicit in class field theory since at least the papers of Takagi.

However, there are other approaches to class field theory, and when it sheds additional light I have not hesitated to include more than one proof. For example, I explain how the use of analysis can be used to simplify some steps of the proof of the fundamental theorem in the global case. Moreover, I explain how (following Lubin and Tate) the theory of formal group laws can be used to make the results of local class field theory more explicit and satisfactory.

Although it is possible to prove the main theorems in class field theory using neither analysis nor cohomology, there are major theorems that cannot even be stated without using one or the other, for example, theorems on densities of primes, or theorems about the cohomology groups associated with number fields. In recent years, the cohomological results have been crucial in many of the applications of class field theory.[17]

The heart of the course is the odd numbered chapters. Chapter II, which is on the cohomology of groups, is basic for the rest of the course, but Chapters IV, VI, and VIII are not essential for reading Chapters III, V, and VII. Except for its first section, Chapter I can be skipped by those wishing to get to the main theorems of global class field theory as rapidly as possible.

EXERCISE 0.11 Complete the proof that the quadratic reciprocity law allows one to describe the sets $\mathrm{Spl}_S(L/\mathbb{Q})$ with $L/\mathbb{Q}$ quadratic.

EXERCISE 0.12 Prove that $\mathbb{Q}[\sqrt{-5}, \sqrt{-1}]$ is the Hilbert class field of $\mathbb{Q}[\sqrt{-5}]$.

EXERCISE 0.13 Prove that the map $I^S \to (\mathbb{Z}/m\mathbb{Z})^\times$ defined on p. 4 has the kernel described and hence induces an isomorphism $C_{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^\times$.

EXERCISE 0.14 Prove the statements in Example 0.6.

EXERCISE 0.15 Let $L = \mathbb{Q}[\sqrt{-1}, \sqrt{-5}]$. Then $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where σ fixes $\mathbb{Q}[\sqrt{-1}]$, τ fixes $\mathbb{Q}[\sqrt{-5}]$, and $\sigma\tau$ fixes $\mathbb{Q}[\sqrt{5}]$.

(a) Show that only $2, 5, \infty$ ramify in L.

(b) Compute $(p, L/\mathbb{Q})$ for all $p \neq 2, 5$.

(c) Let $\mathfrak{m} = (20)\infty$. Show that $p \mapsto (p, L/\mathbb{Q})$ defines an isomorphism $C_{\mathfrak{m}}/H \to \mathrm{Gal}(L/\mathbb{Q})$ for some $H \subset C_{\mathfrak{m}}$, and find H.

Hint: Show $L \subset \mathbb{Q}[\zeta]$, where ζ is a primitive 20th root of 1.

[17] For example, according to Google Scholar, my book *Arithmetic Duality Theorems* has been cited by 1014 research articles (since they started counting). MR lists 430 (since about 2000).

I will tell you a story about the Reciprocity Law. After my thesis, I had the idea to define L-series for non-abelian extensions. But for them to agree with the L-series for abelian extensions, a certain isomorphism had to be true. I could show it implied all the standard reciprocity laws. So I called it the General Reciprocity Law and tried to prove it but couldn't, even after many tries. Then I showed it to the other number theorists, but they all laughed at it, and I remember Hasse in particular telling me it couldn't possibly be true. Still, I kept at it, but nothing I tried worked. Not a week went by — *for three years!*— that I did not try to prove the Reciprocity Law. It was discouraging, and meanwhile I turned to other things. Then one afternoon I had nothing special to do, so I said, "Well, I try to prove the Reciprocity Law again." So I went out and sat down in the garden. You see, from the very beginning I had the idea to use the cyclotomic fields, but they never worked, and now I suddenly saw that all this time I had been using them in the wrong way — and in half an hour I had it.

Emil Artin, as recalled by Mattuck (in Recountings: Conversations with MIT Mathematicians 2009).

Why was it so hard for other mathematicians to believe it? Reciprocity laws at the time were intimately connected to power residue symbols. Actually Euler had formulated the quadratic reciprocity law in the correct way (namely that the symbol (Δ/p) only depends on the residue class of p modulo Δ), but Legendre's formulation prevailed. I'm pretty sure that Hasse would not have laughed had Artin shown him right away that the general reciprocity law is equivalent to the known power reciprocity laws. Hasse did not have to wait for Chebotarev's density law to be convinced that Artin was right — by the time Chebotarev's ideas appeared it was clear that Artin must have been right. And, by the way, Chebotarev's article did a lot more than prove the importance of the Frobenius element — it provided Artin with the key idea for the proof of his reciprocity law, namely Hilbert's technique of abelian crossings.

Let me also add that Felix Bernstein conjectured a reciprocity law in 1904 that is more or less equivalent to Artin's law in the special case of unramified abelian extensions. Its technical nature shows that it was not at all easy to guess a simple law such as Artin's from the known power reciprocity laws.

Franz Lemmermeyer mo243590.

Chapter I

Local Class Field Theory: Lubin-Tate Theory

Local class field theory classifies the abelian extensions of a local field. From a different perspective, it describes the local components of the global Artin map.

By a local field, I mean a field K that is locally compact with respect to a nontrivial absolute value. Thus (ANT, 7.49) it is

(a) a finite extension of $\mathbb{Q}_p$ for some p;

(b) a finite extension of the field of Laurent series $\mathbb{F}_p((T))$ over the field with p elements; or

(c) $\mathbb{R}$ or $\mathbb{C}$ (archimedean case).

When K is nonarchimedean, the ring of integers (alias, valuation ring) in K is denoted by $\mathcal{O}_K$ (or A), its maximal ideal by $\mathfrak{m}_K$ (or just $\mathfrak{m}$), and its group of units by $\mathcal{O}_K^\times$ or U_K. A generator of $\mathfrak{m}$ is called a ***prime element of*** K (or a ***uniformizer*** or a ***local uniformizing parameter***). If π is a prime element of K, then every element of $K^\times$ can be written uniquely in the form $a = u\pi^m$ with $u \in \mathcal{O}_K^\times$ and $m \in \mathbb{Z}$. We define

$$\operatorname{ord}_K(a) = m.$$

There is an exact sequence

$$0 \to U_K \to K^\times \xrightarrow{\operatorname{ord}_K} \mathbb{Z} \to 0$$

The residue field k of K has q elements, and its characteristic is p. The normalized absolute value on K is defined by $|a| = q^{-\operatorname{ord}_K(a)}$.

We let K^{al} denote a fixed algebraic closure of K (or separable algebraic closure in the case that K has characteristic $p \neq 0$), and "extension of K" means "subfield of K^{al} containing K". Both ord_K and $|\cdot|$ have unique extensions to K^{al} (the extension of ord_K takes values in $\mathbb{Q}$).

1 Statements of the Main Theorems

The composite of two finite abelian extensions of K is again a finite abelian extension of K (FT, 3.20). Therefore the union K^{ab} of all finite abelian extensions of K (in K^{al}) is an

infinite abelian extension whose Galois group is the quotient of $\mathrm{Gal}(K^{\mathrm{al}}/K)$ by the closure of its commutator subgroup. (See FT, Chapter 7, and the appendix to this chapter for the Galois theory of infinite extensions.)

Let L be a finite unramified extension of K. Then L is Galois over K, and the action of $\mathrm{Gal}(L/K)$ on $\mathcal{O}_L$ defines an isomorphism $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(l/k)$, where l is the residue field of L. Therefore $\mathrm{Gal}(L/K)$ is a cyclic group, generated by the unique element σ such that $\sigma\alpha \equiv \alpha^q \bmod \mathfrak{m}_L$ for all $\alpha \in \mathcal{O}_L$. This σ is called the ***Frobenius element*** of $\mathrm{Gal}(L/K)$, and is denoted by $\mathrm{Frob}_{L/K}$. See ANT, 7.54.

THEOREM 1.1 (LOCAL RECIPROCITY LAW) *For every nonarchimedian local field K, there exists a unique homomorphism*

$$\phi_K\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following properties:

(a) *for every prime element π of K and every finite unramified extension L of K, $\phi_K(\pi)$ acts on L as $\mathrm{Frob}_{L/K}$;*

(b) *for every finite abelian extension L of K, $\mathrm{Nm}_{L/K}(L^\times)$ is contained in the kernel of $a \mapsto \phi_K(a)|L$, and ϕ_K induces an isomorphism*

$$\phi_{L/K}\colon K^\times/\mathrm{Nm}_{L/K}(L^\times) \to \mathrm{Gal}(L/K).$$

In particular,

$$(K^\times\colon \mathrm{Nm}_{L/K}(L^\times)) = [L\colon K].$$

Denote $\mathrm{Nm}_{L/K}(L^\times)$ by $\mathrm{Nm}(L^\times)$. Statement (b) says that, for every finite abelian extension L of K, the map ϕ_K factors as follows:

$$\begin{array}{ccc} K^\times & \xrightarrow{\ \phi_K\ } & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \big\downarrow & & \big\downarrow{\scriptstyle \tau\mapsto\tau|L} \\ K^\times/\mathrm{Nm}(L^\times) & \xrightarrow[\simeq]{\ \phi_{L/K}\ } & \mathrm{Gal}(L/K). \end{array}$$

We call ϕ_K and $\phi_{L/K}$ the ***local Artin maps*** for K and L/K. They are often also called the ***local reciprocity maps*** and denoted by rec_K and $\mathrm{rec}_{L/K}$, and $\phi_{L/K}$ is often called the ***norm residue map*** or ***symbol*** and denoted $a \mapsto (a, L/K)$.

The subgroups of $K^\times$ of the form $\mathrm{Nm}(L^\times)$ for some finite abelian extension L of K are called the ***norm groups*** in $K^\times$.

COROLLARY 1.2 *Let K be a nonarchimedean local field, and assume that there exists a homomorphism $\phi\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying conditions (a) and (b) of the theorem.*

(a) *The map $L \mapsto \mathrm{Nm}(L^\times)$ is a bijection from the set of finite abelian extensions of K onto the set of norm groups in $K^\times$.*

(b) $L \subset L' \iff \mathrm{Nm}(L^\times) \supset \mathrm{Nm}(L'^\times)$.

(c) $\mathrm{Nm}((L\cdot L')^\times) = \mathrm{Nm}(L^\times) \cap \mathrm{Nm}(L'^\times)$.

(d) $\mathrm{Nm}((L \cap L)^\times) = \mathrm{Nm}(L^\times)\cdot \mathrm{Nm}(L'^\times)$.

(e) *Every subgroup of $K^\times$ containing a norm group is itself a norm group.*

PROOF. Note that the transitivity of norms,

$$\mathrm{Nm}_{L'/K} = \mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{L'/L},$$

shows that $L \subset L' \implies \mathrm{Nm}(L^\times) \supset \mathrm{Nm}(L'^\times)$. Hence,

$$\mathrm{Nm}((L \cdot L')^\times) \subset \mathrm{Nm}(L^\times) \cap \mathrm{Nm}(L'^\times).$$

Conversely, if $a \in \mathrm{Nm}(L^\times) \cap \mathrm{Nm}(L'^\times)$, then

$$\phi_{L/K}(a) = 1 = \phi_{L'/K}(a).$$

But, $\phi_{LL'/K}(a)|L = \phi_{L/K}(a)$ and $\phi_{L'L/K}(a)|L' = \phi_{L'/K}(a)$. As the map

$$\sigma \mapsto (\sigma|L, \sigma|L') : \mathrm{Gal}(LL'/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$$

is injective (FT, 3.20), this shows that $\phi_{LL'/K}(a) = 1$, and hence that $a \in \mathrm{Nm}((L \cdot L')^\times)$. This proves (c), and we now complete the proof of (b). When $\mathrm{Nm}(L^\times) \supset \mathrm{Nm}(L'^\times)$, statement (c) becomes

$$\mathrm{Nm}((LL')^\times) = \mathrm{Nm}(L'^\times).$$

Since the index of a norm group is the degree of the abelian extension defining it (1.1(b)) and $LL' \supset L'$, this implies that $LL' = L'$. Hence $L' \supset L$.

We now prove (a). By definition, the map $L \mapsto \mathrm{Nm}(L^\times)$ is surjective, and it follows from (b) that it is injective.

We next prove (e). Let N be a norm group, say, $N = \mathrm{Nm}(L^\times)$, and let $I \supset N$. Let M be the fixed field of $\phi_{L/K}(I)$, so that $\phi_{L/K}$ maps I/N isomorphically onto $\mathrm{Gal}(L/M)$. Consider the commutative diagram,

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ \| & & \downarrow \\ K^\times & \xrightarrow{\phi_{M/K}} & \mathrm{Gal}(M/K). \end{array}$$

The kernel of $\phi_{M/K}$ is $\mathrm{Nm}(M^\times)$. On the other hand, the kernel of

$$K^\times \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$$

is $\phi_{L/K}^{-1}(\mathrm{Gal}(L/M))$, which equals I (by Galois theory).

Finally, we prove (d). We have an order inverting bijection between the two sets in (a). As $L \cap L'$ is the largest extension of K contained in both L and L', and $\mathrm{Nm}(L^\times) \cdot \mathrm{Nm}(L'^\times)$ is the smallest subgroup containing $\mathrm{Nm}(L^\times)$ and $\mathrm{Nm}(L'^\times)$ (and it is a norm group by (e)), the two must correspond. □

In order to classify the abelian extensions of K, it remains to determine the norm groups. The next lemma shows that (assuming Theorem 1.1), they are open.

LEMMA 1.3 *Let L be an extension of K. If $\mathrm{Nm}(L^\times)$ is of finite index in $K^\times$, then it is open.*

PROOF. The group U_L of units in L is compact, and so $\mathrm{Nm}(U_L)$ is closed in $K^\times$. By looking at ords, one sees that

$$\mathrm{Nm}(L^\times) \cap U_K = \mathrm{Nm}(U_L),$$

and so $U_K/\mathrm{Nm}(U_L) \hookrightarrow K^\times/\mathrm{Nm}(L^\times)$. Therefore, $\mathrm{Nm}(U_L)$ is closed of finite index in U_K, and hence is open in U_K, which itself is open in $K^\times$. Therefore the group $\mathrm{Nm}(L^\times)$ contains an open subgroup of $K^\times$, and so is itself open.[1] □

THEOREM 1.4 (LOCAL EXISTENCE THEOREM) *The norm groups in $K^\times$ are exactly the open subgroups of finite index.*

COROLLARY 1.5 *Corollary 1.2 holds with "norm group" replaced by "open subgroup of finite index".*

Before outlining the proofs of Theorems 1.1 and 1.4, I give some complements to the theorems.

1.6 Corollary 1.5 holds also for archimedean local fields. The abelian extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$, and their norm subgroups are $\mathbb{R}^\times$ and $\mathbb{R}_{>0}$ respectively. Let H be a subgroup of finite index in $\mathbb{R}^\times$. Then $H \supset \mathbb{R}^{\times m}$ for some m, and $\mathbb{R}^{\times m} = \mathbb{R}^\times$ or $\mathbb{R}_{>0}$ according as m is odd or even (apply the intermediate value theorem). Therefore $\mathbb{R}^\times$ and $\mathbb{R}_{>0}$ are the only two subgroups of $\mathbb{R}^\times$ of finite index. The unique isomorphism

$$\mathbb{R}^\times/\mathbb{R}_{>0} \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

is called the local Artin map for $\mathbb{R}$.

1.7 When K has characteristic zero, *every* subgroup H of $K^\times$ of finite index is open. To prove this, observe that a subgroup H of finite index will contain $K^{\times m}$ for some m, and that Newton's lemma (ANT, 7.32) applied to $X^m - a$ shows that every $a \in \mathcal{O}_K^\times$ such that $|1-a| < |m|^2$ is of the form u^m with $u \in 1+\mathfrak{m}$. Therefore H contains an open neighbourhood of 1 in $K^\times$, and, since it is a group, this implies that it is open.

When K has characteristic $p \neq 0$, *not* every subgroup of $K^\times$ of finite index is open. Weil 1967, II 3, Proposition 10, shows that $1+\mathfrak{m} \approx \prod_{\mathbb{N}} \mathbb{Z}_p$ (product of copies of $\mathbb{Z}_p$ indexed by $\mathbb{N}$), from which it follows that $K^\times$ has a quotient isomorphic to $\prod_{\mathbb{N}} \mathbb{F}_p$. The subgroup $\bigoplus_{\mathbb{N}} \mathbb{F}_p$ is dense in $\prod_{\mathbb{N}} \mathbb{F}_p$. Therefore, every proper subgroup of $\prod_{\mathbb{N}} \mathbb{F}_p$ containing $\bigoplus_{\mathbb{N}} \mathbb{F}_p$ is not closed. Choose such a subgroup of finite index, and let U be its pre-image in $1+\mathfrak{m}$. Then $U \cdot \pi^{\mathbb{Z}}$ will be of finite index in $K^\times$ but not closed (hence not open). Cf. FT 7.26.

1.8 The composite of two finite unramified extensions of K is again unramified, and therefore the union K^{un} of all finite unramified extensions of K (in K^{al}) is an unramified extension of K. The residue field $\bar{k}$ of K^{un} is an algebraic closure of the residue field k of K.

Every automorphism σ of K^{un} fixing K preserves the absolute value $|\cdot|$ on K^{un}, and hence induces an automorphism $\bar{\sigma}$ of $\bar{k}/k$. The map $\sigma \mapsto \bar{\sigma}$ is an isomorphism

[1] We used that a closed subgroup of of finite index in a topological group is open (because its complement is a finite union of cosets, which are also closed), and that a subgroup is open if it contains an open subgroup (because it is a union of cosets of the open subgroup).

$\mathrm{Gal}(K^{\mathrm{un}}/K) \to \mathrm{Gal}(\bar{k}/k)$. Therefore, there is a unique element $\mathrm{Frob}_K \in \mathrm{Gal}(K^{\mathrm{un}}/K)$ inducing the map $x \mapsto x^q$ on $\bar{k}$, and the map $\alpha \mapsto \mathrm{Frob}_K^{\alpha}: \hat{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{un}}/K)$ is an isomorphism of topological groups. Condition (a) of Theorem 1.1 can be re-stated as: for every prime element π of K, $\phi_K(\pi)$ acts as Frob_K on K^{un}. In particular, for any unit $u \in \mathcal{O}_K^{\times}$, $\phi_K(\pi)$ and $\phi_K(\pi u)$ have the same action on K^{un} and therefore $\phi_K(u)$ acts as the identity map on K^{un}.

1.9 The groups

$$U_K \supset 1 + \mathfrak{m} \supset \cdots \supset 1 + \mathfrak{m}^n \supset \cdots \tag{7}$$

form a fundamental system of neighbourhoods of 1 in U_K. Let L be a finite abelian extension of K. If L/K is unramified, then $\mathrm{Ker}(\phi_{L/K}) \supset U_K$ by (1.8) and we say that L/K has ***conductor*** 0. Otherwise, the smallest f such that $\mathrm{Ker}(\phi_{L/K})$ contains $1 + \mathfrak{m}^f$ is called the ***conductor*** of L/K. The extension L/K is unramified if and only if it has conductor 0, and it is tamely ramified if and only if it has conductor ≤ 1. [Note that the quotients $1 + \mathfrak{m}^i/1 + \mathfrak{m}^{i+1}$ are p-groups for $i \geq 1$, and so $\phi_{L/K}|U_K$ factors through $U_K/(1 + \mathfrak{m})$ if L/K is tamely ramified. For a better statement, see 1.11.]

1.10 The homomorphisms

$$\phi_{L/K}: K^{\times}/\mathrm{Nm}(L^{\times}) \to \mathrm{Gal}(L/K)$$

form an inverse system as L runs through the finite abelian extensions of K, ordered by inclusion. On passing to the limit, we obtain an isomorphism

$$\hat{\phi}_K: \widehat{K^{\times}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where $\widehat{K^{\times}}$ is the completion of $K^{\times}$ with respect to the topology for which the norm groups form a fundamental system of neighbourhoods of 1. This topology on $K^{\times}$ is called the ***norm topology.*** According to Theorem 1.4, the norm groups are the open subgroups of finite index in $K^{\times}$. Choose a prime element π, and write

$$K^{\times} = U_K \cdot \pi^{\mathbb{Z}} \simeq U_K \times \mathbb{Z}. \tag{8}$$

The subgroups

$$(1 + \mathfrak{m}^n) \cdot \langle \pi^m \rangle \simeq (1 + \mathfrak{m}^n) \times m\mathbb{Z}$$

form a fundamental system of neighbourhoods of 1. In particular, U_K is not open in $K^{\times}$ for the norm topology, which is therefore coarser than the usual topology on $K^{\times}$. When completed, (8) becomes

$$\widehat{K^{\times}} = U_K \cdot \pi^{\hat{\mathbb{Z}}} \simeq U_K \times \hat{\mathbb{Z}},$$

where $\hat{\mathbb{Z}}$ is completion of $\mathbb{Z}$ for the topology defined by the subgroups of finite index. More canonically, the identity map

$$K^{\times}(\text{usual topology}) \to K^{\times}(\text{norm topology})$$

is continuous, and induces a homomorphism on the completions $K^{\times} \to \widehat{K^{\times}}$, which fits into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^{\times} & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U_K & \longrightarrow & \widehat{K^{\times}} & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

Loosely speaking, $\widehat{K^{\times}}$ is obtained from $K^{\times}$ by replacing $\mathbb{Z}$ with $\hat{\mathbb{Z}}$.

1.11 The choice of a prime element π determines a decomposition

$$\widehat{K^\times} = U_K \cdot \pi^{\hat{\mathbb{Z}}},$$

of $\widehat{K^\times}$ into the product of two closed subgroups, and hence (by infinite Galois theory), a decomposition

$$K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}, \tag{9}$$

where K_π is the subfield of K^{ab} fixed by $\phi_K(\pi)$ and K^{un} is the subfield of K^{ab} fixed by $\phi_K(U_K)$. Clearly, K_π is the union of all finite abelian extensions L/K (necessarily totally ramified) such that $\pi \in \mathrm{Nm}(L^\times)$. For example, when we choose the prime element p in $K = \mathbb{Q}_p$, the decomposition (9) becomes

$$\mathbb{Q}_p^{\mathrm{ab}} = \Big(\bigcup\nolimits_n \mathbb{Q}[\zeta_{p^n}]\Big) \cdot \Big(\bigcup\nolimits_{(m,p)=1} \mathbb{Q}[\zeta_m]\Big).$$

The map ϕ_K restricts to an isomorphism

$$U_K \to \mathrm{Gal}(K_\pi/K).$$

This isomorphism maps the filtration (7), p. 23, to the filtration on $\mathrm{Gal}(K_\pi/K)$ by the ramification groups (upper numbering; see 4.3).

1.12 The composite of two totally ramified extensions need not be totally ramified. Consider, for example, the quadratic extensions $\mathbb{Q}[\sqrt{p}]$ and $\mathbb{Q}[\sqrt{pq}]$ of $\mathbb{Q}$, where p and q are distinct odd primes. Then p is totally ramified in both of these extensions, but it is not totally ramified in their composite $\mathbb{Q}[\sqrt{p}, \sqrt{q}]$ because it is unramified in the subfield $\mathbb{Q}[\sqrt{q}]$. When q is chosen not to be a square modulo p, these statements remain true when $\mathbb{Q}$ is replaced by $\mathbb{Q}_p$.

Therefore, in contrast to the situation with abelian and unramified extensions, there is no "largest" totally ramified extension of K in K^{ab} (or K^{al}): there are only the maximal totally ramified extensions K_π, depending on the choice of π.

Outline of the proofs of the main theorems.

We first show that the uniqueness of the local Artin map follows from the remaining statements.

THEOREM 1.13 *Assume the local existence theorem 1.4. There exists at most one homomorphism $\phi\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying the conditions (a) and (b) of Theorem 1.1.*

PROOF. If no ϕ exists, there is nothing to prove, and so we assume there does exist a ϕ, and therefore that Corollary 1.2 holds with "norm group" replaced by "open subgroup of finite index". Let π be a prime element of $\mathcal{O}_K$, let $K_{\pi,n}$ be the extension of K with $\mathrm{Nm}(K_{\pi,n}) = (1 + \mathfrak{m}^n) \cdot \langle\pi\rangle$, and let $K_\pi = \bigcup_n K_{\pi,n}$. Because π is a norm from every $K_{\pi,n}$, $\phi(\pi)$ acts as 1 on K_π. Since it acts as the Frobenius automorphism on K^{un}, the action of $\phi(\pi)$ on $K_\pi \cdot K^{\mathrm{un}}$ is completely determined. But $K_\pi \cdot K^{\mathrm{un}} = K^{\mathrm{ab}}$ (cf. 1.11), and so this shows that $\phi(\pi) = \phi'(\pi)$ for any two homomorphisms ϕ and ϕ' satisfying the conditions. As π was arbitrary, we have shown that if ϕ and ϕ' satisfy the conditions, then $\phi(\pi) = \phi'(\pi)$ for *all* π. The group $K^\times$ is generated by the prime elements π of $\mathcal{O}_K$, and so this proves that $\phi = \phi'$. □

It remains to prove existence, namely, the existence of a local Artin map and the local existence theorem. We shall offer three proofs of this. The first two have the advantage that they explicitly construct the extension $K_{\pi,n}$ with norm group $(1+\mathfrak{m}^n)\cdot\langle\pi\rangle$ and the local Artin map $K^\times/\operatorname{Nm}(K_{\pi,n}) \to \operatorname{Gal}(K_{\pi,n}/K)$. The last two have the advantage that they prove the cohomological results used in global class field theory. The third has the advantage of brevity.

The reader looking for the fastest route to the main theorems of global class field theory need only understand the third proof, and so can skip the rest of the chapter and go directly to Chapter II.

FIRST PROOF OF EXISTENCE (LUBIN-TATE AND HASSE-ARF; I §§2–4)

The theory of Lubin and Tate explicitly constructs the fields $K_{\pi,n}$ for each prime, and hence the field K_π, and it explicitly constructs a homomorphism $\phi_\pi\colon U_K \to \operatorname{Gal}(K_\pi/K)$; moreover, it shows that $K_\pi\cdot K^{\mathrm{un}}$ and the unique extension of ϕ_π to a homomorphism $K^\times \to \operatorname{Gal}(K_\pi\cdot K^{\mathrm{un}}/K)$ such that $\phi(\pi)|K^{\mathrm{un}} = \operatorname{Frob}_K$ are independent of π. From this one gets Theorems 1.1 and 1.2 but with K^{ab} replaced by $K_\pi\cdot K^{\mathrm{un}}$.

> Need to add a proof of this to the notes. Let $K^{\mathrm{LT}} = K_\pi\cdot K^{\mathrm{un}}$. A key point is that, if L is a finite extension of K, then
>
> $$\begin{array}{ccc} L^\times & \xrightarrow{\phi_L} & \operatorname{Gal}(L^{\mathrm{LT}}/L) \\ \downarrow{\scriptstyle \operatorname{Nm}} & & \downarrow{\scriptstyle \tau\mapsto\tau|K^{\mathrm{LT}}} \\ K^\times & \xrightarrow{\phi_K} & \operatorname{Gal}(K^{\mathrm{LT}}/K) \end{array}$$
>
> commutes (Iwasawa 1986, Theorem 6.9, p. 89). This shows that, for any abelian extension L of K contained in K^{LT}, ϕ_K defines a surjective homomorphism
>
> $$\phi_{L/K}\colon K^\times/\operatorname{Nm}(L^\times) \to \operatorname{Gal}(L/K).$$
>
> Next one shows that this is injective (ibid., Corollary, p. 90). This proves the local reciprocity law (with K^{LT} for K^{ab}), and the local existence theorem follows easily.

All that remains is to show that $K_\pi\cdot K^{\mathrm{un}} = K^{\mathrm{ab}}$. The most direct proof of this uses the Hasse-Arf theorem from algebraic number theory.

SECOND PROOF OF THE MAIN THEOREMS (LUBIN-TATE AND COHOMOLOGY; I §§2–3; III §§1–3)

According to Theorems 1.1 and 1.4, there exists for each prime element π of $\mathcal{O}_K$ and integer $n \geq 1$, an abelian extension $K_{\pi,n}$ of K with

$$\operatorname{Nm}(K_{\pi,n}) = (1+\mathfrak{m}^n)\cdot\pi^{\mathbb{Z}}.$$

These extensions have the following properties:

***a** $[K_{\pi,n}\colon K] = (q-1)q^{n-1}$;

***b** for all n, π is a norm from $K_{\pi,n}$.

Moreover, $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$, where $K_\pi = \bigcup_{n\geq 1} K_{\pi,n}$.

In §3 of this chapter, we shall explicitly construct, for each prime element π of $\mathcal{O}_K$ and integer $n \geq 1$, a totally ramified abelian extension $K_{\pi,n}$ of K satisfying *a and *b. Let $K_\pi = \bigcup_{n\geq 1} K_{\pi,n}$ and, for $m \geq 1$, let K_m be the unramified extension of K of degree m. We shall explicitly construct a homomorphism

$$\phi_\pi \colon K^\times \to \mathrm{Gal}((K_\pi \cdot K^{\mathrm{un}})/K)$$

such that

***c** $\phi_\pi(\pi)|K^{\mathrm{un}} = \mathrm{Frob}_K$;

***d** for all m and n, $\phi_\pi(a)|\left(K_{\pi,n} \cdot K_m\right) = \mathrm{id}$ for $a \in (1+\mathfrak{m}^n)\cdot\langle\pi^m\rangle$.

Moreover, we shall prove that both $K_\pi \cdot K^{\mathrm{un}}$ and ϕ_π are independent of the choice of π.

In Chapter III, Theorem 3.4, we shall prove that there exists a homomorphism $\phi\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying conditions (a) and (b) of Theorem 1.1.

In the remainder of this subsubsection, we explain how these two results imply Theorem 1.4 (hence also Theorem 1.1) with the added precision that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$ and $\phi = \phi_\pi$ for all π.

Let K' be the subfield $K_\pi \cdot K^{\mathrm{un}}$ of K^{ab}, and let $\phi' = \phi_\pi$ — recall that both K' and ϕ' are independent of the choice of the prime element π.

1.14 *For all $a \in K^\times$, $\phi(a)|K' = \phi'(a)$.*

PROOF. For every prime element π of K, $\phi(\pi)$ acts trivially on $K_{\pi,n}$ because π is a norm from $K_{\pi,n}$, and $\phi'(\pi)$ acts trivially on $K_{\pi,n}$ because of condition *c with $m = 1$ (we may assume that the prime element used in the definition of ϕ' is π). Since $\phi(\pi)$ and $\phi'(\pi)$ both act as Frob_K on K^{un}, they must agree on $K' = \bigcup_n K_{\pi,n} \cdot K^{\mathrm{un}}$. But the prime elements of K generate $K^\times$ as a multiplicative group ($a \in K^\times$ can be written $a = u\pi^r$, and $u = (u\pi)\pi^{-1}$), and so this proves the claim. □

1.15 (LOCAL KRONECKER-WEBER THEOREM) *For any prime element π,*

$$K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}.$$

PROOF. Let

$$K_{n,m} = K_{\pi,n} \cdot K_m,$$

and

$$U_{n,m} = (1+\mathfrak{m}^n)\cdot\langle\pi^m\rangle.$$

We are given that $\phi_\pi(a)|K_{n,m} = 1$ for all $a \in U_{n,m}$. Hence $\phi(a)|K_{m,n} = 1$ for all $a \in U_{n,m}$, and so $U_{n,m} \subset \mathrm{Nm}(K_{n,m}^\times)$. But

$$\begin{aligned}(K^\times : U_{n,m}) &= (U : 1+\mathfrak{m}^n)(\langle\pi\rangle : \langle\pi^m\rangle)\\ &= (q-1)q^{n-1}\cdot m\\ &= [K_{\pi,n} : K][K_m : K]\\ &= [K_{m,n} : K],\end{aligned}$$

and we are given that ϕ induces an isomorphism

$$K^\times/\mathrm{Nm}(K_{n,m}^\times) \to \mathrm{Gal}(K_{n,m}/K).$$

Therefore,

$$U_{n,m} = \mathrm{Nm}(K^\times_{n,m}).$$

Now let L be a finite abelian extension of K. We are given that ϕ defines an isomorphism $K^\times/\mathrm{Nm}(L^\times) \to \mathrm{Gal}(L/K)$, and so $\mathrm{Nm}(L^\times)$ is of finite index in $K^\times$. According to Lemma 1.3, it is also open, and so it contains $U_{n,m}$ for some $n, m \geq 0$. The map

$$\phi\colon K^\times \to \mathrm{Gal}(L \cdot K_{n,m}/K)$$

is onto and, for $a \in K^\times$,

$$\begin{aligned} \phi(a) \text{ fixes the elements of } L &\iff a \in \mathrm{Nm}(L^\times), \\ \phi(a) \text{ fixes the elements of } K_{n,m} &\iff a \in \mathrm{Nm}(K^\times_{n,m}) = U_{n,m}. \end{aligned}$$

Because $\mathrm{Nm}(L^\times) \supset U_{n,m}$, this implies that $L \subset K_{n,m}$.

It follows that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$. □

We now know that, for every prime element π of K, $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$ and $\phi = \phi_\pi$. To complete the proof of the local existence theorem (1.4), we have to show that every open subgroup H of $K^\times$ of finite index is a norm group, but, as we observed above, every such group contains $U_{n,m}$ for some n and m, and $U_{n,m} = \mathrm{Nm}(K_{n,m})$. Now (1.2e) shows that H is a norm group.

THIRD PROOF OF THE MAIN THEOREMS (COHOMOLOGY AND HILBERT SYMBOLS; III §§1–5)

In Chapter III, we shall use cohomology (specifically, a theorem of Tate) to construct the local Artin maps, and we shall make use of Hilbert symbols to prove that every open subgroup of $K^\times$ of finite index is a norm group.

EXERCISE 1.16 Use only results from algebraic number theory (e.g., ANT) to prove that a finite extension L/K of local fields is totally ramified if and only if $\mathrm{Nm}(L/K)$ contains a prime element.

2 Lubin-Tate Formal Group Laws

> The important fact about a formal group law over A is that it turns the maximal ideal $\mathfrak{M}$ in the integers of each finite extension L/K into a group that is a Galois module. Being suitably careful, you can even let L be an infinite complete extension of K. In any case, this group may be very different indeed from the additive group $(\mathfrak{M}, +)$ and from the multiplicative group $(1 + \mathfrak{M}, \times)$. In particular, its torsion subgroup may give a very useful representation module for the Galois group. (Lubin, sx2061570)

Power series

Let A be a ring (always commutative with 1). A ***power series with coefficients*** in A is an infinite sequence

$$f = (a_0, a_1, a_2, \ldots), \quad a_i \in A, \quad i \in \mathbb{N}.$$

Addition and multiplication are defined by

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$
$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (a_0 b_0, \ldots, \sum_{i+j=k} a_i b_j, \ldots).$$

These formulas are easier to remember if we write

$$f = \sum_{i \geq 0} a_i T^i.$$

The power series with coefficients in A form a commutative ring, which we denote by $A[[T]]$. Power series can be manipulated in the same way as polynomials, with a few cautions. For example, in general we cannot substitute an element $c \in A$ into a power series $f(T) \in A[[T]]$, because computing $f(c) = \sum_{i \geq 0} a_i c^i$ requires us to sum an infinite number of elements of A, which, not being analysts, we are unable to do. For the same reason, we can substitute one power series $g(T)$ into a second $f(T)$ only if the constant term of $g(T)$ is zero, in which case $f(g(T))$ is defined, and we denote it by $f \circ g$.

LEMMA 2.1 (a) *For all power series $f \in A[[T]]$ and $g, h \in TA[[T]]$,*

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

(b) *Let $f = \sum_{i \geq 1}^{\infty} a_i T^i \in TA[[T]]$. There exists a $g \in TA[[T]]$ such that $f \circ g = T$ if and only if a_1 is a unit in A, in which case g is unique, and has the property that $g \circ f = T$.*

PROOF. (a) In general, $(f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)$, and so $f^n \circ g = (f \circ g)^n$. Therefore, when $f = T^n$, both $f \circ (g \circ h)$ and $(f \circ g) \circ h$ equal $(g \circ h)^n$, and when $f = \sum a_i T^i$, both equal $\sum a_i (g \circ h)^i$.

(b) We seek a $g = \sum_{i \geq 1} b_i T^i$ such that

$$\sum_{i \geq 1} a_i g^i = T,$$

i.e., such that

$$\begin{aligned} a_1 b_1 &= 1 \\ a_1 b_2 + a_2 b_1^2 &= 0 \\ &\cdots\cdots\cdots \\ a_1 b_n + \text{ polynomial in } a_2, \ldots, a_n, b_1, \ldots, b_{n-1} &= 0 \\ &\cdots\cdots\cdots \end{aligned}$$

The first equation shows that, in order for g to exist, a_1 must be invertible. When a_1 is invertible, the equations define the b_i's uniquely. Now, because b_1 is invertible, the same argument shows that there exists an $h \in TA[[T]]$ such that $g \circ h = T$. But

$$f = f \circ T = f \circ g \circ h = T \circ h = h,$$

and so $g \circ f = T$. □

Caution: $f \circ (g + h) \neq f \circ g + f \circ h$ in general.

Power series in several variables can be defined similarly. Moreover, if $f(X_1, \dots, X_n) \in A[[X_1, \dots, X_n]]$ and $g_1, g_2, \dots, g_n \in A[[Y_1, \dots, Y_m]]$, then $f(g_1, \dots, g_n)$ is a well-defined element of $A[[Y_1, \dots, Y_m]]$ provided that the constant terms of the g_i are all zero.

REMARK 2.2 Let A be a complete discrete valuation ring, and let $\mathfrak{m}$ be the maximal ideal in A. For every $f = \sum_{i \geq 0} a_i T^i \in A[[T]]$ and every $c \in \mathfrak{m}$, $a_i c^i \to 0$ as $i \to \infty$. Therefore the series $\sum_{i \geq 0} a_i c^i$ converges to an element $f(c)$ of A, which lies in $\mathfrak{m}$ if $a_0 \in \mathfrak{m}$.

Formal group laws

A group is a nonempty set together with a law of composition satisfying the group axioms. A formal group law is a law of composition (without the set) satisfying the group axioms. More precisely:

DEFINITION 2.3 Let A be a commutative ring. A ***one-parameter commutative formal group law*** is a power series $F \in A[[X, Y]]$ such that

(a) $F(X, Y) = X + Y +$ terms of degree ≥ 2;

(b) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

(c) there exists a unique $i_F(X) \in XA[[X]]$ such that $F(X, i_F(X)) = 0$;

(d) $F(X, Y) = F(Y, X)$.

REMARK 2.4 (a) Condition (a) ensures that $F(X, Y)$ has no constant term, and so axiom (b) makes sense: we are comparing finite sums at each degree.

(b) On taking $Y = Z = 0$ in Axioms (a) and (b), we find that

$$F(X, 0) = X + \text{terms of degree } \geq 2, \qquad F(F(X, 0), 0) = F(X, 0).$$

Denote the power series $F(X, 0)$ by $f(X)$. The first equality implies that there exists a g such that $f \circ g = X$, and the second equality says that $f \circ f = f$. On composing the second equality with g we find that $f = X$. Thus $F(X, 0) = X$, and similarly $F(0, Y) = Y$. Hence

$$F(X, Y) = X + Y + \sum_{\substack{1 \leq i < \infty \\ 1 \leq j < \infty}} a_{i,j} X^i Y^j.$$

To get an n-parameter group law, replace each of X and Y with sequences of n-variables. Axiom (d) is the commutativity condition. Since we consider no other, we shall refer to one-parameter commutative formal group laws simply as ***formal group laws***.

Let $A = \mathcal{O}_K$, the ring of integers in a nonarchimedean local field K, and let $F = \sum_{i,j}^{\infty} a_{ij} X^i Y^j$ be a formal group law over $\mathcal{O}_K$. For every $x, y \in \mathfrak{m}_K$, $a_{ij} x^i y^j \to 0$ as $(i, j) \to \infty$, and so the series

$$F(x, y) = \sum a_{ij} x^i y^j$$

converges to an element $x +_F y$ of $\mathfrak{m}_K$. In this way, $\mathfrak{m}_K$ becomes a commutative group $(\mathfrak{m}_K, +_F)$. Similarly, $\mathfrak{m}_L$ acquires a group structure for every finite extension L of K, and the inclusion $(\mathfrak{m}_K, +_F) \hookrightarrow (\mathfrak{m}_L, +_F)$ is a homomorphism.

EXAMPLE 2.5 (a) Let $F(X,Y) = X + Y$. Then $+_F$ is the usual addition law on $\mathfrak{m}_K$.

(b) Let $F(X,Y) = X + Y + XY$. The map

$$a \mapsto 1 + a : \mathfrak{m} \to 1 + \mathfrak{m}$$

is an isomorphism $(\mathfrak{m}, +_F) \to (1 + \mathfrak{m}, \times)$. Check:

$$\begin{array}{ccc} (a,b) & \longrightarrow & (1+a, 1+b) \\ \downarrow{\scriptstyle +_F} & & \downarrow{\scriptstyle \times} \\ a+b+ab & \longrightarrow & 1+a+b+ab. \end{array}$$

(c) Let E be an elliptic curve over a nonarchimedean local field K, and let

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

be a minimal Weierstrass model of E. Let $T = -X/Y$. On expanding the group law on E as a power series in T_1, T_2, we obtain a formal group law $F_E(T_1, T_2)$ over $\mathcal{O}_K$. See Milne 2020, 2.6, 2.7.

DEFINITION 2.6 Let $F(X,Y)$ and $G(X,Y)$ be formal group laws. A ***homomorphism*** $F \to G$ is a power series $h \in TA[[T]]$ such that

$$h(F(X,Y)) = G(h(X), h(Y)).$$

When h has an inverse, i.e., there exists a homomorphism $h' : G \to F$ such that

$$h \circ h' = T = h' \circ h,$$

then h is called an ***isomorphism.*** A homomorphism $h : F \to F$ is called an ***endomorphism*** of F.

In the case $A = \mathcal{O}_K$, a homomorphism $f : F \to G$ defines a homomorphism

$$a \mapsto f(a) : (\mathfrak{m}_L, +_F) \to (\mathfrak{m}_L, +_G)$$

for every $L \supset K$.

EXAMPLE 2.7 Let $F = X + Y + XY = (1+X)(1+Y) - 1$. Then $f(T) = (1+T)^p - 1$ is an endomorphism of F, because

$$F(f(X), f(Y)) = (1+X)^p(1+Y)^p - 1 = f(F(X,Y)).$$

Note that the following diagram commutes,

$$\begin{array}{ccc} \mathfrak{m} & \xrightarrow{f} & \mathfrak{m} \\ \downarrow{\scriptstyle a \mapsto 1+a} & & \downarrow{\scriptstyle a \mapsto 1+a} \\ 1+\mathfrak{m} & \xrightarrow{a \mapsto a^p} & 1+\mathfrak{m} \end{array}$$

i.e., when we identify $(\mathfrak{m}, +_F)$ with $(1 + \mathfrak{m}, \times)$, f becomes identified with $a \mapsto a^p$.

Let G be a formal group law. For any $f, g \in TA[[T]]$, we define

$$f +_G g = G(f(T), g(T)).$$

Because of the Axioms 2.3a,b,c,d, this composition law makes $TA[[T]]$ into a commutative group. In particular,

$$f +_G (i_G \circ f) = 0.$$

LEMMA 2.8 (a) *For any formal group laws F and G, the set $\mathrm{Hom}(F, G)$ of homomorphisms from F to G becomes an abelian group with the addition $f +_G g$.*

(b) *For any formal group law F, the abelian group $\mathrm{End}(F)$ of endomorphisms of F becomes a ring (not necessarily commutative) with the multiplication $f \circ g$.*

PROOF. Let f and g be homomorphisms $F \to G$, and let $h = f +_G g$. Then

$$\begin{aligned} h(F(X,Y)) &\overset{\text{def}}{=} G(f(F(X,Y)), g(F(X,Y))) \\ &= G(G(f(X), f(Y)), G(g(X), g(Y))). \end{aligned}$$

Symbolically (at least), we can write this last power series as

$$(f(X) +_G f(Y)) +_G (g(X) +_G g(Y)), \qquad (*)$$

which associativity and commutativity allow us to rewrite as

$$(f(X) +_G g(X)) +_G (f(Y) +_G g(Y)), \qquad (**)$$

that is, as $G(h(X), h(Y))$. More formally, the operations that carry $(*)$ into $(**)$, also carry $G(G(f(X), f(Y)), G(g(X), g(Y)))$ into $G(h(X), h(Y))$. This proves that $h \in \mathrm{Hom}(F, G)$. Similarly, one shows that $i_G \circ f \in \mathrm{Hom}(F, G)$. As $0 \in \mathrm{Hom}(F, G)$, this completes the proof that $\mathrm{Hom}(F, G)$ is a subgroup of $(TA[[T]], +_G)$.

We showed in Lemma 2.1 that $f, g \mapsto f \circ g$ is associative. To show that $\mathrm{End}(F)$ is a ring, it remains to observe that, for $f, g, h \in \mathrm{End}(F)$,

$$f \circ (g +_F h) \overset{\text{def}}{=} f(F(g(T), h(T))) = F((f \circ g)(T), (f \circ h)(T)) = f \circ g +_F f \circ h,$$
$$(f +_F g) \circ h = f \circ h +_F g \circ h \text{ (similarly)},$$

and that $\mathrm{End}(F)$ has an identity element, namely, T. □

Formal group laws are similar to algebraic groups. The main difference is that, because they are defined by power series rather than polynomials, their points must have coordinates "close to 1" in order for products to be defined. There is a very extensive theory of formal group laws—see, for example, M. Hazewinkel, Formal Groups and Applications, Academic Press, 1978.

Lubin-Tate group laws

We now let $A = \mathcal{O}_K$, the ring of integers in a nonarchimedean local field K, and we choose a prime element π of A.

DEFINITION 2.9 Let $\mathcal{F}_\pi$ be the set of $f(X) \in A[[X]]$ such that

(a) $f(X) = \pi X +$ terms of degree ≥ 2;

(b) $f(X) \equiv X^q \mod \pi$.

EXAMPLE 2.10 (a) The polynomial $f(X) = \pi X + X^q$ lies in $\mathcal{F}_\pi$.

(b) Let $K = \mathbb{Q}_p$ and $\pi = p$; then the polynomial

$$f(X) = (1+X)^p - 1 = pX + \tbinom{p}{2}X^2 + \cdots + pX^{p-1} + X^p$$

lies in $\mathcal{F}_p$.

LEMMA 2.11 *Let $f, g \in \mathcal{F}_\pi$, and let $\phi_1(X_1, \cdots, X_n)$ be a linear form with coefficients in A. There is a unique $\phi \in A[[X_1, \ldots, X_n]]$ such that*

$$\begin{cases} \phi(X_1, \ldots, X_n) & = & \phi_1 + \textit{ terms of degree } \geq 2 \\ f(\phi(X_1, \ldots, X_n)) & = & \phi(g(X_1), \ldots, g(X_n)). \end{cases}$$

PROOF. We prove by induction on r that there is a unique polynomial $\phi_r(X_1, \ldots, X_n)$ of degree r such that

$$\begin{cases} \phi_r(X_1, \ldots, X_n) & = & \phi_1 + \text{ terms of degree } \geq 2 \\ f(\phi_r(X_1, \ldots, X_n)) & = & \phi_r(g(X_1), \ldots, g(X_n)) + \text{ terms of degree } \geq r+1. \end{cases}$$

The unique candidate for the first polynomial is ϕ_1 itself. It certainly satisfies the first condition, and, if we write $\phi_1 = \sum a_i X_i$, the second says that

$$\pi(\textstyle\sum a_i X_i) = \sum a_i(\pi X_i) + \deg \geq 2,$$

which is also true.

Suppose $r \geq 1$ and we have defined ϕ_r. Because ϕ_r is unique, ϕ_{r+1} must equal $\phi_r + Q$, where Q is a homogeneous polynomial of degree $r+1$ in $A[X_1, \ldots, X_n]$. We need that

$$f(\phi_{r+1}(X_1, \ldots, X_n)) \stackrel{?}{=} \phi_{r+1}(g(X_1), \ldots, g(X_n)) + \text{terms of degree } \geq r+2.$$

The left hand side is

$$f(\phi_r(X_1, \ldots, X_n)) + \pi Q(X_1, \ldots, X_n) + \text{terms of degree } \geq r+2,$$

while the right hand side is

$$\phi_r(g(X_1), \ldots, g(X_n)) + Q(\pi X_1, \ldots, \pi X_n) + \text{terms of degree } \geq r+2.$$

As Q is homogeneous of degree $r+1$, $Q(\pi X_1, \ldots) = \pi^{r+1} Q(\pi X_1, \ldots)$, and so we need that

$$(\pi^{r+1} - \pi)Q(X_1, \ldots, X_n) \stackrel{?}{=} f(\phi_r(X_1, \ldots, X_n)) - \phi_r(g(X_1), \ldots, g(X_n)) + \text{terms of degree} \geq r+2.$$

Thus Q must be the unique polynomial such that

$$\frac{f(\phi_r(X_1, \ldots, X_n)) - \phi_r(g(X_1), \ldots, g(X_n))}{(\pi^r - 1)\pi} = Q + \text{terms of degree } \geq r+2.$$

Note that, because of the simple form that binomial theorem takes in characteristic p,

$$f \circ \phi_r - \phi_r \circ g \equiv \phi_r(X_1, \dots, X_n)^q - \phi_r(X_1^q, \dots, X_n^q) \equiv 0 \mod \pi.$$

Because π divides $f \circ \phi_r - \phi_r \circ g$ and $\pi^r - 1$ is invertible in A, Q does have coefficients in A, and because ϕ_r satisfies the induction hypothesis, it does have degree $r+1$.

Having defined the ϕ_r for $r = 1, 2, \dots$ and noted that

$$\phi_{r+1} = \phi_r + \text{terms of degree } \geq r+1,$$

we can define ϕ to be the unique power series such that

$$\phi = \phi_r + \text{terms of degree } \geq r+1$$

for all r. Clearly, it has the first of the required properties, and for any r,

$$\begin{aligned} f(\phi(X_1, \dots, X_n)) &= f(\phi_r(X_1, \dots, X_n)) + \text{terms of degree } \geq r+1 \\ &= \phi_r(g(X_1, \dots, X_n)) + \text{terms of degree } \geq r+1 \\ &= \phi(f(X_1, \dots, X_n)) + \text{terms of degree } \geq r+1. \end{aligned}$$

Since this holds for all r, ϕ also has the second required property. □

PROPOSITION 2.12 *For every $f \in \mathcal{F}_\pi$, there is a unique formal group law F_f with coefficients in A admitting f as an endomorphism.*

PROOF. According to Lemma 2.11, there is a unique power series $F_f(X, Y)$ such that

$$\begin{cases} F_f(X,Y) &= X + Y + \text{ terms of degree } \geq 2 \\ f(F_f(X,Y)) &= F_f(f(X), f(Y)). \end{cases}$$

It remains to check that this is a formal group law.

Commutativity: Let $G = F_f(Y, X)$. Then

$$\begin{cases} G(X,Y) &= X + Y + \text{ terms of degree } \geq 2 \\ f(G(X,Y)) &= f(F_f(Y,X)) = F_f(f(Y), f(X)) = G(f(X), f(Y)). \end{cases}$$

Since $F_f(X, Y)$ is the unique power series with these properties, it follows that $G(X, Y) = F_f(X, Y)$.

Associativity: Let $G_1(X, Y, Z) = F_f(X, F_f(Y, Z))$ and $G_2(X, Y, Z) = F_f(F_f(X, Y), Z)$. Then, for $i = 1, 2$,

$$\begin{cases} G_i(X,Y,Z) &= X + Y + Z + \text{ terms of degree } \geq 2 \\ G_i(f(X), f(Y), f(Z)) &= f(G_i(X,Y,Z)) \end{cases}$$

and again Lemma 2.11 shows that there is only one power series satisfying these conditions. □

EXAMPLE 2.13 Let $K = \mathbb{Q}_p$ and $\pi = p$. Then $f(T) = (1+T)^p - 1$ lies in $\mathcal{F}_p$, and $F(X, Y) = X + Y + XY$ admits f as an endomorphism (see 2.7). Therefore, $F = F_f$.

The formal group laws F_f defined by the proposition are the ***Lubin-Tate formal group laws.*** They are exactly the formal group laws admitting an endomorphism

- ◇ that has derivative at the origin equal to a prime element of K, and
- ◇ reduces mod $\mathfrak{m}$ to the Frobenius map $T \mapsto T^q$.

PROPOSITION 2.14 *For $f, g \in \mathcal{F}_\pi$ and $a \in A$, let $[a]_{g,f}$ be the unique element of $A[[T]]$ such that*

$$\begin{cases} [a]_{g,f}(T) &= aT + \text{ terms of degree } \geq 2 \\ g \circ [a]_{g,f} &= [a]_{g,f} \circ f. \end{cases}$$

Then $[a]_{g,f}$ is a homomorphism $F_f \to F_g$.

PROOF. Let $h = [a]_{g,f}$—its existence is guaranteed by Lemma 2.11. We have to show that

$$h(F_f(X, Y)) = F_g(h(X), h(Y)).$$

Obviously each is equal to $aX + aY +$terms of degree ≥ 2. Moreover,

$$h(F_f(f(X), f(Y))) = (h \circ f)(F_f(X, Y)) = g(h(F_f(X, Y))),$$

$$F_g(h(f(X)), h(f(Y))) = F_g(g(h(X)), g(h(Y))) = g(F_g(h(X), h(Y))),$$

and we can apply the uniqueness in Lemma 2.11 again. □

PROPOSITION 2.15 *For any $a, b \in A$,*

$$[a + b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$$

and

$$[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}.$$

PROOF. In each case, the power series on the right satisfies the conditions characterizing the power series on the left. □

COROLLARY 2.16 *For $f, g \in \mathcal{F}_\pi$, $F_f \approx F_g$.*

PROOF. For every $u \in A^\times$, $[u]_{f,g}$ and $[u^{-1}]_{g,f}$ are inverse isomorphisms. □

In fact, there is a unique isomorphism $h\colon F_f \to F_g$ such that $h(T) = T + \cdots$ and $g \circ h = h \circ f$, namely, $[1]_{g,f}$. Thus $F_f \simeq F_g$.

COROLLARY 2.17 *For each $a \in A$, there is a unique endomorphism $[a]_f\colon F_f \to F_f$ such that $[a]_f = aT +$terms of degree ≥ 2 and $[a]_f$ commutes with f. The map*

$$a \mapsto [a]_f\colon A \hookrightarrow \mathrm{End}(F_f)$$

is a ring homomorphism.

PROOF. Take $[a]_f = [a]_{f,f}$—it is the unique power series $aT + \cdots$ commuting with f, and it is an endomorphism of F_f. That $a \mapsto [a]_f$ is a ring homomorphism follows from Lemma 2.15 and the obvious fact that $[1]_f = T$. □

It follows that the abelian group $(\mathfrak{m}_L, +_{F_f})$ has a natural A-module structure for L a finite extension of K.

EXAMPLE 2.18 Let $K = \mathbb{Q}_p$ and $f = (1+T)^p - 1 \in \mathcal{F}_p$, so that $F_f = X + Y + XY$. For every $a \in \mathbb{Z}_p$, define

$$(1+T)^a = \sum_{m\geq 0} \binom{a}{m} T^m, \quad \binom{a}{m} \stackrel{\text{def}}{=} \frac{a(a-1)\cdots(a-m+1)}{m(m-1)\cdots 1}.$$

When $a \in \mathbb{Z}$, these definitions agree with the usual ones, and if $(a_i)_{i\geq 1}$ is a sequence of integers converging to $a \in \mathbb{Z}_p$, then $\binom{a_i}{m} \to \binom{a}{m}$ as $i \to \infty$. Therefore $\binom{a}{m} \in \mathbb{Z}_p$. I claim that

$$[a]_f = (1+T)^a - 1.$$

Certainly, $(1+T)^a - 1 = aT + \cdots$, and

$$f \circ ((1+T)^a - 1) = (1+T)^{ap} - 1 = ((1+T)^a - 1) \circ f$$

holds when a is an integer, which (by continuity) implies that it holds for all $a \in \mathbb{Z}_p$.

Under the isomorphism $(\mathfrak{m}, +_{F_f}) \xrightarrow{t\mapsto 1+t} (1+\mathfrak{m}, \times)$, the action of $[a]_f$ corresponds to the map sending an element of $1+\mathfrak{m}$ to its ath power.

REMARK 2.19 (a) Note that $[\pi]_f = f$, because f satisfies the two defining conditions.

(b) The homomorphism $a \mapsto [a]_f : A \mapsto \mathrm{End}(F_f)$ is injective, because a can be recovered as the leading coefficient of $[a]_f$.

(c) The canonical isomorphism $[1]_{g,f} : F_f \to F_g$ commutes with the actions of A on F_f and F_g, because

$$[a]_g \circ [1]_{g,f} = [a]_{g,f} = [1]_{g,f} \circ [a]_f.$$

SUMMARY 2.20 For each $f \in \mathcal{F}_\pi$, there exists a unique formal group law F_f admitting f as an endomorphism. Moreover, there is a unique A-module structure $a \mapsto [a]_f : A \to \mathrm{End}(F_f)$ on F_f such that

(a) $[a]_f = aT +$terms of degree ≥ 2, all $a \in A$;

(b) $[a]_f$ commutes with f.

We have $[\pi]_f = f$. If $g \in \mathcal{F}_\pi$, then $F_f \simeq F_g$ (by a canonical A-isomorphism).

EXERCISE 2.21 Let $F(X,Y)$ be a power series such that $F(X,0) = X$ and $F(0,Y) = Y$. Show that there is a unique power series $G(X) = -X + \sum_{i=2}^{\infty} a_i X$ such that $F(X, G(X)) = 0$. Hence Axiom (c) in Definition 2.3 is redundant.

NOTES Let $f \in \mathcal{F}_\pi$. There is a unique power series $\log(T) = T + \cdots \in K[[T]]$ such that $\log(F(x,y)) = \log(x) + \log(y)$. It has the property that

$$\log([a]_f(T)) = a \log(T)$$

for $a \in A$. See sx3644403.

3 Construction of the extension K_π of K.

In this section, $A = \mathcal{O}_K$, where K is a nonarchimedean local field with residue field $A/\mathfrak{m} = k$ having q (a power of p) elements. We fix a prime element π of A.

According to the discussion in Section 1, there should be a unique extension K_π of K in K^{al} such that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$ and π is a norm from every finite subextension of K_π, namely, the subfield K_π of K^{ab} fixed by $\phi(\pi)$.

It is easy to construct K^{un}. Let μ_m be the set of mth roots of 1 in K^{al}, i.e., μ_m is the set of roots of $X^m - 1$. When m is not divisible by p, the discriminant of $X^m - 1$ is a unit in $\mathcal{O}_K$, and so the field $K[\mu_m]$ generated by the elements of μ_m is unramified over K; moreover, the residue field of $K[\mu_m]$ is the splitting field of $X^m - 1$ over k, and so has q^f elements, where f is the smallest positive integer such that $m | p^f - 1$. Therefore $\bigcup_{p\nmid m} K[\mu_m]$ is an unramified extension of K with residue field an algebraic closure of k, and so equals K^{un}. The Galois group $\mathrm{Gal}(K^{\mathrm{un}}/K) \simeq \hat{\mathbb{Z}}$, and $a \in \hat{\mathbb{Z}}$ acts K^{un} as follows: for every $\zeta \in \mu_m$ and every integer a_0 sufficiently close to a (depending on m), $a * \zeta = \zeta^{a_0} \quad (= \mathrm{Frob}_K^a(\zeta))$.

In the case $K = \mathbb{Q}_p$ and $\pi = p$, there is a similar construction for K_π, namely, $(\mathbb{Q}_p)_p = \bigcup \mathbb{Q}_p[\mu_{p^n}]$—we shall prove later that this has the indicated properties. The action

$$([m], \zeta) \mapsto \zeta^m : \mathbb{Z}/p^n\mathbb{Z} \times \mu_{p^n} \to \mu_{p^n}$$

makes μ_{p^n} into a free $\mathbb{Z}/p^n\mathbb{Z}$-module of rank 1. Since $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$, we can regard μ_{p^n} as a $\mathbb{Z}_p$-module, isomorphic to $\mathbb{Z}_p/(p^n)$. The action of $\mathbb{Z}_p$ on μ_{p^n} induces an isomorphism $(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times \to \mathrm{Gal}(\mathbb{Q}_p[\mu_{p^n}]/\mathbb{Q}_p)$, and, on passing to limit over all n, we obtain an isomorphism

$$\mathbb{Z}_p^\times \to \mathrm{Gal}((\mathbb{Q}_p)_p/\mathbb{Q}_p).$$

Thus, for both the extensions K^{un}/K and $(\mathbb{Q}_p)_p/\mathbb{Q}_p$, we have an explicit set of generators for the extension, an explicit description of the Galois group, and an explicit description of the Galois group on the set of generators. Remarkably, the Lubin-Tate groups provide similar results for K_π/K for every K and π.

The absolute value $|\cdot|$ on K extends uniquely to every subfield L of K^{al} of finite degree over K, and hence to K^{al}. Let $f \in \mathcal{F}_\pi$. For any $\alpha, \beta \in K^{\mathrm{al}}$ with $|\alpha|, |\beta| < 1$ and $a \in A$, the series $F_f(\alpha, \beta)$ and $[a]_f(\alpha)$ converge. Therefore, we can define Λ_f to be the A-module with:

$$\begin{aligned} \Lambda_f &= \{\alpha \in K^{\mathrm{al}} \mid |\alpha| < 1\} \quad \text{(as a set)}, \\ \alpha +_{\Lambda_f} \beta &= \alpha +_{F_f} \beta = F_f(\alpha, \beta), \\ a * \alpha &= [a]_f(\alpha). \end{aligned}$$

We define Λ_n to be the submodule of Λ_f of elements killed by $[\pi]_f^n$. If g is a second element of $\mathcal{F}_\pi$, then the canonical A-isomorphism $F_f \to F_g$ induces an A-isomorphism $\Lambda_f \to \Lambda_g$.

REMARK 3.1 Recall that $[\pi]_f(T) = f(T)$, and therefore Λ_n is the set of roots of

$$f^{(n)} \stackrel{\text{def}}{=} f \circ f \circ \cdots \circ f \qquad (n \text{ factors})$$

in K^{al} with absolute value < 1. For simplicity, we let f be a polynomial $\pi T + a_2 T^2 + \cdots + T^q$ rather than a more complicated power series — according to 2.16 it even suffices

to take $f = \pi T + T^q$.[2] Then,

$$(f \circ f)(T) \stackrel{\text{def}}{=} f(f(T)) = \pi(\pi T + \cdots + T^q) + \cdots + (\pi T + \cdots + T^q)^q$$
$$= \pi^2 T + \cdots + T^{q^2},$$

and

$$f^{(n)}(T) = \pi^n T + \cdots + T^{q^n}.$$

From the Newton polygon of $f^{(n)}$ (cf. ANT, 7.44), we see that the roots of $f^{(n)}$ all have positive ord_K, hence absolute value < 1, and so Λ_n is the set of *all* roots of $f^{(n)}$ in K^{al} endowed with the commutative group stucture

$$\alpha +_{F_f} \beta = F_f(\alpha, \beta) = \alpha + \beta + \cdots,$$

and the A-module structure,

$$[a]_f \alpha = a\alpha + \cdots.$$

EXAMPLE 3.2 Take $K = \mathbb{Q}_p$ and $f = (T+1)^p - 1 \in \mathcal{F}_p$; then

$$\Lambda_n = \{\alpha \in \mathbb{Q}_p^{\mathrm{al}} \mid (\alpha - 1)^{p^n} = 1\} \simeq \{\zeta \mid \zeta^{p^n} = 1\} = \mu_{p^n}.$$

The addition $+_F$ on Λ_n corresponds to multiplication on μ_{p^n}, and the $\mathbb{Z}_p$-module structure is as defined before. It follows that $\Lambda_n \approx \mathbb{Z}/p^n\mathbb{Z}$ (as a $\mathbb{Z}_p$-module).

Recall that a ***cyclic module*** is a module that can be generated by a single element. Because A is a principal ideal domain with only one prime element up to conjugates, every finitely generated torsion A-module M decomposes into a direct sum of cyclic modules

$$M \approx A/(\pi^{n_1}) \oplus \cdots \oplus A/(\pi^{n_r}), \quad n_1 \le n_2 \le \ldots,$$

and the sequence $n_1, \ldots, n_r$ is uniquely determined.

LEMMA 3.3 *Let M be an A-module, and let $M_n = \operatorname{Ker}(\pi^n : M \to M)$. Assume,*

(a) *M_1 has $q \stackrel{\text{def}}{=} (A : (\pi))$ elements, and*

(b) *$\pi : M \to M$ is surjective.*

Then $M_n \approx A/(\pi^n)$; in particular, it has q^n elements.

PROOF. We use induction on n. Because A/π has order q, condition (a) and the structure theorem imply that $M_1 \approx A/(\pi)$. Consider the sequence

$$0 \to M_1 \to M_n \xrightarrow{\pi} M_{n-1} \to 0.$$

Condition (b) implies that it is exact at M_{n-1}, and is therefore exact. It follows that M_n has q^n elements. If M_n is not cyclic,

$$M_n \approx A/(\pi^{n_1}) \oplus A/(\pi^{n_2}) \oplus \cdots, \quad n_1, n_2, \ldots \ge 1,$$

then M_1 is not cyclic,

$$M_1 \approx (\pi^{n_1 - 1})/(\pi^{n_1}) \oplus (\pi^{n_2 - 1})/(\pi^{n_2}) \oplus \cdots.$$

Therefore M_n is a cyclic A-module of order q^n, and every such module is isomorphic to $A/(\pi^n)$. □

[2] Alternatively, the p-adic Weierstrass preparation theorem (Washington 1997, 7.3) implies that every $f \in \mathcal{F}_\pi$ factors into $f_1(T)u(T)$, where $f_1(T)$ is a polynomial $\pi T + \cdots + aT^q$, $a \equiv 1 \mod \mathfrak{m}$, and $u(T)$ is a unit in $A[[T]]$. Obviously, the roots of $f^{(n)}$ are the roots of $f_1^{(n)}$.

PROPOSITION 3.4 *The A-module Λ_n is isomorphic to $A/(\pi^n)$. Hence $\mathrm{End}_A(\Lambda_n) \simeq A/(\pi^n)$ and $\mathrm{Aut}_A(\Lambda_n) \simeq (A/(\pi^n))^\times$.*

PROOF. An A-isomorphism $h\colon F_f \to F_g$ of formal group laws induces an isomorphism of A-modules $\Lambda_f \to \Lambda_g$, and so it does not matter which $f \in \mathcal{F}_\pi$ we choose. We take $f \in \mathcal{F}_\pi$ to be a polynomial of the form $\pi T + \cdots + T^q$. This is an Eisenstein polynomial (ANT, p. 129), and so has q distinct roots, each with absolute value < 1. Let $\alpha \in K^{\mathrm{al}}$ have absolute value < 1. From the Newton polygon of

$$f(T) - \alpha = T^q + \cdots + \pi T - \alpha$$

we see that its roots have absolute value < 1, and so lie in Λ_f. We have shown that Λ_f satisfies the hypotheses of the lemma, and so $\Lambda_n \approx A/(\pi^n)$. It follows that the action of A on Λ_n induces an isomorphism $A/(\pi^n) \to \mathrm{End}_A(\Lambda_n)$. □

LEMMA 3.5 *Let L be a finite Galois extension of a local field K, with Galois group G. For every $F \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ and $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}_L$,*

$$F(\tau\alpha_1, \ldots, \tau\alpha_n) = \tau F(\alpha_1, \ldots, \alpha_n), \quad \text{all } \tau \in G.$$

PROOF. If F is a polynomial, this follows from the fact that τ is a field isomorphism fixing the elements of $\mathcal{O}_K$. Because the absolute value on L is the unique extension of the absolute value on K (ANT, 7.38), it is preserved by $\tau \in G$, i.e., $|\tau\alpha| = |\alpha|$ all $\alpha \in L$, and so τ is continuous. Therefore it preserves limits,

$$\lim_{m\to\infty} \alpha_m = L \Rightarrow \lim_{m\to\infty} \tau\alpha_m = \tau L.$$

Write $F = F_m + \text{terms of degree} \geq m+1$ with F_m a polynomial of degree m. Then

$$\begin{aligned} \tau(F(\alpha_1, \ldots, \alpha_n)) &= \tau(\lim_{m\to\infty} F_m(\alpha_1, \ldots, \alpha_n)) \\ &= \lim_{m\to\infty} \tau\,(F_m(\alpha_1, \ldots, \alpha_n)) \\ &= \lim_{m\to\infty} F_m(\tau\alpha_1, \ldots, \tau\alpha_n). \end{aligned}$$

□

THEOREM 3.6 *Let $K_{\pi,n}$ denote the subfield $K[\Lambda_n]$ of K^{al} generated over K by the elements of Λ_n.*

(a) *For each n, $K_{\pi,n}/K$ is totally ramified of degree $(q-1)q^{n-1}$.*

(b) *The action of A on Λ_n defines an isomorphism*

$$(A/\mathfrak{m}^n)^\times \to \mathrm{Gal}(K_{\pi,n}/K).$$

In particular, $K_{\pi,n}/K$ is abelian.

(c) *For each n, π is a norm from $K_{\pi,n}$.*

PROOF. Again, we may assume that $f \in \mathcal{F}_\pi$ is a polynomial of the form $\pi T + \cdots + T^q$.

(a), (b). Choose a nonzero root π_1 of $f(T)$ and (inductively) a root π_n of $f(T) - \pi_{n-1}$. Consider the sequence of fields

$$K[\Lambda_n] \supset K[\pi_n] \overset{q}{\supset} K[\pi_{n-1}] \overset{q}{\supset} \cdots \overset{q}{\supset} K[\pi_1] \overset{q-1}{\supset} K.$$

Each extension is Eisenstein (ANT, 7.55) with the degree indicated. Therefore $K[\pi_n]$ is totally ramified over K of degree $q^{n-1}(q-1)$.

Recall that Λ_n is the set of roots of $f^{(n)}$ in K^{al}, and so $K[\Lambda_n]$ is the splitting field of $f^{(n)}$. Therefore $\mathrm{Gal}(K[\Lambda_n]/K)$ can be identified with a subgroup of the group of permutations of the set Λ_n, but Lemma 3.5 implies that each element of $\mathrm{Gal}(K[\Lambda_n]/K)$ acts on Λ_n as an A-module isomorphism, and so the image of $\mathrm{Gal}(K[\Lambda_n]/K)$ in the automorphism group of Λ_n is contained in

$$\mathrm{End}_A(\Lambda_n) = (A/(\pi^n))^\times.$$

Hence

$$(q-1)q^{n-1} \geq |\mathrm{Gal}(K[\Lambda_n]/K)| = [K[\Lambda_n]:K] \geq [K[\pi_n]:K] = (q-1)q^{n-1}.$$

We must have equalities throughout, and so $\mathrm{Gal}(K[\Lambda_n]/K) \simeq (A/\mathfrak{m}^n)^\times$ and $K[\Lambda_n] = K[\pi_n]$.

(c) Let $f^{[n]}(T) = (f/T) \circ f \circ \cdots \circ f$ (n terms), so that

$$f^{[n]}(T) = \pi + \cdots + T^{(q-1)q^{n-1}}.$$

Then $f^{[n]}(\pi_n) = f^{[n-1]}(\pi_{n-1}) = \cdots = f(\pi_1) = 0$. Because $f^{[n]}$ is monic of degree $(q-1)q^{n-1} = [K[\pi_n]:K]$, it must be the minimal polynomial of π_n over K. Therefore,

$$\begin{aligned} \mathrm{Nm}_{K[\Lambda_n]/K}\,\pi_n &= (-1)^{(q-1)q^{n-1}}\pi \\ &= \pi \quad \text{unless } q = 2 \text{ and } n = 1. \end{aligned}$$

In the exceptional case, $K[\Lambda_1] = K$, and π is certainly a norm. □

SUMMARY 3.7 Let $f(T) = \pi T + \cdots + T^q$, and let Λ_n be the set of roots of $f^{(n)}$ in K^{al}. Define $K_{\pi,n} = K[\Lambda_n]$. Then

$$\begin{array}{lcl} K_\pi & = & \bigcup K_{\pi,n} \\ | & & \\ \vdots & & \\ | & & \\ K_{\pi,n} & = & K[\pi_n] \quad f(\pi_n) = \pi_{n-1} \quad \mathfrak{m}_{K_{\pi,n}} = (\pi_n) \\ | \, q & & \\ \vdots & & \\ | \, q & & \\ K_{\pi,2} & = & K[\pi_2] \quad f(\pi_2) = \pi_1 \quad \mathfrak{m}_{K_{\pi,2}} = (\pi_2) \\ | \, q & & \\ K_{\pi,1} & = & K[\pi_1] \quad f(\pi_1) = 0 \quad \mathfrak{m}_{K_{\pi,1}} = (\pi_1) \quad \pi_1 \neq 0 \\ | \, q-1 & & \\ K & & \end{array}$$

Moreover, the action

$$a * \lambda = [a]_f(\lambda), \quad a \in A, \quad \lambda \in \Lambda_n,$$

induces an isomorphism

$$(A/\mathfrak{m}^n)^\times \to \mathrm{Gal}(K_{\pi,n}/K).$$

On passing to the inverse limit, we obtain an isomorphism

$$A^\times \to \mathrm{Gal}(K_\pi/K).$$

EXAMPLE 3.8 Let $K = \mathbb{Q}_p$ and $f = (T+1)^p - 1$. For each r, choose a p^rth root ζ_{p^r} of 1 in such a way that ζ_p is primitive and $\zeta_{p^r}^p = \zeta_{p^{r-1}}$. Then $\pi_r = \zeta_{p^r} - 1$ and $(\mathbb{Q}_p)_{p,n} = \mathbb{Q}_p[\pi_r] = \mathbb{Q}_p[\zeta_{p^r}]$. Moreover, the isomorphism

$$(\mathbb{Z}_p/(p^n))^\times \to \mathrm{Gal}(\mathbb{Q}_p[\zeta_{p^r}]/\mathbb{Q}_p)$$

is the standard one.

The local Artin map

We define a homomorphism

$$\phi_\pi \colon K^\times \to \mathrm{Gal}((K_\pi \cdot K^{\mathrm{un}})/K)$$

as follows. Let $a \in K^\times$. Because $K_\pi \cap K^{\mathrm{un}} = K$, it suffices to describe the actions of $\phi_\pi(a)$ on K_π and K^{un} separately. Let $a = u\pi^m$, $u \in U$. We decree that $\phi_\pi(a)$ acts on K^{un} as Frob^m, and that it acts on K_π according to the rule

$$\phi_\pi(a)(\lambda) = [u^{-1}]_f(\lambda), \qquad \text{all } \lambda \in \bigcup \Lambda_n.$$

The $^{-1}$ is inserted so that the following theorem is true.

THEOREM 3.9 *Both $K_\pi \cdot K^{\mathrm{un}}$ and ϕ_π are independent of the choice of π.*

The proof will occupy the rest of this section.

Recall that K^{al} is not complete (see ANT, Exercise 7-7); in fact even K^{un} is not complete. We write $\hat{K}^{\mathrm{un}}$ for its completion and B for the valuation ring of $\hat{K}^{\mathrm{un}}$ (the absolute value $|\cdot|$ on K^{un} extends uniquely to $\hat{K}^{\mathrm{un}}$, and B is the set of elements with value ≤ 1). We write σ for the Frobenius automorphism Frob_K of K^{un}/K, and also for its extension to $\hat{K}^{\mathrm{un}}$. For a power series $\theta(T) = \sum b_i T^i \in B[[T]]$, we define $(\sigma\theta)(T)$ to be the power series $\sum (\sigma b_i)\, T^i$.

PROPOSITION 3.10 *Let F_f and F_g be the formal group laws defined by $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\varpi$, where π and $\varpi = u\pi$ are two prime elements of K. Then F_f and F_g become A-isomorphic over B. More precisely, there exists an $\varepsilon \in B^\times$ such that $\sigma\varepsilon = \varepsilon u$, and a power series $\theta(T) \in B[[T]]$ such that:*

(a) $\theta(T) = \varepsilon T +$ *terms of degree* ≥ 2;

(b) $\sigma\theta = \theta \circ [u]_f$;

(c) $\theta(F_f(X,Y)) = F_g(\theta(X), \theta(Y))$;

(d) $\theta \circ [a]_f = [a]_g \circ \theta$.

The last two conditions say that θ is a homomorphism $F_f \to F_g$ commuting with the actions of A, and the first condition implies that θ is an isomorphism (because ε is a unit).

LEMMA 3.11 *The homomorphisms*

$$b \mapsto \sigma b - b \colon B \to B,$$
$$b \mapsto \sigma b / b \colon B^\times \to B^\times,$$

are surjective with kernels A and $A^\times$ respectively.

PROOF. Let R be the valuation ring in K^{un}, and let $\mathfrak{n}$ be its maximal ideal. Then R is a discrete valuation ring, and $\varprojlim R/\mathfrak{n}^n = B$ (see (A.7 below). We shall show by induction that the sequence

$$0 \longrightarrow A/\mathfrak{m}_K^n \longrightarrow R/\mathfrak{n}^n \xrightarrow{\sigma-1} R/\mathfrak{n}^n \longrightarrow 0 \tag{10}$$

is exact. For $n = 1$, the sequence becomes

$$0 \longrightarrow k \longrightarrow \bar{k} \xrightarrow{x\mapsto x^q-x} \bar{k} \longrightarrow 0.$$

Here $\bar{k}$ is the algebraic closure of k. This is obviously exact. Assume that the sequence is exact for $n-1$, and consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R/\mathfrak{n} & \longrightarrow & R/\mathfrak{n}^n & \longrightarrow & R/\mathfrak{n}^{n-1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \sigma-1} & & \downarrow{\scriptstyle \sigma-1} & & \downarrow{\scriptstyle \sigma-1} & & \\ 0 & \longrightarrow & R/\mathfrak{n} & \longrightarrow & R/\mathfrak{n}^n & \longrightarrow & R/\mathfrak{n}^{n-1} & \longrightarrow & 0. \end{array}$$

From the snake lemma, we find that $\sigma - 1 : R/\mathfrak{n}^n \to R/\mathfrak{n}^n$ is surjective and that its kernel has q^n elements. As $A/\mathfrak{n}^n$ is contained in the kernel and has q^n elements, it must equal the kernel. This shows that (10) is exact, and, when we pass to the inverse limit over n, the sequence becomes

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\sigma-1} B \longrightarrow 0,$$

which is therefore exact (see Proposition A.8 below).

The proof for $B^\times$ is similar. □

The inverse of a power series h for composition will be denoted h^{-1}. Thus $h \circ h^{-1} = T = h^{-1} \circ h$.

The proof of the Proposition 3.10 has four steps.

Step 1. Show there exists a $\theta(T) \in B[[T]]$ satisfying (a) and (b).

Step 2. Show that the θ in Step 1 can be chosen so that $g = \sigma\theta \circ f \circ \theta^{-1}$.

Step 3. Show that the power series $\theta(F_f(\theta^{-1}(X), \theta^{-1}(Y)))$ has the properties characterizing $F_f(X, Y)$, and therefore equals it.

Step 4. Show that the power series $\theta \circ [a]_f \circ \theta^{-1}$ has the properties characterizing $[a]_g$, and therefore equals it.

PROOF (OF STEP 1) Choose an $\varepsilon \in B^\times$ such that $\sigma\varepsilon = \varepsilon u$—its existence is ensured by Lemma 3.11. Starting with $\theta_1(T) = \varepsilon T$, we shall construct a sequence of polynomials θ_r such that

$$\begin{aligned} \theta_r(T) &= \theta_{r-1}(T) + bT^r \text{ , some } b \in B, \\ \sigma\theta_r &= \theta_r \circ [u]_f + \text{terms of degree } \geq r+1. \end{aligned}$$

Note, that for $\theta_1(T) = \varepsilon T$, the second equation becomes

$$\sigma\varepsilon T = \varepsilon(uT + \cdots) + \text{terms of degree } \geq 2,$$

which is true because of our choice of ε. Suppose that θ_r has been found, and we wish to find $\theta_{r+1}(T) = \theta_r(T) + bT^{r+1}$. Write $b = a\varepsilon^{r+1}$, $a \in B$. Then the second equation becomes

$$(\sigma\theta_r)(T)+(\sigma a)(\sigma\varepsilon)^{r+1}T^{r+1} \stackrel{?}{=} \theta_r([u]_f(T))+a\varepsilon^{r+1}(uT)^{r+1}+\text{terms of degree } \geq r+1.$$

Thus, we need

$$(\sigma a - a)(\varepsilon u)^{r+1} \stackrel{?}{=} c,$$

where c is the coefficient of T^{r+1} in $\theta_r \circ [u]_f - \sigma\theta_r$. We can choose a to be any element of B such that $\sigma a - a = c/(\varepsilon u)^{r+1}$. □

PROOF (OF STEP 2) Define

$$h = \sigma\theta \circ f \circ \theta^{-1} = \theta \circ [u]_f \circ f \circ \theta^{-1} = \theta \circ f \circ [u]_f \circ \theta^{-1}.$$

Then, because f and $[u]_f$ have coefficients in A,

$$\sigma h = \sigma\theta \circ f \circ [u]_f \circ \sigma\theta^{-1} = \sigma\theta \circ f \circ \theta^{-1} = h.$$

For the middle equality, we used that $[u]_f \circ \sigma\theta^{-1} = \theta^{-1}$ which follows from $\theta \circ [u]_f \circ \sigma\theta^{-1} = T$. Because $\sigma h = h$, it lies in $A[[T]]$. Moreover,

$$h(T) = \sigma\varepsilon \cdot \pi \cdot \varepsilon^{-1}T + \cdots = \varpi T + \text{terms of degree } \geq 2,$$

and

$$h(T) \equiv \sigma\theta \circ (\theta^{-1})^q \equiv \sigma\theta(\sigma\theta^{-1}(T^q)) \equiv T^q \mod \mathfrak{m}_K.$$

Therefore, $h \in \mathcal{F}_\varpi$. Let $\theta' = [1]_{g,h} \circ \theta$. Then θ' obviously still satisfies condition (a) of the proposition, and it still satisfies (b) because $[1]_{g,h} \in A[[T]]$. Moreover,

$$\sigma\theta' \circ f \circ \theta'^{-1} = [1]_{g,h} \circ h \circ [1]_{g,h}^{-1} = g.$$ □

The proofs of Steps 3 and 4 are straightforward applications of Lemma 2.11, and so will be left to the reader.

PROOF (THAT $K_\pi \cdot K^{\text{un}}$ IS INDEPENDENT OF π) Let π and $\varpi = \pi u$ be two prime elements of K. From Proposition 3.10 we find that

$$(\sigma\theta) \circ [\pi]_f = \theta \circ [u]_f \circ [\pi_f] = \theta \circ [\varpi]_f = [\varpi]_g \circ \theta,$$

that is, that

$$(\sigma\theta)(f(T)) = g(\theta(T)).$$

Therefore, for any $\alpha \in K^{\text{al}}$ (recall that this is the *separable* algebraic closure of K),

$$f(\alpha) = 0 \Rightarrow g(\theta(\alpha)) = 0,$$

and, similarly,

$$g(\alpha) = 0 \Rightarrow f(\theta^{-1}(\alpha)) = 0.$$

Therefore θ defines a bijection $\Lambda_{f,1} \to \Lambda_{g,1}$, and so

$$\hat{K}^{\text{un}}[\Lambda_{g,1}] = \hat{K}^{\text{un}}[\theta(\Lambda_{f,1})] \subset \hat{K}^{\text{un}}[\Lambda_{f,1}] = \hat{K}^{\text{un}}[\theta^{-1}(\Lambda_{g,1})] \subset \hat{K}^{\text{un}}[\Lambda_{g,1}].$$

Therefore

$$\hat{K}^{\mathrm{un}}[\Lambda_{g,1}] = \hat{K}^{\mathrm{un}}[\Lambda_{f,1}].$$

Now the next lemma shows that

$$\hat{K}^{\mathrm{un}}[\Lambda_{g,1}] \cap K^{\mathrm{al}} = K^{\mathrm{un}}[\Lambda_{g,1}], \qquad \hat{K}^{\mathrm{un}}[\Lambda_{f,1}] \cap K^{\mathrm{al}} = K^{\mathrm{un}}[\Lambda_{f,1}],$$

and so

$$K^{\mathrm{un}}[\Lambda_{g,1}] = K^{\mathrm{un}}[\Lambda_{f,1}].$$

The argument extends without difficulty to show that

$$K^{\mathrm{un}}[\Lambda_{g,n}] = K^{\mathrm{un}}[\Lambda_{f,n}]$$

for all n, and so $K^{\mathrm{un}} \cdot K_\varpi = K^{\mathrm{un}} \cdot K_\pi$. □

LEMMA 3.12 *Every subfield E of K^{al} containing K is closed (in the topological sense).*

PROOF. Let $H = \mathrm{Gal}(K^{\mathrm{al}}/E)$. Then H fixes every element of E and so, by continuity, it fixes every element in the closure of E. By Galois theory, this implies that E equals its closure in K^{al}. □

PROOF (THAT ϕ_π IS INDEPENDENT OF π.) We shall show that, for any two prime elements π and ϖ,

$$\phi_\pi(\varpi) = \phi_\varpi(\varpi).$$

Since π is arbitrary, this implies that for any other prime element π' of K,

$$\phi_{\pi'}(\varpi) = \phi_\varpi(\varpi) = \phi_\pi(\varpi).$$

Since ϖ is also arbitrary, and the prime elements generate the group $K^\times$, this implies that $\phi_\pi = \phi_{\pi'}$.

On K^{un}, both $\phi_\pi(\varpi)$ and $\phi_\varpi(\varpi)$ induce the Frobenius automorphism. It remains to prove that they have the same effect on K_ϖ.

Let θ be an isomorphism $F_f \to F_g$ over $\hat{K}^{\mathrm{un}}$ as in Proposition 3.10. It induces an isomorphism $\Lambda_{f,n} \to \Lambda_{g,n}$ for all n. By definition, $\phi_\varpi(\varpi)$ is the identity on K_ϖ, and since $K_{\varpi,n}$ is generated over K by the elements $\theta(\lambda)$ for $\lambda \in \Lambda_{f,n}$, it remains to prove that

$$\phi_\pi(\varpi)(\theta(\lambda)) = \theta(\lambda), \qquad \text{all } \lambda \in \Lambda_{f,n}.$$

Write $\varpi = u\pi$. Then $\phi_\pi(\varpi) = \phi_\pi(u) \cdot \phi_\pi(\pi) = \tau\sigma$, say, where

$$\sigma = \begin{cases} \mathrm{Frob}_K & \text{on } K^{\mathrm{un}} \\ \mathrm{id} & \text{on } \lambda \end{cases} \qquad \tau = \begin{cases} \mathrm{id} & \text{on } K^{\mathrm{un}} \\ [u^{-1}]_f & \text{on } \lambda. \end{cases}$$

Using that the series θ has coefficients in $\hat{K}^{\mathrm{un}}$ and (3.10), we find that

$$\phi_\pi(\varpi)(\theta(\lambda)) = \tau\sigma(\theta(\lambda)) = (\sigma\theta)(\tau\lambda) = (\sigma\theta)([u^{-1}]_f(\lambda) = \theta(\lambda).$$

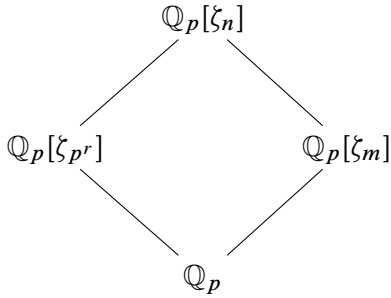
□

EXAMPLE 3.13 We describe the local Artin map $\phi_p: \mathbb{Q}_p^\times \to \mathrm{Gal}(L/\mathbb{Q}_p)$ in the case $L = \mathbb{Q}_p[\zeta]$, where ζ is a primitive nth root of 1.

(a) Suppose n is prime to p. Then L is unramified over $\mathbb{Q}_p$, with degree equal to the degree of the residue field extension. The residue field is $\mathbb{F}_{p^f}$, where p^f is the smallest power of p such that $n|(p^f - 1)$. The map $\phi_p : \mathbb{Q}_p^\times \to \mathrm{Gal}(L/\mathbb{Q}_p)$ sends $u \cdot p^t$ to the tth power of the Frobenius element, and its kernel is $\mathbb{Z}_p^\times \cdot \langle p^f \rangle$,

(b) Suppose n is a power p^r of p. In this case, L is totally ramified of degree $(p-1)p^{r-1}$ over K, and $L = (\mathbb{Q}_p)_{p,n}$ (see 3.8). The map $\phi_p: \mathbb{Q}_p^\times \to \mathrm{Gal}(L/\mathbb{Q}_p)$ can be described as follows: let $a = up^t$, and let $u_0 \in \mathbb{Z}$ represent the class of u in $(\mathbb{Z}_p/p^r\mathbb{Z}_p)^\times$; then $\phi_p(a)$ sends ζ to $\zeta^{u^{-1}}$. Its kernel is $\{up^m \mid u \equiv 1 \mod p^r, \quad m \in \mathbb{Z}\}$.

(c) In the general case, write $n = m \cdot p^r$ with m prime to p. Then we have



The map $\mathbb{Q}_p^\times/\mathrm{Nm}(\mathbb{Q}_p[\zeta_n]^\times) \to \mathrm{Gal}(\mathbb{Q}_p[\zeta_n]/\mathbb{Q}_p)$ can be described as follows: write $a = up^t$, $u \in \mathbb{Z}_p^\times$; then a acts on $\mathbb{Q}_p[\zeta_m]$ by $\zeta_m \mapsto \zeta_m^t$, and it acts on $\mathbb{Q}_p[\zeta_{p^n}]$ by $\zeta_{p^n} \mapsto \zeta_{p^n}^{u_0^{-1}}$, where u_0 is an integer congruent to $u \bmod p^r$.

4 The Local Kronecker-Weber Theorem

The main result proved in this section is that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$. Since this is not needed for the proofs of the main theorems of local class field theory, and is implied by them, this section may be skipped.

The ramification groups of $K_{\pi,n}/K$.

Let L/K be a finite Galois extension with Galois group G. Recall (ANT, 7.57, 7.58,...) that the ith ramification group is defined to be

$$G_i = \{\tau \in G \mid \mathrm{ord}_L(\tau a - a) \geq i + 1, \text{ all } a \in \mathcal{O}_L\};$$

moreover, for $i \geq 1$,

$$G_i = \{\tau \in G_0 \mid \mathrm{ord}_L(\tau\Pi - \Pi) \geq i + 1\},$$

where Π is a prime element for L. Here ord_L is the normalized valuation $L^\times \twoheadrightarrow \mathbb{Z}$. Then $G/G_0 = \mathrm{Gal}(l/k)$, and there are inclusions:

$$\begin{aligned} (\Pi \mapsto \tau\Pi/\Pi \mod \Pi): G_0/G_1 &\hookrightarrow l^\times \\ (\Pi \mapsto (\tau\Pi - \Pi)/\Pi^{i+1} \mod \Pi): G_i/G_{i+1} &\hookrightarrow l, \end{aligned}$$

where $l \supset k$ are the residue fields of L and K. Thus $(G_0 : G_1) | q-1$ and $(G_i : G_{i+1}) | q$ for $i \geq 1$. Moreover $G_i = \{1\}$ for i sufficiently large.

Let

$$U^{(0)} = U = A^\times,$$
$$U^{(i)} = 1 + \mathfrak{m}^i, \quad i \geq 1.$$

Then we have a filtration

$$U/U^{(n)} \supset U^{(1)}/U^{(n)} \supset \cdots \supset U^{(n)}/U^{(n)} = 0$$

on $A^\times/(1+\mathfrak{m}^n) = U/U^{(n)}$.

PROPOSITION 4.1 *Let $L = K_{\pi,n}$. Under the isomorphism $A^\times/U^{(n)} \xrightarrow{\simeq} G$ of Theorem 3.6, $U^{(i)}/U^{(n)}$ maps onto G_{q^i-1}.*

PROOF. We take $f = \pi T + T^q$. Certainly $G = G_0$, and $U^{(0)}/U^{(n)}$ maps onto G_0. Now take $i \geq 1$, and let $u \in U^{(i)} \smallsetminus U^{(i+1)}$. Then $u = 1 + v\pi^i$ with $v \in A^\times$, and

$$[u]_f(\pi_n) = [1]_f(\pi_n) + [v]_f[\pi^i]_f(\pi_n) = \pi_n + [v]_f(\pi_{n-i}) = \pi_n + (\text{unit})\pi_{n-i}.$$

For every $i \geq 1$, $\pi_i = \pi\pi_{i+1} + \pi_{i+1}^q = \pi_{i+1}^q(\frac{\pi\pi_{i+1}}{\pi_{i+1}^q} + 1) = \pi_{i+1}^q \times$ unit because $\operatorname{ord}(\frac{\pi}{\pi_{i+1}^{q-1}}) > 0$. Hence $\pi_{n-i} = \pi_n^{q^i} \times$ unit, and

$$[u]_f(\pi_n) - \pi_n = \pi_n^{q^i} \times \text{unit}.$$

By definition, this means that $[u]_f \in G_{q^i-1}$, $[u]_f \notin G_{q^i}$. Since this is true for all i, it implies that $U^{(i)}$ maps onto G_{q^i-1}. □

Hence

$$\begin{aligned} G_0 &= G \\ G_{q-1} &= G_{q-2} = \cdots = G_1 \\ G_{q^2-1} &= G_{q^2-2} = \cdots = G_q \\ &\cdots \\ G_{q^n-1} &= 1 \end{aligned}$$

is a complete set of distinct ramification groups for $K_{\pi,n}/K$.

Upper numbering on ramification groups

Let L be a finite Galois extension of K with Galois group G. We extend the definition of G_u to all real numbers $u \geq -1$, by setting

$$G_u = G_i, \quad \text{where } i \text{ is the least integer} \geq u.$$

For $u > 0$,

$$G_u = \{\tau \in G_0 \mid \operatorname{ord}_L(\tau\Pi - \Pi) \geq i+1\}.$$

Define $\varphi\colon \mathbb{R}_{\geq 0} \to \mathbb{R}$ to be the unique continuous piecewise linear function such that

$$\begin{cases} \varphi(0) &= 0 \\ \varphi'(u) &= (G_0 : G_u)^{-1} \text{ if } u \text{ is not an integer.} \end{cases}$$

Define $G^v = G_u$ if $v = \varphi(u)$, i.e., $G^v = G_{\varphi^{-1}(v)}$.

EXAMPLE 4.2 Let $L = K_{\pi,n}$. Then

$$(G_0 \colon G_1) = q - 1, \qquad G_1 = G_2 = \cdots = G_{q-1}.$$

Thus $\varphi'(u) = \frac{1}{q-1}$ for $0 < u < q-1$, and the first segment of the graph of φ runs from $(0,0)$ to $(q-1,1)$; hence $G^1 = G_{q-1}$. Next

$$(G_{q-1} \colon G_q) = q, \qquad G_q = G_{q+1} = \cdots = G_{q^2-1}.$$

Thus $\varphi'(u) = \frac{1}{q(q-1)}$ for $q-1 < u < q^2-1$, and the second segment of the graph of φ runs from $(q-1,1)$ to $(q^2-1,2)$. Thus $G^2 = G_{q^2-1}$. Continuing in this fashion, we arrive at the following picture,

$$\begin{array}{ccccccccc} G_0 & \overset{q-1}{\supset} & G_{q-1} & \overset{q}{\supset} & G_{q^2-1} & \supset \cdots & \supset G_{q^n-1} = 1 \\ \| & & \| & & \| & & \| \\ G^0 & & G^1 & & G^2 & & G^n \end{array}$$

PROPOSITION 4.3 *Under the isomorphism $A^\times/U^{(n)} \to G$,*

$$U^{(i)}/U^{(n)} \xrightarrow{\approx} G^i.$$

PROOF. Immediate consequence of (4.1) and (4.2). □

The upper numbering is defined so as to be compatible with the passage to the quotient (whereas the lower numbering is compatible with passage to the subgroups).

PROPOSITION 4.4 *Consider Galois extensions $M \supset L \supset K$, and let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$ (assumed normal) so that $G/H = \mathrm{Gal}(L/K)$. Then*

$$(G/H)^v = \mathrm{Im}(G^v \to G/H),$$

i.e., $(G/H)^v = G^v H/H$.

PROOF. See Serre 1962, IV.3, Pptn 14. □

Now consider an infinite Galois extension Ω/K. Using (4.4) we can define a filtration on $G = \mathrm{Gal}(\Omega/K)$:

$$\tau \in G^v \iff \tau \in \mathrm{Gal}(L/K)^v, \qquad \text{all } L/K \text{ finite and Galois } L \subset \Omega.$$

DEFINITION 4.5 For a finite Galois extension L/K, v is called a ***jump*** in the filtration $\{G^v\}$ if, for all $\varepsilon > 0$, $G^v \neq G^{v+\varepsilon}$.

THEOREM 4.6 (HASSE-ARF) *If L/K is abelian, then the jumps are integers, i.e., if $G_i \neq G_{i+1}$, then $\varphi(i) \in \mathbb{Z}$.*

PROOF. See Serre 1962, V.7. (The proof is fairly elementary, but complicated. It is does not require that residue fields be finite, but only that the residue field extension be separable.)□

Thus, for a finite abelian extension L/K, the filtration on $G_0 = G^0$ is of the form

$$G^0 \supsetneq G^{i_1} \supsetneq G^{i_2} \dots . \qquad i_j \in \mathbb{N}.$$

Moreover $G^n = \{1\}$ for n sufficiently large, and $(G^{i_j}: G^{i_j+1})$ divides $q-1$ or q. For an infinite abelian extension, the same statements hold, except that the filtration need not terminate: we can only say that

$$\bigcap G^i = \{1\}.$$

EXAMPLE 4.7 Let $L = K_{\pi,n}$. If $G_i \neq G_{i+1}$, then $i = 0, q-1, \dots, q^n - 1$, and at those points φ takes the values $1, 2, 3, \dots, n$. Thus we have verified the Hasse-Arf theorem for all these extensions, and, because of (4.4), all subextensions. In particular, we have shown that the local Kronecker-Weber theorem implies the Hasse-Arf theorem.

The local Kronecker-Weber theorem

As usual, K is a local nonarchimedean field, and all extensions of K will be required to be subfields of a fixed separable algebraic closure K^{al} of K.

THEOREM 4.8 *For every prime element π of K,*

$$K_\pi \cdot K^{\mathrm{un}} = K^{\mathrm{ab}}.$$

LEMMA 4.9 *Let L be an abelian totally ramified extension of K. If $L \supset K_\pi$, then $L = K_\pi$.*

PROOF. Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/K_\pi)$, so that $G/H = \mathrm{Gal}(K_\pi/K)$. Consider the diagram (of abelian groups)

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G^{n+1} \cap H & \longrightarrow & G^{n+1} & \longrightarrow & (G/H)^{n+1} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G^n \cap H & \longrightarrow & G^n & \longrightarrow & (G/H)^n & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \dfrac{G^n \cap H}{G^{n+1} \cap H} & \longrightarrow & \dfrac{G^n}{G^{n+1}} & \longrightarrow & \dfrac{(G/H)^n}{(G/H)^{n+1}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

The columns are obviously exact, and Proposition 4.4 shows that the top two rows are exact. Therefore, the third row is exact (by the snake lemma, for example) and so

$$\underset{\leq q}{(G^n: G^{n+1})} = \underset{= q-1 \text{ or } q}{((G/H)^n: (G/H)^{n+1})} \quad (G^n \cap H: G^{n+1} \cap H).$$

From this we deduce that $G^n \cap H = G^{n+1} \cap H$ for all n. Thus

$$G^{n+1} \cap H = G^n \cap H = \cdots = G^0 \cap H = H,$$

i.e., $H \subset G^{n+1}$ for all n. Since $\bigcap G^n = 1$, this shows that $H = 1$. □

LEMMA 4.10 *Every finite unramified extension of K_π is contained in $K_\pi \cdot K^{\mathrm{un}}$.*

PROOF. Let L be an unramified extension of K_π. Then $L = K_\pi \cdot L'$ for some unramified extension L' of $K_{\pi,n}$ for some n.[3] Now apply (ANT, 7.58) to see that $L' = K_{\pi,n} \cdot L''$ for some unramified extension L'' of K. □

LEMMA 4.11 *Let L be a finite abelian extension of K_π of exponent m (i.e., $\tau^m = 1$ all $\tau \in \mathrm{Gal}(L/K)$), and let K_m be the unramified extension of K_π of degree m. Then there exists a totally ramified abelian extension L_t of K_π such that*

$$L \subset L_t \cdot K_m = L \cdot K_m.$$

PROOF. For every $\tau \in \mathrm{Gal}(LK_m/K_\pi)$, $\tau^m|L = 1 = \tau^m|K_m$, and so $\mathrm{Gal}(LK_m/K_\pi)$ is still abelian of exponent m. Let $\tau \in \mathrm{Gal}(LK_m/K_\pi)$ be such that $\tau|K_m$ is the Frobenius automorphism. Then τ has order m, and so

$$\mathrm{Gal}(LK_m/K) = \langle\tau\rangle \times H \quad \text{(direct product)}.$$

for some subgroup H. Let $L_t = L^{\langle\tau\rangle}$; then L_t is totally ramified over K and $L \cdot K_m = L_t \cdot K_m$. □

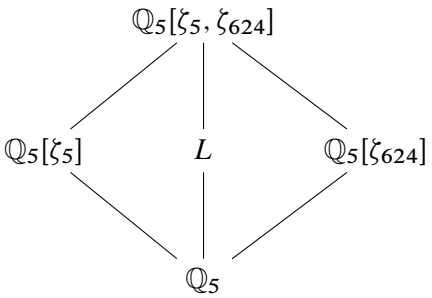
PROOF (OF THEOREM 4.8) Let L be a finite abelian extension of K; we have to show that $L \subset K_\pi \cdot K^{\mathrm{un}}$. Lemma 4.11 applied to $L \cdot K_\pi$ shows that there exists a totally ramified extension L_t of K_π and an unramified extension L_u of K_π such that

$$L \cdot K_\pi \subset L_t \cdot L_u.$$

Now (4.9) implies that $L_t \subset K_\pi$ and (4.10) implies that $L_u \subset K_\pi \cdot K^{\mathrm{un}}$. □

COROLLARY 4.12 *Every finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension.*

EXAMPLE 4.13 A finite abelian extension L of K need not be of the form $L_t \cdot L_u$ with L_t totally ramified over K and L_u unramified over K. Consider:



[3] The finite extension L of K_π is separable, so generated by an element θ whose minimal K_π-equation has only finitely many coefficients. Since K_π is union of the chain of subfields $K_{\pi,n}$, one of these must contain all the coefficients of your polynomial.

The field $\mathbb{Q}_5[\zeta_5]$ is totally ramified of degree 4 over $\mathbb{Q}_5$ with Galois group $(\mathbb{Z}/5)^\times$, which is cyclic of order 4. Note that $624 = 5^4 - 1$, and so $\mathbb{Q}_5[\zeta_{624}]$ is unramified of degree 4 over $\mathbb{Q}_5$, and its Galois group is also cyclic. Clearly

$$\mathrm{Gal}(\mathbb{Q}_5[\zeta_{3120}]/\mathbb{Q}_5) = \langle\sigma\rangle \times \langle\tau\rangle,$$

where

$$\begin{cases} \sigma(\zeta_{624}) = \zeta_{624}^5 \\ \sigma(\zeta_5) = \zeta_5 \end{cases} \quad \begin{cases} \tau(\zeta_{624}) = \zeta_{624} \\ \tau(\zeta_5) = \zeta_5^2 \end{cases}.$$

Let L be the fixed field of $\langle\sigma^2\tau\rangle$. Then L is a cyclic Galois extension of $\mathbb{Q}_5$ of degree 4. Its maximal unramified subfield

$$L_u = L \cap \mathbb{Q}_5[\zeta_{624}] = \mathbb{Q}_5[\zeta_{624}]^{\langle\sigma^2\rangle} = \mathbb{Q}_5[\zeta_{624}^{25}]$$

which has degree 2 over $\mathbb{Q}_5$. If there existed field a L_t such that $L = L_t \cdot L_u$, then $\mathrm{Gal}(L/\mathbb{Q}_5)$ would be the product of two cyclic groups of order 2, contradicting the fact that it is cyclic.

We recover the fact that $K_\pi \cdot K^{\mathrm{un}}$ is independent of π without using Proposition 3.10. However, this proposition is still required to show that ϕ_π is independent of π.

REMARK 4.14 The original Kronecker-Weber Theorem (proved by Hilbert in 1896 using an analysis of the ramification groups after earlier incomplete proofs by Kronecker and Weber) states that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension. For $\mathbb{Q}_p$ the same statement is called the Local Kronecker-Weber Theorem, and Theorem 4.8 is usually referred to as the Local Kronecker-Weber Theorem for K. It is in fact possible to give an elementary proof of the Local Kronecker-Weber Theorem for $\mathbb{Q}_p$ (see Cassels 1986, p 151).

REMARK 4.15 In Chapter III, we shall deduce the Local Kronecker-Weber Theorem from Theorem 1.1 without making use of the Hasse-Arf theorem—this was the original approach of Lubin and Tate. The above proof follows Gold 1981 and Lubin 1981 (apparently a similar proof was found earlier by Leopoldt but not published). For a proof of the local Kronecker-Weber theorem for local fields of characteristic zero that does not make use of the Hasse-Arf theorem or cohomology, but which is more complicated than the above, see Rosen 1981. As Iwasawa points out (1986, p. 115), once Proposition 4.4 and certain properties of the abelian extensions $K_{\pi,n}/K$ are taken for granted, then the Local Kronecker-Weber Theorem for K and the Hasse-Arf Theorem are essentially equivalent.

The global Kronecker-Weber theorem

Since it is now so easy, we might as well prove the original Kronecker-Weber theorem.

THEOREM 4.16 *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

LEMMA 4.17 *Let K be a finite Galois extension of $\mathbb{Q}$ with Galois group G. Then G is generated by the inertia groups of the prime ideals $\mathfrak{p}$ of K that are ramified in the extension $K/\mathbb{Q}$.*

PROOF. Let H be the subgroup of G generated by the inertia groups, and let M be the fixed field of H. Then $K^{I(\mathfrak{p})} \supset M$ for all prime ideals $\mathfrak{p}$ of K, and so $\mathfrak{p} \cap M$ is unramified in the extension $M/\mathbb{Q}$. Therefore M is an unramified extension of $\mathbb{Q}$, and so equals $\mathbb{Q}$ (by ANT, 4.9). □

PROOF (OF THE KRONECKER-WEBER THEOREM) [4]Let K be an abelian extension of $\mathbb{Q}$. Let p be a prime number, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over it. From the local Kronecker-Weber theorem, $K_\mathfrak{p}$ is contained in a cyclotomic extension of $\mathbb{Q}_p$, say $K_\mathfrak{p} = \mathbb{Q}_p[u_p, v_p]$, where u_p is a p^{s_p}th root of 1 and v_p is a root of 1 of order prime to p. Note that s_p depends only on p (not $\mathfrak{p}$) because $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ acts transitively on the primes lying over p, and hence on the set of fields $K_\mathfrak{p}$.

Let L be the cyclotomic extension of $\mathbb{Q}$ generated by the p^{s_p}th roots of 1 for all prime numbers p ramified in K, and let $K' = K \cdot L$. Then K' is again abelian over $\mathbb{Q}$, and for every prime $\mathfrak{p}'$ of K', we have

$$K'_{\mathfrak{p}'} \subset \mathbb{Q}_p[u_p, w_p], \qquad (*)$$

where w_p is a root of 1 of order prime to p. Clearly it suffices to prove the theorem with K replaced with K', and so we can assume $K \supset L$.

We now have

$$[K:\mathbb{Q}] \geq [L:\mathbb{Q}] = \prod_p \varphi(p^{s_p}) \quad \text{(product over } p \text{ ramifying in } K\text{)}.$$

Since the Galois group G of $K/\mathbb{Q}$ is commutative, the inertia group $I(\mathfrak{p})$ depends only on the underlying prime p, and so we denote it $I(p)$. From (*) we have

$$(I(p):1) \leq \varphi(p^{s_p})$$

because $I(p)$ is a quotient of the corresponding group for $\mathbb{Q}_p[u_p, w_p]$. By (4.17), G is generated by the groups $I(p)$, and so there is a surjective map $\prod I(p) \to G$; thus

$$(G:1) \leq \prod_p (I(p):1) \leq \prod \varphi(p^{s_p}).$$

But $(G:1) = [K:\mathbb{Q}]$ and so we have equality everywhere, and $K = L$. □

REMARK 4.18 At this point, it is not too difficult to complete the proofs of main theorems of global class field theory (see the Introduction) in the case $K = \mathbb{Q}$. From the fact that L is contained in a cyclotomic extension we deduce that the Artin map $\phi_{L/\mathbb{Q}}$ has a modulus. Now use Dirichlet's theorem on the density of primes in arithmetic progressions to show that $\varphi_{L/\mathbb{Q}}$ is surjective. We know that $\mathrm{Nm}(I_L^S)$ is contained in the kernel, and so the only thing that is lacking at this point is that

$$(I_K^S : \mathrm{Nm}\, I_L^S \cdot i(K_{\mathfrak{m},1})) \leq [L:\mathbb{Q}].$$

This is the ***first inequality***, which is not difficult by analytic methods (see Janusz 1996, IV, 5.6). Once one has that, the existence theorem follows from the fact that $\mathbb{Q}[\zeta_m]$ has modulus $(m)\infty$.

[4]Following Cassels 1986, p. 236.

Notes

The original source for the theory of Lubin-Tate extensions is Lubin and Tate 1965. The theory is also treated in Serre 1967a, Iwasawa 1986, and Fesenko and Vostokov 1993.

Where did it all come from?

We have seen that the Lubin-Tate formal group laws provide a remarkably simple solution to an apparently very complicated problem, that of giving explicit generators for the largest abelian extension of a local field and describing how the Galois group acts on them. The only mystery is how anyone ever thought of them. The following speculations may help.

That such a theory might exist was suggested by the theory of complex multiplication of elliptic curves. Here one shows that, for a quadratic imaginary number field K, there exists an elliptic curve E, unique up to isogeny, having $\mathcal{O}_K$ as its endomorphism ring. For every n, the points of order dividing n on E form a cyclic $\mathcal{O}_K$-module, and it is this fact that allows one to prove that adjoining their coordinates gives an abelian extension.

In seeking an analogous theory for local fields, it is natural to replace the algebraic group E by the local analogue, namely, by a formal group law. Thus we seek a formal group law whose endomorphism ring is so large that its torsion points form a cyclic module. The obvious candidate for the endomorphism ring is again the ring of integers $\mathcal{O}_K$ in K. Initially, it is natural to ask only that the formal group admit an endomorphism corresponding to a prime element π of $\mathcal{O}_K$. Considerations of the heights of formal group laws together with the desire for the torsion points to form a cyclic module suggest that this endomorphism should be given by a power series $f(T)$ such that $f(T) \equiv T^q \bmod \mathfrak{m}$. Moreover, since we truly want the formal group to depend on the choice of π (because the extension K_π we wish to construct does), it is natural to require that $f(T) = \pi T + \cdots$. Thus, we are led to the set $\mathcal{F}_\pi$, and once we have that, the theory follows naturally.

Actually, the true story is more interesting — see below.

Lubin mo220796

Since I had read and enjoyed Lazard's paper on one-dimensional formal group (laws), which dealt with the case of a base field of characteristic p, I decided to look at formal groups over p-adic rings. For whatever reason, I wanted to know about the endomorphism rings of these things, and gradually recognized the similarity between, on the one hand, the case of elliptic curves and their supersingular reduction mod p, when that phenomenon did occur, and, on the other hand, formal groups over p-adic integer rings of higher height than 1.

I had taken, or sat in on, Tate's first course on Arithmetic on Elliptic Curves, and was primed for all of this. In addition, I was aware of Weierstrass Preparation, and the power it gave to anyone who wielded it. And in the attempt to prove a certain result for my thesis, I had thought of looking at the torsion points on a formal group, and I suppose it was clear to me that they formed a module over the endomorphism ring. Please note that it was not my idea at all to use them as a representation module for the Galois group.

But Tate was looking over my shoulder at all times, and no doubt he saw all sorts of things that I was not considering. At the time of submission of my thesis, I did not have a construction of formal groups of height h with endomorphism ring o equal to the integers of a local field k of degree h over $\mathbb{Q}_p$. Only for the unramified case, and I used extremely tiresome degree-by-degree methods based on the techniques of Lazard. Some while after

my thesis, I was on a bus from Brunswick to Boston, and found not only that I could construct formal groups in all cases that had this maximal endomorphism structure, but that one of them could take the polynomial form $\pi x + x^q$. Tate told me that when he saw this, Everything Fell Into Place. The result was the wonderful and beautiful first Lemma in our paper, for which I can claim absolutely no responsibility. My recollection, always undependable, is that the rest of the paper came together fairly rapidly. Remember that Tate was already a master of all aspects of Class Field Theory. But if the endomorphism ring of your formal group is $\mathfrak{o}$ and the Tate module of the formal group is a rank-one module over this endomorphism ring, can the isomorphism between the Galois group of $k(F[p^\infty])$ over k and the subgroup $\mathfrak{o}^* \subset k^*$ fail to make you think of the reciprocity map?

TATE, LETTER TO SERRE JANUARY 10, 1964; COLLECTED WORKS, L8

[From Lubin's results] we get a homomorphism $G_K \to U_K$ = units in K. Restricting this to the inertia group $G_{K^{\text{un}}}$ we get a homomorphism $G_{K^{\text{un}}} \to U_K$, which is probably canonical by the unicity remarks above, and which it is impossible to doubt is in fact the *reciprocity law isomorphism* (or its negative!)...The miracle seems to be that once one abandons algebraic groups, and goes to formal groups, the theory of complex multiplication applies *universally* (locally).

A Appendix: Infinite Galois Theory and Inverse Limits

We review two topics required for this chapter (see also FT, Chapter 7).

Galois theory for infinite extensions

Fix a field K.

DEFINITION A.1 A field $\Omega \supset K$ (not necessarily of finite degree) is said to be ***Galois*** over K if

(a) it is algebraic and separable over K, i.e., every element of Ω is a simple root of a polynomial with coefficients in K;

(b) it is normal over K, i.e., every irreducible polynomial with coefficients in K having a root in Ω splits in $\Omega[X]$.

PROPOSITION A.2 *A field Ω is Galois over K if and only if it is a union of finite Galois extensions of K.*

PROOF. Suppose Ω is Galois over K. For every $\alpha \in \Omega$, the splitting field in Ω of the minimal polynomial of α over K is a finite Galois extension of K, and Ω is the union of such fields. Conversely, if Ω is a union of finite Galois extensions of K, then it is algebraic and separable over K. Moreover, if $f(X) \in K[X]$ has a root in Ω, then it has a root in some finite Galois subextension E of Ω, and therefore splits in $E[X]$. □

If Ω is a Galois extension of K, then the ***Galois group*** $\mathrm{Gal}(\Omega/K)$ is defined to be the group of automorphisms of Ω fixing the elements of K, endowed with the topology for which the sets

$$\mathrm{Gal}(\Omega/E), \quad \Omega \supset E \supset K, \quad [E:K] < \infty$$

form a fundamental system of neighbourhoods of 1. This means that two elements of $\mathrm{Gal}(\Omega/K)$ are close if they agree on some "large" field E, $\Omega \supset E \supset K$, $[E\colon K] < \infty$.

PROPOSITION A.3 *The group $\mathrm{Gal}(\Omega/K)$ is compact and Hausdorff.*

PROOF. Consider the map

$$\sigma \mapsto \sigma|E\colon \mathrm{Gal}(\Omega/K) \to \prod \mathrm{Gal}(E/K),$$

where the product runs over all $E \subset \Omega$ with E finite and Galois over K. Proposition A.2 implies that the map is injective. When we endow each group $\mathrm{Gal}(E/K)$ with the discrete topology, and the product with the product topology, then the topology induced on $\mathrm{Gal}(\Omega/K)$ is the above topology. I claim that the image is closed. The image is equal to the set of families $(\sigma_E)_E$ such that $\sigma_{E'}|E = \sigma_E$ whenever $E' \supset E$. Suppose that (σ_E) is not in the image. Then there exists a pair of fields $E_2 \supset E_1$ such that $\sigma_{E_2}|E_1 \neq \sigma_{E_1}$. Let

$$U = \prod_{E \neq E_1, E_2} \mathrm{Gal}(E/K) \times \{\sigma_{E_2}\} \times \{\sigma_{E_1}\}$$

This is an open neighbourhood of $(\sigma_E)_E$, and $U \cap \mathrm{Im}(\mathrm{Gal}(\Omega/K)) = \emptyset$. □

The topology on $\mathrm{Gal}(\Omega/K)$ is discrete if and only if Ω is a finite extension of K.

THEOREM A.4 *Let Ω be a (possibly infinite) Galois extension of K with Galois group G. Then there is a one-to-one correspondence between the subfields of Ω and the closed subgroups of G. More precisely:*

(a) *For a subfield E of Ω, $H \stackrel{\text{def}}{=} \mathrm{Gal}(\Omega/E)$ is a closed subgroup of G, and $E = \Omega^H$.*

(b) *If H is a subgroup of G, then $\mathrm{Gal}(\Omega/\Omega^H)$ is the closure of H in $\mathrm{Gal}(\Omega/K)$.*

Moreover, the normal closed subgroups of G correspond to the Galois extensions of K, and the open subgroups of G correspond to the finite extensions of K.

PROOF. Let $E \subset \Omega$ be a finite extension of K. Because every K-homomorphism $E \to \Omega$ extends to Ω, the map $\sigma \mapsto \sigma|\Omega\colon \mathrm{Gal}(\Omega/K) \to \mathrm{Hom}_K(E, \Omega)$ is surjective, and so induces a bijection

$$\mathrm{Gal}(\Omega/K)/\mathrm{Gal}(\Omega/E) \to \mathrm{Hom}_K(E, \Omega).$$

This shows that $\mathrm{Gal}(\Omega/E)$ is of finite index $[E : K]$ in $\mathrm{Gal}(\Omega/E)$. Because it is open (by definition), it is also closed (its complement is a finite union of open cosets).

Let $E \subset \Omega$ be an arbitrary extension of K. Then $E = \bigcup E_i$, where the E_i run over the finite extensions of K contained in E. Correspondingly, $\mathrm{Gal}(\Omega/E) = \bigcap \mathrm{Gal}(\Omega/E_i)$, which is therefore closed. Moreover, if $\alpha \in \Omega$ is not fixed by $\mathrm{Gal}(\Omega/E)$, then it is not fixed by any $\mathrm{Gal}(\Omega/E_i)$, and so does not lie in E. Thus $E = \Omega^{\mathrm{Gal}(\Omega/E)}$.

Let H be a subgroup of $\mathrm{Gal}(\Omega/K)$, and let $H' = \mathrm{Gal}(\Omega/\Omega^H)$. It follows from the Galois theory of finite extensions that, for every open subgroup U of $\mathrm{Gal}(\Omega/K)$, $UH = UH'$, and it follows from the theory of topological groups, the closure of H is $\bigcap UH$ (intersection over the open subgroups U of $\mathrm{Gal}(\Omega/K)$), and so $\bar{H} = \bigcap UH = \bigcap UH' = H'$. □

EXAMPLE A.5 (a) Endow $\mathbb{Z}$ with the topology for which the subgroups of finite index form a fundamental system of neighbourhoods, and let $\hat{\mathbb{Z}}$ be the completion. Then $\hat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$, and $\hat{\mathbb{Z}}/m\hat{\mathbb{Z}} = \mathbb{Z}/m\mathbb{Z}$ for every m. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$. There is a canonical isomorphism

$$\hat{\mathbb{Z}} \to \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$$

sending $1 \in \hat{\mathbb{Z}}$ to the automorphism $x \mapsto x^q$. The extension of $\mathbb{F}_q$ of degree m corresponds to the subgroup $m\hat{\mathbb{Z}}$ of $\hat{\mathbb{Z}}$. Let σ be the automorphism of $\mathbb{F}/\mathbb{F}_q$ such that $\sigma(x) = x^q$. For $\alpha \in \hat{\mathbb{Z}}$, define σ^α to be the element of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ such that, for each m, $\sigma^\alpha|\mathbb{F}_{q^m} = \sigma^a|\mathbb{F}_{q^m}$ for every $a \in \mathbb{Z}$ sufficiently close to α (depending on m). The above isomorphism sends α to σ^α. (For a detailed description of $\hat{\mathbb{Z}}$ and the isomorphism $\hat{\mathbb{Z}} \to \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$, see Artin 1951, 9.2.)

(b) Let $\Omega_p = \bigcup_r \mathbb{Q}[\zeta_{p^r}]$, where ζ_{p^r} is a primitive p^rth root of 1. For $u \in \mathbb{Z}_p^\times$, write $u = a_0 + a_1 p + a_2 p^2 + \cdots$, $0 \le a_i \le p-1$, and define

$$\zeta_{p^r}^u = \zeta_{p^r}^{a_0 + a_1 p + \cdots + a_s p^s}, \text{ every } s \ge r-1.$$

This defines an action of $\mathbb{Z}_p^\times$ on Ω_p, and in fact an isomorphism of topological groups

$$\mathbb{Z}_p^\times \to \mathrm{Gal}(\Omega_p/\mathbb{Q}).$$

(c) Let $\Omega = \bigcup \mathbb{Q}[\zeta_n]$, where n is a primitive nth root of 1. Then

$$\Omega = \Omega_2 \cdot \Omega_3 \cdot \Omega_5 \cdots, \quad \Omega_p \cap \Omega_{p'} = \mathbb{Q}, \quad p \ne p'.$$

Just as in the case of a finite number of finite Galois extensions, this implies that

$$\mathrm{Gal}(\Omega/\mathbb{Q}) = \prod \mathrm{Gal}(\Omega_p/\mathbb{Q})$$

(topological product of closed subgroups). Thus there is an isomorphism

$$\hat{\mathbb{Z}}^\times \to \mathrm{Gal}(\Omega/\mathbb{Q}).$$

It can be described as follows: if ζ is an nth root of 1 and $u \in \hat{\mathbb{Z}}^\times$, then

$$\zeta^u = \zeta^m \text{ for any } m \in \mathbb{Z} \text{ with } \quad m \equiv u \mod n.$$

(d) Let $\Omega_p = \bigcup \mathbb{Q}[\zeta_{p^r}]$, as in (b). Then

$$\mathbb{Z}_p^\times \simeq \Delta_p \times C_p,$$

where $\Delta_p \simeq (\mathbb{Z}/(p))^\times \approx \mathbb{Z}/(p-1)$ for $p \ne 2$ and $\Delta_2 = \mathbb{Z}/2\mathbb{Z}$, and $C_p \approx \mathbb{Z}_p$. Let $\Omega'_p = \Omega_p^{\Delta_p}$. Then $\mathrm{Gal}(\Omega'_p/\mathbb{Q}_p) \approx \mathbb{Z}_p$. Let

$$\Omega' = \Omega'_2 \cdot \Omega'_3 \cdots$$

(composite inside $\mathbb{Q}^{\mathrm{al}}$). Then $\mathrm{Gal}(\Omega'/\mathbb{Q}) \approx \prod \mathbb{Z}_p \simeq \hat{\mathbb{Z}}$.

(e) For every finite extension K of $\mathbb{Q}$, $K\cdot\Omega'$ is a Galois extension of K with Galois group isomorphic to a subgroup of finite index in $\hat{\mathbb{Z}}$. But every such subgroup is again isomorphic to $\hat{\mathbb{Z}}$ (because it is again the completion of a subgroup of $\mathbb{Z}$ of finite index). Therefore $\mathrm{Gal}(K \cdot \Omega'/K) \approx \hat{\mathbb{Z}}$. If we fix an isomorphism, and let K_m be the field corresponding to $m\hat{\mathbb{Z}}$, then we see that:

(a) K_m is cyclic of degree m;

(b) K_m is cyclotomic, i.e., contained in an extension of K obtained by adjoining roots of 1.

REMARK A.6 In general, there may exist subgroups of finite index in $\mathrm{Gal}(\Omega/K)$ which are not open, even when $K = \mathbb{Q}$ (see FT, 7.26).

Inverse limits

A partially ordered set $(I, \preceq)$ is said to be ***directed*** if, for any $\alpha, \beta \in I$, there exists a $\gamma \in I$ such that $\alpha, \beta \preceq \gamma$. For example, the set of positive integers ordered by divisibility,

$$m \preceq n \iff m|n,$$

is directed.

An ***inverse system*** (or ***projective system)*** of sets is a family $(S_\alpha)_{\alpha \in I}$ of sets indexed by a directed set I together with, for each pair $\alpha \preceq \beta$, a map $\varphi_{\alpha,\beta}\colon S_\beta \to S_\alpha$ such that

(a) for all $\alpha \in I$, $\varphi_{\alpha,\alpha}$ is the identity map;

(b) for all $\alpha \preceq \beta \preceq \gamma$ in I, $\varphi_{\alpha,\beta} \circ \varphi_{\beta,\gamma} = \varphi_{\alpha,\gamma}$.

A set S together with, for each $\alpha \in I$, a map $\varphi_\alpha\colon S \to S_\alpha$ such that $\varphi_\alpha = \varphi_{\alpha,\beta} \circ \varphi_\beta$ is said to be the ***inverse limit*** (or ***projective limit***) of the inverse system (S_α), $(\varphi_{\alpha,\beta})$ if it satisfies the obvious universal property.

Every inverse system of sets, groups, or rings has an inverse limit. For example, $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$.

EXAMPLE A.7 The completion $\hat{R}$ of a discrete valuation ring R is canonically isomorphic to $\varprojlim R/\mathfrak{m}^n$, where $\mathfrak{m}$ is the maximal ideal in R.

The profinite completion of a group G is defined to be $\varprojlim G/H$, where H runs through the normal subgroups of finite index in G.

PROPOSITION A.8 *The inverse limit of an inverse system of exact sequences of finite abelian groups is again exact.*

REMARK A.9 The Galois group $\mathrm{Gal}(\Omega/K)$ is the projective limit of the groups $\mathrm{Gal}(E/K)$, where E runs over the subfields of Ω that are finite and Galois over K. A topological group that is a projective limit of finite groups is called a ***profinite group.*** They are precisely the compact totally disconnected topological groups. (A topological space is ***totally disconnected*** if its connected components are the one-point subsets.) See Serre 1964 or Shatz 1972.

Chapter II

The Cohomology of Groups

We take a respite from number theory and do some homological algebra. In an appendix to the chapter, we review the general theory of derived functors.

1 Cohomology

The category of G-modules

Let G be a group. A ***G-module*** is an abelian group M together with a map

$$(g, m) \mapsto gm: G \times M \to M$$

such that, for all $g, g' \in G$, $m, m' \in M$,

(a) $g(m + m') = gm + gm'$;

(b) $(gg')(m) = g(g'm)$, $1m = m$.

Equivalently, a G-module is an abelian group M together with a homomorphism of groups $G \to \mathrm{Aut}(M)$. We also say that G ***acts*** on M, and we say that the action is ***trivial*** if $gm = m$ for all $g \in G$ and $m \in M$.

A ***homomorphism*** of G-modules (or a ***G-homomorphism)*** is a map $\alpha: M \to N$ such that

(a) $\alpha(m + m') = \alpha(m) + \alpha(m')$ (i.e., α is a homomorphism of abelian groups);

(b) $\alpha(gm) = g(\alpha(m))$ for all $g \in G$, $m \in M$.

We write $\mathrm{Hom}_G(M, N)$ for the set of G-homomorphisms $M \to N$.

REMARK 1.1 The ***group algebra*** $\mathbb{Z}[G]$ of G is the free abelian group with basis the elements of G and with the multiplication provided by the group law on G. Thus the elements of $\mathbb{Z}[G]$ are the finite sums

$$\sum\nolimits_i n_i g_i, \quad n_i \in \mathbb{Z}, \quad g_i \in G,$$

and

$$\left(\sum\nolimits_i n_i g_i\right)\left(\sum\nolimits_j n'_j g'_j\right) = \sum\nolimits_{i,j} n_i n'_j (g_i g'_j).$$

A G-module structure on an abelian group M extends uniquely to a $\mathbb{Z}[G]$-module structure, and a homomorphism of abelian groups is a homomorphism of G-modules if and only if

it is a homomorphism of $\mathbb{Z}[G]$-modules. Thus the category Mod_G of G-modules can be identified with the category of modules over the ring $\mathbb{Z}[G]$. In particular, Mod_G is an abelian category.

If M and N are G-modules, then the set $\mathrm{Hom}(M, N)$ of homomorphisms $\varphi: M \to N$ (M and N regarded only as abelian groups) becomes a G-module with the structures

$$\begin{aligned}(\varphi + \varphi')(m) &= \varphi(m) + \varphi'(m)\\ (g\varphi)(m) &= g(\varphi(g^{-1}m)).\end{aligned} \tag{11}$$

Induced modules

For an H-module M, we define $\mathrm{Ind}_H^G(M)$ to be the set of maps (not necessarily homomorphisms) $\varphi: G \to M$ such that $\varphi(hg) = h\varphi(g)$ for all $h \in H$. Then $\mathrm{Ind}_H^G(M)$ becomes a G-module with the operations

$$\begin{aligned}(\varphi + \varphi')(x) &= \varphi(x) + \varphi'(x)\\ (g\varphi)(x) &= \varphi(xg).\end{aligned} \tag{12}$$

A homomorphism $\alpha: M \to M'$ of H-modules defines a homomorphism

$$\varphi \mapsto \alpha \circ \varphi: \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(M')$$

of G-modules.

LEMMA 1.2 (a) *For every G-module M and H-module N,*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \simeq \mathrm{Hom}_H(M, N).$$

(b) *The functor*

$$\mathrm{Ind}_H^G: \mathsf{Mod}_H \to \mathsf{Mod}_G$$

is exact.

PROOF. (a) Given a G-homomorphism $\alpha: M \to \mathrm{Ind}_H^G(N)$, we define a map $\beta: M \to N$ by the rule

$$\beta(m) = \alpha(m)(1_G),$$

where 1_G is the identity element in G. For every $g \in G$,

$$\beta(gm) \overset{\text{def}}{=} (\alpha(gm))(1_G) = (g(\alpha(m)))(1_G) \overset{(12)}{=} \alpha(m)(g).$$

Because $\alpha(m) \in \mathrm{Ind}_H^G(N)$, when $g \in H$, $\alpha(m)(g) = g(\alpha(m)(1_G)) = g(\beta(m))$. Therefore, β is an H-homomorphism $M \to N$.

Conversely, given an H-homomorphism $\beta: M \to N$, we define α to be the map $M \to \mathrm{Ind}_H^G(N)$ such that $\alpha(m)(g) = \beta(gm)$. Then α is a G-homomorphism.

Since the maps $\alpha \mapsto \beta$ and $\beta \mapsto \alpha$ are inverse, both are isomorphisms.

(b) Given an exact sequence

$$0 \to M \to N \to P \to 0,$$

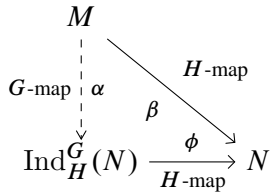
we have to prove that

$$0 \to \mathrm{Ind}_H^G M \to \mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G P \to 0$$

is exact. This is obvious except at the last position. Let S be a set of right coset representatives for H in G, so that $G = \bigcup_{s\in S} Hs$, and let $\varphi \in \mathrm{Ind}_H^G(P)$. For each $s \in S$, choose an $n(s) \in N$ mapping to $\varphi(s)$ in P, and define $\tilde{\varphi}(hs) = h \cdot n(s)$. Then $\tilde{\varphi} \in \mathrm{Ind}_H^G(N)$ and maps to φ. □

Let ϕ be the map $\mathrm{Ind}_H^G(N) \to N$, $\varphi \mapsto \varphi(1_G)$; this is an H-homomorphism, and the lemma shows that $(\mathrm{Ind}_H^G(N), \phi)$ has the following universal property:

for any H-homomorphism $\beta: M \to N$ from a G-module M to N, there exists a unique G-homomorphism $\alpha: M \to \mathrm{Ind}_H^G(N)$ such that $\phi \circ \alpha = \beta$.



When $H = \{1\}$, an H-module is just an abelian group. In this case, we drop the H from the notation Ind_H^G. Thus

$$\begin{aligned}\mathrm{Ind}^G(M_0) &= \{\varphi: G \to M_0\} \qquad (\text{maps, not necessarily homomorphisms})\\ &= \mathrm{Hom}(\mathbb{Z}[G], M_0) \quad (\text{homomorphisms of abelian groups}).\end{aligned}$$

A G-module is said to be ***induced*** if it isomorphic to $\mathrm{Ind}^G(M_0)$ for some abelian group M_0.

REMARK 1.3 Let G be a finite group.

(a) A G-module M is induced if and only if there exists an abelian group $M_0 \subset M$ such that

$$M = \bigoplus\nolimits_{g\in G} gM_0 \qquad (\text{direct sum of abelian groups}),$$

in which case there is an isomorphism of G-modules

$$\varphi \mapsto \sum_{g\in G} g \otimes \varphi(g^{-1}): \mathrm{Ind}^G(M_0) \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0.$$

Here $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ is endowed with the G-structure such that

$$g(z \otimes m) = gz \otimes m.$$

(b) Let H be a subgroup of G. An induced G-module is also induced when considered as an H-module: let S be a set of right coset representatives for H in G, so that $G = \bigcup_{s\in S} Hs$; if $M = \bigoplus_{g\in G} gM_0$, then $M = \bigoplus_{h\in H} hM_1$ with $M_1 = \bigoplus_{s\in S} sM_0$.

(c) Let M be a G-module, and let M_0 be M regarded as an abelian group. Then

$$\pi: \mathrm{Ind}^G(M_0) \to M, \quad \varphi \mapsto \sum_{g\in G} g\varphi(g^{-1})$$

is a surjective homomorphism of G-modules. It corresponds to the map

$$\mathbb{Z}[G] \otimes M_0 \to M, \quad \Big(\sum n_g g\Big) \otimes m \mapsto \sum n_g gm.$$

REMARK 1.4 Let M and N be G-modules. Then the rule

$$g(m \otimes n) = gm \otimes gn$$

defines a G-module structure on $M \otimes_{\mathbb{Z}} N$. Let M_0 be M regarded as an abelian group. Then $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M = \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ as abelian groups, but their G-module structures do not correspond. However, one checks easily that the map $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ sending $g \otimes m$ to $g \otimes gm$ is an isomorphism of G-modules.

Injective G-modules

A G-module I is said to be ***injective*** if every G-homomorphism from a submodule of a G-module extends to the whole module, or, equivalently, if $\mathrm{Hom}_G(\cdot, I)$ is an exact functor.

PROPOSITION 1.5 *The category Mod_G has enough injectives, i.e., every G-module M can be embedded into an injective G-module, $M \hookrightarrow I$.*

PROOF. When $G = \{1\}$, so that Mod_G is the category of abelian groups, this is proved in the Appendix (A.4). Now let M be a G-module, and let M_0 be M regarded as an abelian group. We can embed M_0 into an injective abelian group, say, $M_0 \hookrightarrow I$. On applying the functor Ind^G, we obtain an inclusion $\mathrm{Ind}^G(M_0) \hookrightarrow \mathrm{Ind}^G(I)$ of G-modules. There is an inclusion of G-modules $M \hookrightarrow \mathrm{Ind}^G(M_0)$ sending m to the function $g \mapsto gm$. On composing these maps, we obtain an injective homomorphism $M \hookrightarrow \mathrm{Ind}^G(I)$, and so it remains to show that $\mathrm{Ind}^G(I)$ is an injective G-module, but the natural isomorphism

$$\mathrm{Hom}_{\mathsf{Mod}_G}(M, \mathrm{Ind}^G(I)) \simeq \mathrm{Hom}_{\mathsf{Ab}}(M, I)$$

shows that $\mathrm{Hom}_{\mathsf{Mod}_G}(-, \mathrm{Ind}^G(I))$ is exact. □

Definition of the cohomology groups

For a G-module M, define

$$M^G = \{m \in M \mid gm = m \text{ all } g \in G\}.$$

The functor

$$M \mapsto M^G : \mathsf{Mod}_G \to \mathsf{Ab}$$

is left exact, i.e., if

$$0 \to M' \to M \to M'' \to 0$$

is exact, then

$$0 \to M'^G \to M^G \to M''^G$$

is exact. This can be checked directly, or by observing that $(-)^G$ is isomorphic to the left exact functor $\mathrm{Hom}_G(\mathbb{Z}, -)$.

Since the category of G-modules has enough injectives, we can apply the theory of derived functors (see the appendix to this chapter) to this situation.

Let M be a G-module, and choose an injective resolution

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

of M. The complex

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \to \cdots \xrightarrow{d^{r-1}} (I^r)^G \xrightarrow{d^r} (I^{r+1})^G \to \cdots$$

need no longer be exact, and we define the rth ***cohomology group of G with coefficients in M*** to be

$$H^r(G, M) = \frac{\operatorname{Ker}(d^r)}{\operatorname{Im}(d^{r-1})}.$$

These groups have the following basic properties.

1.6 The zeroth group $H^0(G, M) = M^G$, because

$$0 \to M^G \to I^{0G} \xrightarrow{d^0} I^{1G}$$

is exact, and $H^0(G, M) \overset{\text{def}}{=} \frac{\operatorname{Ker}(d^0)}{\operatorname{Im}(d^{-1})} = \operatorname{Ker}(d^0)$.

1.7 If I is an injective G-module, then $H^r(G, I) = 0$ for all $r > 0$, because

$$0 \to I \to I \to 0 \to \cdots$$

is an injective resolution of I.

1.8 Let $M \to I^\bullet$ and $N \to J^\bullet$ be injective resolutions of the G-modules M and N. Any homomorphism $\alpha\colon M \to N$ of G-modules extends to a map of complexes

$$\begin{array}{ccc} M & \longrightarrow & I^\bullet \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^\bullet} \\ N & \longrightarrow & J^\bullet, \end{array}$$

and the homomorphisms

$$H^r(\alpha^\bullet)\colon H^r(I^\bullet) \to H^r(J^\bullet)$$

are independent of the choice of $\alpha^\bullet$. On applying this statement to the identity map $\mathrm{id}\colon M \to M$, we find that the groups $H^r(G, M)$ are well-defined up to a well-defined isomorphism. The statement for a general α then shows that $M \mapsto H^r(G, M)$ is a functor from the category of G-modules to the category of abelian groups.

1.9 A short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of G-modules gives rise to a long exact sequence

$$0 \to H^0(G, M') \to \cdots \to H^r(G, M) \to H^r(G, M'') \xrightarrow{\delta^r} H^{r+1}(G, M') \to \cdots$$

Moreover, the association

$$\text{short exact sequence} \mapsto \text{ long exact sequence}$$

is functorial, i.e., a morphism of short exact sequences induces a morphism of long exact sequences (see A.11).

REMARK 1.10 The family of functors $(H^r(G, \cdot))_{r \geq 0}$ and coboundary maps δ^r are uniquely determined by the properties (1.6, 1.7, 1.9).

Shapiro's lemma

Let M be a G-module, and regard $\mathbb{Z}$ as a G-module with the trivial action: $gm = m$ for all $g \in G$, $m \in \mathbb{Z}$. A homomorphism $\alpha\colon \mathbb{Z} \to M$ is uniquely determined by $\alpha(1)$, and $m \in M$ is the image of 1 under a G-homomorphism $\mathbb{Z} \to M$ if and only if it is fixed by G. Therefore

$$\mathrm{Hom}_G(\mathbb{Z}, M) \simeq M^G. \tag{13}$$

PROPOSITION 1.11 (SHAPIRO'S LEMMA) *Let H be a subgroup of G. For every H-module N, there is a canonical isomorphism*

$$H^r(G, \mathrm{Ind}_H^G(N)) \to H^r(H, N)$$

for all $r \geq 0$.

PROOF. For $r = 0$, the isomorphism is the composite

$$N^H \overset{(13)}{\simeq} \mathrm{Hom}_H(\mathbb{Z}, N) \overset{(1.2)}{\simeq} \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G(N)) \overset{(13)}{\simeq} \mathrm{Ind}_H^G(N)^G. \tag{14}$$

Now choose an injective resolution $N \to I^\bullet$ of N. On applying the functor Ind_H^G, we obtain an injective resolution $\mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^\bullet)$ of the G-module $\mathrm{Ind}_H^G(N)$ because the functor Ind_H^G is exact (1.2) and preserves injectives (proof of 1.5). Hence

$$H^r(G,\ \mathrm{Ind}_H^G(N)) = H^r((\mathrm{Ind}_H^G(I^\bullet))^G) \overset{(14)}{\simeq} H^r(I^{\bullet H}) = H^r(H, N). \qquad \square$$

COROLLARY 1.12 *If M is an induced G-module, then $H^r(G, M) = 0$ for $r > 0$.*

PROOF. If $M = \mathrm{Ind}^G(M_0)$, then

$$H^r(G, M) \simeq H^r(\{1\}, M_0) = 0 \quad \text{for } r > 0. \qquad \square$$

REMARK 1.13 Consider an exact sequence

$$0 \to M \to J \to N \to 0$$

of G-modules. If $H^r(G, J) = 0$ for all $r > 0$, then the cohomology sequence becomes the exact sequence

$$0 \to M^G \to J^G \to N^G \to H^1(G, M) \to 0$$

and the collection of isomorphisms

$$H^r(G, N) \xrightarrow{\approx} H^{r+1}(G, M), \quad r \geq 1.$$

For example, let M be a G-module, and let M_* be the induced module $\mathrm{Ind}^G(M_0)$, where M_0 is M regarded as an abelian group. As we noted in the proof of (1.5), M can be identified with the G-submodule of M_* consisting of maps of the form $g \mapsto gm$, $m \in M$. Let $M_\dagger = M_*/M$. On applying the above remark to the sequence

$$0 \to M \to M_* \to M_\dagger \to 0 \tag{15}$$

we find that

$$H^r(G, M_\dagger) \simeq H^{r+1}(G, M), \quad \text{all } r \geq 1.$$

More generally, an exact sequence

$$0 \to M \to J^1 \to \cdots \to J^s \to N \to 0$$

such that $H^r(G, J^i) = 0$ for all $r, i > 0$, defines isomorphisms

$$H^r(G, N) \xrightarrow{\simeq} H^{r+s}(G, M), \quad \text{all } r \geq 1.$$

To prove this, break the sequence up into short exact sequences

$$\begin{aligned} &0 \to M \to J^1 \to N^1 \to 0 \\ &0 \to N^1 \to J^2 \to N^2 \to 0 \\ &\cdots \\ &0 \to N^{s-1} \to J^s \to N \to 0 \end{aligned}$$

and note that we have isomorphisms

$$H^r(G, N) \simeq H^{r+1}(G, N^{s-1}) \simeq H^{r+2}(G, N^{s-2}) \simeq \cdots .$$

REMARK 1.14 Let

$$0 \to M \xrightarrow{\varepsilon} J^0 \xrightarrow{d^0} J^1 \xrightarrow{d^1} J^2 \to \cdots$$

be an exact sequence such that $H^s(G, J^r) = 0$ for all $s > 0$ and all r. Then

$$H^r(G, M) = H^r(J^{\bullet G}).$$

This remark applies to every resolution of M by induced modules.

Description of the cohomology groups by means of cochains

Let P_r, $r \geq 0$, be the free $\mathbb{Z}$-module with basis the $(r+1)$-tuples $(g_0, \ldots, g_r)$ of elements of G, endowed the action of G such that

$$g(g_0, \ldots, g_r) = (gg_0, \ldots, gg_r).$$

Note that P_r is also free as a $\mathbb{Z}[G]$-module, with basis $\{(1, g_1, \ldots, g_r) \mid g_i \in G\}$. Define a homomorphism $d_r \colon P_r \to P_{r-1}$ by the rule

$$d_r(g_0, \ldots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_r),$$

where the symbol $\hat{\cdot}$ means that $\cdot$ is omitted. Let $P_\bullet$ be

$$\cdots \to P_r \xrightarrow{d_r} P_{r-1} \to \cdots \to P_0$$

One checks easily that $d_{r-1} \circ d_r = 0$, and so this is a complex. Let ε be the map $P_0 \to \mathbb{Z}$ sending each basis element to 1.

LEMMA 1.15 *The complex* $P_\bullet \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ *is exact.*

PROOF. Choose an element $o \in G$, and define $k_r: P_r \to P_{r+1}$ by

$$k_r(g_0, \dots, g_r) = (o, g_0, \dots, g_r).$$

One checks easily that $d_{r+1} \circ k_r + k_{r-1} \circ d_r = 1$. Hence, if $d_r(x) = 0$, then $x = d_{r+1}(k_r(x))$. □

PROPOSITION 1.16 *For every G-module M,*

$$H^r(G, M) \simeq H^r(\mathrm{Hom}_G(P_\bullet, M)).$$

PROOF. This follows from the fact that $P_\bullet \to \mathbb{Z}$ is a projective resolution of $\mathbb{Z}$ — see Example A.14. □

An element of $\mathrm{Hom}(P_r, M)$ can be identified with a function $\varphi: G^{r+1} \to M$, and φ is fixed by G if and only if

$$\varphi(gg_0, \dots, gg_r) = g(\varphi(g_0, \dots, g_r)) \text{ all } g, g_0, \dots, g_r \in G.$$

Thus $\mathrm{Hom}_G(P_r, M)$ can be identified with the set $\tilde{C}^r(G, M)$ of φ's satisfying this condition. Such φ are called ***homogeneous r-cochains of G with values in M***. The boundary map $\tilde{d}^r: \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M)$ induced by d_{r+1} is

$$(\tilde{d}^r\varphi)(g_0, \dots, g_{r+1}) = \sum (-1)^i \varphi(g_0, \dots, \hat{g}_i, \dots, g_{r+1}).$$

Proposition 1.16 says that

$$H^r(G, M) \simeq \frac{\mathrm{Ker}(\tilde{d}^r)}{\mathrm{Im}(\tilde{d}^{r-1})}.$$

A homogenous cochain $\varphi: G^{r+1} \to M$ is determined by its values on the elements $(1, g_1, g_1g_2, \dots, g_1 \dots g_r)$. We are therefore led to introduce the group $C^r(G, M)$ of ***inhomogeneous r-cochains of G with values in M*** consisting of all maps $\varphi: G^r \to M$. We set $G^0 = \{1\}$, so that $C^0(G, M) = M$. Define

$$d^r: C^r(G, M) \to C^{r+1}(G, M),$$

by $(d^r\varphi)(g_1, \cdots, g_{r+1}) =$

$$g_1\varphi(g_2, \dots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \varphi(g_1, \dots, g_jg_{j+1}, \dots, g_{r+1}) + (-1)^{r+1}\varphi(g_1, \dots, g_r).$$

Define

$$Z^r(G, M) = \mathrm{Ker}(d^r) \qquad \textbf{\textit{(group of r-cocycles)}}$$

and

$$B^r(G, M) = \mathrm{Im}(d^{r-1}) \qquad \textbf{\textit{(group of r-coboundaries)}}.$$

PROPOSITION 1.17 *The sequence of maps*

$$C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} \cdots \xrightarrow{d^{r-1}} C^r(G, M) \xrightarrow{d^r} C^{r+1}(G, M) \to \cdots$$

is a complex, i.e., $d^r \circ d^{r-1} = 0$, and there is a canonical isomorphism

$$H^r(G, M) \simeq \frac{Z^r(G, M)}{B^r(G, M)}.$$

PROOF. For $\varphi \in \tilde{C}^r(G, M)$, define

$$\varphi'(g_1, \dots, g_r) = \varphi(1, g_1, g_1g_2, \dots, g_1 \cdots g_r).$$

Then $\varphi \mapsto \varphi'$ is a bijection $\tilde{C}^r(G, M) \to C^r(G, M)$ transforming the boundary maps in $\tilde{C}^\bullet(G, M)$ into the boundary maps in $C^\bullet(G, M)$. □

EXAMPLE 1.18 (a) A map $\varphi: G \to M$ is a ***crossed homomorphism*** if

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma), \text{ all } \sigma, \tau \in G.$$

Notice that the condition implies that, for e the identity element of G,

$$\varphi(e) = \varphi(ee) = e\varphi(e) + \varphi(e) = 2\varphi(e)$$

and so $\varphi(e) = 0$. For every $m \in M$, the map $\sigma \mapsto \sigma m - m$ is a crossed homomorphism—called a ***principal crossed homomorphism.*** According to the proposition

$$H^1(G, M) = \frac{\{\text{ crossed homomorphisms } G \to M\}}{\{\text{ principal crossed homomorphisms}\}}.$$

If the action of G on M is trivial, then a crossed homomorphism is a homomorphism, and the principal crossed homomorphisms are zero. Thus, in this case,

$$H^1(G, M) \simeq \mathrm{Hom}(G, M). \tag{16}$$

(b) Let M be an abelian group (with the law of composition written as multiplication). An ***extension of G by M*** is an exact sequence of groups

$$1 \to M \to E \xrightarrow{\pi} G \to 1.$$

We set

$$\sigma m = s(\sigma) \cdot m \cdot s(\sigma)^{-1}, \quad \sigma \in G, m \in M,$$

where $s(\sigma)$ is any element of E mapping to σ. Because M is commutative, σm depends only on σ, and this defines an action of G on M. Note that

$$s(\sigma) \cdot m = \sigma m \cdot s(\sigma), \quad \text{all } \sigma \in G, \quad m \in M.$$

Now choose a section s to π, i.e., a map (not necessarily a homomorphism) $s: G \to E$ such that $\pi \circ s = \mathrm{id}$. Then $s(\sigma)s(\sigma')$ and $s(\sigma\sigma')$ both map to $\sigma\sigma' \in G$, and so they differ by an element $\varphi(\sigma, \sigma') \in M$:

$$s(\sigma)s(\sigma') = \varphi(\sigma, \sigma') \cdot s(\sigma\sigma').$$

From

$$s(\sigma)(s(\sigma')s(\sigma'')) = (s(\sigma)s(\sigma'))s(\sigma'')$$

we deduce that

$$\sigma\varphi(\sigma', \sigma'') \cdot \varphi(\sigma, \sigma'\sigma'') = \varphi(\sigma, \sigma') \cdot \varphi(\sigma\sigma', \sigma''),$$

i.e., that $\varphi \in Z^2(G, M)$. If s is replaced by a different section, φ is replaced by a cohomologous cocycle, and so the class of φ in $H^2(G, M)$ is independent of the choice of s. Every such φ arises from an extension. In this way, $H^2(G, M)$ classifies the isomorphism classes of extensions of G by M with a fixed action of G on M.

REMARK 1.19 Let G be a group, and let M be a G-module. For $m \in M$, let $\varphi_m: G \to M$ be the constant map $\sigma \mapsto m$. Then

$$(d^1\varphi_m)(\sigma,\tau) = \sigma m - m + m = \sigma m.$$

In particular, $(d^1\varphi_m)(1,1) = m$. Therefore, every class in $H^2(G,M)$ is represented by a 2-cocycle φ with $\varphi(1,1) = 0$. Such a 2-cocycle is said to be ***normalized***.

EXAMPLE 1.20 Let $\varphi: G \to M$ be a crossed homomorphism. For every $\sigma \in G$,

$$\begin{aligned}\varphi(\sigma^2) &= \sigma\varphi(\sigma) + \varphi(\sigma)\\ \varphi(\sigma^3) &= \varphi(\sigma\cdot\sigma^2) = \sigma^2\varphi(\sigma) + \sigma\varphi(\sigma) + \varphi(\sigma)\\ &\cdots\\ \varphi(\sigma^f) &= \sigma^{f-1}\varphi(\sigma) + \cdots + \sigma\varphi(\sigma) + \varphi(\sigma).\end{aligned}$$

Thus, if G is a cyclic group of order f generated by σ, then a crossed homomorphism φ is determined by its value, m say, on σ, and m satisfies the equation

$$\sigma^{f-1}m + \cdots + \sigma m + m = 0. \tag{17}$$

Conversely, if $m \in M$ satisfies (17), then the formulas $\varphi(\sigma^i) = \sigma^{i-1}m + \cdots + \sigma m + m$ define a crossed homomorphism $\varphi: G \to M$, and

$$\varphi \text{ is principal} \iff m = \sigma x - x \text{ for some } x \in M.$$

Define maps

$$\begin{aligned}\mathrm{Nm}_G: M \to M, &\quad m \mapsto \textstyle\sum_{\sigma\in G}\sigma m\\ \sigma - 1: M \to M, &\quad m \mapsto \sigma m - m.\end{aligned}$$

Then, for a cyclic group G of finite order, we have shown that the choice of a generator σ for G determines an isomorphism

$$\varphi \mapsto \varphi(\sigma): H^1(G,M) \to \frac{\mathrm{Ker}(\mathrm{Nm}_G)}{(\sigma-1)M}.$$

REMARK 1.21 Let

$$0 \to M \to N \to P \to 0$$

be an exact sequence of G-modules. The boundary map

$$\delta^r: H^r(G,P) \to H^{r+1}(G,M)$$

has the following description: let $\gamma \in H^r(G,P)$ be represented by the r-cocycle $\varphi: G^r \to P$; because N maps onto P, there exists an r-cochain $\tilde{\varphi}: G^r \to N$ lifting φ; because $d\varphi = 0$, $d\tilde{\varphi}$ takes values in M — it is the cocycle representing $\delta^r\gamma$.

The cohomology of L and $L^\times$

Let L be a finite Galois extension of the field K, and let $G = \mathrm{Gal}(L/K)$. Then both L (regarded as a group under addition) and $L^\times$ are G-modules.

PROPOSITION 1.22 *Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.*

PROOF. Let $\varphi: G \to L^\times$ be a crossed homomorphism. In multiplicative notation, this means that

$$\varphi(\sigma\tau) = \sigma\varphi(\tau)\cdot\varphi(\sigma), \quad \sigma, \tau \in G,$$

and we have to find a $c \in L^\times$ such that $\varphi(\sigma) = \sigma c/c$. For $a \in L^\times$, let

$$b = \sum_{\sigma\in G} \varphi(\sigma)\cdot\sigma a.$$

Suppose $b \neq 0$. Then

$$\tau b = \sum_{\sigma} \tau\varphi(\sigma)\cdot\tau\sigma a = \sum_{\sigma} \varphi(\tau)^{-1}\varphi(\tau\sigma)\tau\sigma a = \varphi(\tau)^{-1}b.$$

Hence

$$\varphi(\tau) = b/\tau b = \tau(b^{-1})/b^{-1},$$

which shows that φ is principal.

It remains to show that there exists an a for which $b \neq 0$. Recall (FT, 5.14, Dedekind's theorem on the independence of characters):

> Let L be a field and H a group; then every finite set $\{f_i\}$ of distinct homomorphisms $H \to L^\times$ is linearly independent over L, i.e.,
>
> $$\sum a_i f_i(\alpha) = 0 \quad \text{all } \alpha \in H \Rightarrow a_1 = a_2 = \cdots = a_n = 0.$$

When we apply this to the homomorphisms $\sigma: L^\times \to L^\times$, $\sigma \in G$, we find that $\sum_\sigma \varphi(\sigma)\sigma$ is not the zero map, and so there exists an a for which $b \neq 0$. □

COROLLARY 1.23 *Let L/K be a cyclic extension, and let σ generate $\mathrm{Gal}(L/K)$. If $\mathrm{Nm}_{L/K}\, a = 1$, then a is of the form $\frac{\sigma b}{b}$.*

PROOF. We have $0 = H^1(G, L^\times) = \mathrm{Ker}(\mathrm{Nm}_G)/(\sigma - 1)L^\times$. □

Corollary 1.23 occurs as Satz 90 of Hilbert's book, Die Theorie der algebraischen Zahlkörper, 1894/95, and Theorem 1.22 is Emmy Noether's generalization. Both are usually referred to as Hilbert's Theorem 90.

PROPOSITION 1.24 *Let L/K be a finite Galois extension with Galois group G. Then $H^r(G, L) = 0$ for all $r > 0$.*

PROOF. Recall (FT, 5.18, Normal Basis Theorem):

> There exists an $\alpha \in L$ such that $\{\sigma\alpha \mid \sigma \in G\}$ is a basis for L as a K-vector space. (A basis of this form is said to be ***normal***.)

A normal basis $(\sigma\alpha)_{\sigma\in G}$ defines an isomorphism of G-modules

$$\sum\nolimits_{\sigma\in G} a_\sigma\sigma \mapsto \sum\nolimits_{\sigma\in G} a_\sigma\sigma\alpha: K[G] \to L.$$

But $K[G] = \mathrm{Ind}_{\{1\}}^G K$, and so $H^r(G, L) \simeq H^r(\{1\}, K) = 0$ for $r > 0$ (Shapiro's lemma, 1.11). □

The cohomology of products

A product $M = \prod_i M_i$ of G-modules becomes a G-module under the diagonal action:

$$\sigma(\dots, m_i, \dots) = (\dots, \sigma m_i, \dots).$$

PROPOSITION 1.25 *For all families of G-modules $(M_i)_i$,*

$$H^r(G, \textstyle\prod_i M_i) \simeq \prod_i H^r(G, M_i).$$

PROOF. A product of exact sequences of abelian groups is again exact. From this it follows that a product $I = \prod I_i$ of injective G-modules is again injective, because

$$\mathrm{Hom}_G(\cdot, I) \simeq \textstyle\prod_i \mathrm{Hom}_G(\cdot, I_i)$$

is exact. Let $M_i \to I_i^\bullet$ be an injective resolution of M_i. Then $\prod M_i \to \prod I_i^\bullet$ is an injective resolution of $\prod M_i$, and

$$H^r(G, \textstyle\prod_i M_i) \simeq H^r((\prod_i I_i^\bullet)^G) \simeq H^r(\prod_i (I_i^{\bullet G})) \simeq \prod_i H^r(I_i^{\bullet G}) \simeq \prod_i H^r(G, M_i).$$

□

In particular, for any G-modules M, N,

$$H^r(G, M \oplus N) = H^r(G, M) \oplus H^r(G, N).$$

This can be proved more directly by noting that to say that a module P is a direct sum of modules M and N means that certain maps, and relations between the maps, exist (see p. 90). These maps and relations persist when we apply the additive functor $H^r(G, \cdot)$.

REMARK 1.26 The formation of inverse limits of arbitrary abelian groups is not exact. Therefore, in general, one can not expect cohomology to commute with inverse limits.

Functorial properties of the cohomology groups

Let M and M' respectively be G and G' modules. Homomorphisms

$$\alpha: G' \to G, \quad \beta: M \to M'$$

are said to be ***compatible*** if

$$\beta(\alpha(g)m) = g(\beta(m)).$$

Then (α, β) defines a homomorphism of complexes

$$C^\bullet(G, M) \to C^\bullet(G', M'), \quad \varphi \mapsto \beta \circ \varphi \circ \alpha^r,$$

and hence homomorphisms

$$H^r(G, M) \to H^r(G', M').$$

EXAMPLE 1.27 (a) Let H be a subgroup of G. For every H-module M, the map

$$\varphi \mapsto \varphi(1_G): \mathrm{Ind}_H^G(M) \to M$$

is compatible with the inclusion $H \hookrightarrow G$, and the induced homomorphism

$$H^r(G, \operatorname{Ind}_H^G(M)) \to H^r(H, M)$$

is the isomorphism in Shapiro's Lemma 1.11. To show that the two isomorphisms agree, first check it for $r = 0$, and then use dimension-shifting (II, 1.28) to get it for all r.

(b) Let H be a subgroup of G. Let α be the inclusion $H \hookrightarrow G$, and let β be the identity map on a G-module M. In this case, we obtain ***restriction homomorphisms***

$$\operatorname{Res}: H^r(G, M) \to H^r(H, M).$$

They can also be constructed as follows: let $M \to \operatorname{Ind}_H^G(M)$ be the homomorphism sending m to the map $g \mapsto gm$; the composite of the homomorphism this defines on cohomology with the isomorphism in Shapiro's Lemma,

$$H^r(G, M) \to H^r(G, \operatorname{Ind}_H^G(M)) \xrightarrow{\simeq} H^r(H, M)$$

is the restriction map.

(c) Let H be a normal subgroup of G, let α be the quotient map $G \to G/H$, and let β be the inclusion $M^H \hookrightarrow M$. In this case, we obtain the ***inflation homomorphisms***

$$\operatorname{Inf}: H^r(G/H, M^H) \to H^r(G, M).$$

(d) For any $g_0 \in G$, the homomorphisms $\alpha: G \to G$, $\sigma \mapsto g_0 \sigma g_0^{-1}$, and $\beta: M \to M$, $m \mapsto g_0^{-1}m$, are compatible. I claim that the homomorphisms

$$H^r(G, M) \to H^r(G, M)$$

they define are each the identity map. For $r = 0$, the homomorphism is

$$m \mapsto g_0^{-1}m: M^G \to M^G,$$

which is obviously the identity. Let $r > 0$, and suppose the statement is known for $r - 1$. From the exact sequence (15, p. 62)

$$0 \to M \to M_* \to M_\dagger \to 0,$$

$M_* = \operatorname{Ind}^G(M_0)$, we obtain a diagram with exact rows

$$\begin{array}{ccccccc} H^{r-1}(G, M_*) & \longrightarrow & H^{r-1}(G, M_\dagger) & \longrightarrow & H^r(G, M) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ H^{r-1}(G, M_*) & \longrightarrow & H^{r-1}(G, M_\dagger) & \longrightarrow & H^r(G, M) & \longrightarrow & 0. \end{array}$$

The 0's at right result from the fact that M_* is an induced module. The vertical maps are those defined by the pair (α, β) (for the different modules). One checks easily that the diagram commutes. By induction, the middle vertical map is the identity, which implies that the third is also.

REMARK 1.28 (a) The method of proof in (d) is called ***dimension shifting.***

(b) Let H be a normal subgroup of G. For every G-module M, the recipe in (d) gives an action of G on $H^r(H, M)$, which the above result shows to factor through G/H.

EXAMPLE 1.29 We shall need one more functorial map of cohomology groups. Let H be a subgroup of finite index of G, and let S be a set of left coset representatives for H in G, $G = \bigcup_{s\in S} sH$. Let M be a G-module. For every $m \in M^H$,

$$\mathrm{Nm}_{G/H}\, m \overset{\text{def}}{=} \sum_{s\in S} sm$$

is independent of the choice of S, and is fixed by G. Thus $\mathrm{Nm}_{G/H}$ is a homomorphism

$$M^H \to M^G.$$

This can be extended to a ***corestriction homomorphism***[1]

$$\mathrm{Cor}\colon H^r(H, M) \to H^r(G, M)$$

for all r as follows: for every G-module M, there is a canonical homomorphism of G-modules

$$\varphi \mapsto \sum\nolimits_{s\in S} s\varphi(s^{-1})\colon \mathrm{Ind}_H^G M \to M;$$

the map on cohomology which it defines, when composed with the isomorphism in Shapiro's lemma, gives Cor,

$$H^r(H, M) \xrightarrow{\simeq} H^r(G, \mathrm{Ind}_H^G M) \to H^r(G, M).$$

PROPOSITION 1.30 *Let H be a subgroup of G of finite index. The composite*

$$\mathrm{Cor} \circ \mathrm{Res}\colon H^r(G, M) \to H^r(G, M)$$

is multiplication by $(G\colon H)$.

PROOF. For $m \in M$, let φ_m be the map $g \mapsto gm\colon G \to M$. Then $\mathrm{Cor} \circ \mathrm{Res}$ is the map on cohomology defined by the composite of

$$M \to \mathrm{Ind}_H^G(M) \to M, \quad m \mapsto \varphi_m \mapsto \sum_s s\varphi_m(s^{-1}) = \sum_s m = (G : H)m.$$

□

COROLLARY 1.31 *If $(G\colon 1) = m$, then $mH^r(G, M) = 0$ for $r > 0$.*

PROOF. According to the proposition, multiplication by m factors through $H^r(\{1\}, M) = 0$,

$$H^r(G, M) \xrightarrow{\text{Res}} H^r(\{1\}, M) \xrightarrow{\text{Cor}} H^r(G, M).$$

□

COROLLARY 1.32 *If G is finite and M is finitely generated as an abelian group, then $H^r(G, M)$ is finite.*

PROOF. From the description of $H^r(G, M)$ as the group of cocycles modulo coboundaries, it is clear that $H^r(G, M)$ is finitely generated as an abelian group, and we have just seen that it is killed by $(G\colon 1)$. Therefore it is finite. □

[1] The corestriction homomorphism is also called the ***transfer homomorphism.***

For an abelian group A and prime number p, the ***p*-primary component** $A(p)$ of A is the subgroup consisting of all elements killed by a power of p.

COROLLARY 1.33 *Let G be a finite group, and let G_p be its Sylow p-subgroup. For every G-module M, the restriction map*

$$\text{Res}: H^r(G, M) \to H^r(G_p, M)$$

is injective on the p-primary component of $H^r(G, M)$.

PROOF. The composite

$$\text{Cor} \circ \text{Res} : H^r(G, M) \to H^r(G_p, M) \to H^r(G, M)$$

is multiplication by $(G: G_p)$, which is not divisible by p, and so is injective on the p-primary component of $H^r(G, M)$. □

The inflation-restriction exact sequence

PROPOSITION 1.34 *Let H be a normal subgroup of G, and let M be a G-module. Let r be an integer > 0. If $H^j(H, M) = 0$ for all j with $0 < j < r$, then the sequence*

$$0 \to H^r(G/H, M^H) \xrightarrow{\text{Inf}} H^r(G, M) \xrightarrow{\text{Res}} H^r(H, M)$$

is exact.

PROOF. We first prove this for $r = 1$. In this case, the hypothesis on $H^j(H, M)$ is vacuous. Let $\varphi: G \to M$ be a crossed homomorphism whose restriction to H is principal, say, $\varphi(h) = hm_0 - m_0$. Define $\varphi'(g) = \varphi(g) - (gm_0 - m_0)$. Then φ' represents the same class in $H^1(G, M)$, but now $\varphi'(h) = 0$ for all $h \in H$, and so φ' comes by "inflation" from a crossed homomorphism $G/H \to M$.

We show that φ' takes values in M^H. As φ' is a crossed homomorphism and $\varphi'(h) = 0$ for $h \in H$, we have

$$\varphi'(hg) = h\varphi'(g) + \varphi'(h) = h\varphi'(g)$$
$$\varphi'(gh) = g\varphi'(h) + \varphi'(g) = \varphi'(g).$$

The second equation says that φ' is constant on left cosets of H. As H is normal, left cosets and right cosets are the same, and so φ' is constant on right cosets. Since hg and g are in the same right coset Hg, we have $\varphi'(hg) = \varphi'(g)$. Combining this with the first equation gives $h\varphi'(g) = \varphi'(g)$, i.e., $\varphi'(g) \in M^H$.

We have shown that φ' comes by "inflation" from a crossed homomorphism $G/H \to M^H$, which proves the exactness at $H^1(G, M)$. The proof of the exactness at $H^1(G/H, M^H)$ is easy.

Now assume that $r > 1$ and that the statement is true for $r - 1$. Consider the exact sequence (15), p. 62,

$$0 \to M \to M_* \to M_\dagger \to 0.$$

Then

$$H^j(H, M_\dagger) \simeq H^{j+1}(H, M), \quad j > 0,$$

and so $H^j(H, M_\dagger) = 0$ for $0 < j < r-1$. By induction, the sequence

$$0 \to H^{r-1}(G/H, M_\dagger^H) \xrightarrow{\text{Inf}} H^{r-1}(G, M_\dagger) \xrightarrow{\text{Res}} H^{r-1}(H, M_\dagger)$$

is exact, and this is isomorphic to the sequence

$$0 \to H^r(G/H, M^H) \xrightarrow{\text{Inf}} H^r(G, M) \xrightarrow{\text{Res}} H^r(H, M).$$

□

REMARK 1.35 (a) With a little more effort, one can extend the sequence to

$$\begin{aligned} 0 \to & H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H} \to \\ & H^2(G/H, M^H) \xrightarrow{\text{Inf}} H^2(G, M)^* \to H^1(G/H, H^1(H, M)) \to H^3(G/H, M^H), \end{aligned}$$

where $H^2(G, M)^* = \text{Ker}(\text{Res}\colon H^2(G, M) \to H^2(H, M))$. See Dekimpe, Hartl, and Wauters, J. Algebra 369 (2012), 70–95.

(b) For the experts, the Hochschild-Serre (or Lyndon) spectral sequence takes the form

$$H^i(G/H, H^j(H, M)) \Rightarrow H^{i+j}(G, M);$$

here G/H acts on $H^j(H, M)$ as described in (1.28b). It is possible to read off from this sequence, an exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M).$$

The hypotheses that $H^i(H, M) = 0$ for $0 < i < r$ forces r rows of the spectral sequence to vanish, and allows one to read off the same sequence with 1 replaced with r.

EXAMPLE 1.36 Let $\Omega \supset L$ be Galois extensions of K. Then $H \overset{\text{def}}{=} \text{Gal}(\Omega/L)$ is a normal subgroup of $G \overset{\text{def}}{=} \text{Gal}(\Omega/K)$. According to Proposition 1.22, $H^1(H, \Omega^\times) = 0$, and so there is an exact sequence

$$0 \to H^2(G/H, L^\times) \to H^2(G, \Omega^\times) \to H^2(H, \Omega^\times).$$

A direct proof (not involving dimension shifting) that this sequence is exact can be found in Artin 1951, 6.4.

Cup-products

LEMMA 1.37 *The exact sequence (15), p. 62,*

$$0 \to M \to M_* \to M_\dagger \to 0,$$

is split as a sequence of abelian groups, i.e., $M_* \approx M \oplus M_\dagger$ (as abelian groups).

PROOF. Recall that M_* consists of the maps $\varphi\colon G \to M$ and that the first homomorphism in the sequence sends an element m of M to φ_m, where $\varphi_m(g) = gm$. For $\varphi \in M_*$, let $s(\varphi) = \varphi(1_G)$. Then s is a homomorphism of abelian groups $M_* \to M$ such that $s(\varphi_m) = m$, and so

$$M_* \simeq \text{Ker}(1 - s) \oplus \text{Ker}(s) \simeq M \oplus M_\dagger$$

as abelian groups. □

Let G be a group. For G-modules M and N, we write $M \otimes N$ for $M \otimes_{\mathbb{Z}} N$ regarded as a G-module with

$$g(m \otimes n) = gm \otimes gn, \quad g \in G, \quad m \in M, \quad n \in N.$$

PROPOSITION 1.38 *There exists one and only one family of bi-additive pairings*

$$(m, n) \mapsto m \cup n \colon H^r(G, M) \times H^s(G, N) \to H^{r+s}(G, M \otimes N),$$

defined for all G-modules M, N and all integers $r, s \geq 0$, satisfying the following conditions:

(a) *these maps become morphisms of functors when the two sides are regarded as covariant bifunctors on (M, N);*

(b) *for $r = s = 0$, the pairing is*

$$(m, n) \mapsto m \otimes n \colon M^G \otimes N^G \to (M \otimes N)^G;$$

(c) *if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of G-modules such that*

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

is exact, then

$$(\delta m'') \cup n = \delta(m'' \cup n), \quad m'' \in H^r(G, M''), \quad n \in H^s(G, N).$$

Here δ denotes the connecting homomorphism $H^r(G, M'') \to H^{r+1}(G, M')$ or $H^{r+s}(G, M'' \otimes N) \to H^{r+s+1}(G, M' \otimes N)$.

(d) *if $0 \to N' \to N \to N'' \to 0$ is an exact sequence of G-modules such that*

$$0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

is exact, then

$$m \cup \delta n'' = (-1)^r \delta(m \cup n''), \quad m \in H^r(G, M), \quad n'' \in H^s(G, N'').$$

PROOF. The uniqueness is proved using dimension shifting, a key point being that, because the sequence (15) is split-exact as a sequence of abelian groups (see 1.37), it remains exact when tensored over $\mathbb{Z}$ with a G-module. For the existence, one proves that the pairing defined as follows has the required properties: let $m \in H^r(G, M)$ and $n \in H^s(G, N)$ be represented by the (inhomogeneous) cocycles φ and ψ; then $m \cup n$ is represented by the cocycle

$$(g_1, \dots, g_{r+s}) \mapsto \varphi(g_1, \dots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \cdots, g_{r+s}).$$

It takes several pages to write out the details, but the proof is not difficult. □

PROPOSITION 1.39 *The following formulas hold:*

(a) $(x \cup y) \cup z = x \cup (y \cup z)$ *(in $H^{r+s+t}(G, M \otimes N \otimes P)$);*

(b) $x \cup y = (-1)^{rs} y \cup x$ *if $x \in H^r(G, M)$, $y \in H^s(G, N)$ (we identify $M \otimes N$ and $N \otimes M$);*

(c) $\operatorname{Res}(x \cup y) = \operatorname{Res}(x) \cup \operatorname{Res}(y)$;

(d) $\mathrm{Cor}(x \cup \mathrm{Res}\, y) = \mathrm{Cor}(x) \cup y$.

(e) $\mathrm{Inf}(x \cup y) = \mathrm{Inf}(x) \cup \mathrm{Inf}(y)$.

PROOF. In each case, one verifies the formula when $x, y, \ldots$ have degree 0, and then uses dimension shifting to deduce the general case. For example, the proof of (d) is written out in detail in Atiyah and Wall 1967, Proposition 9. For (e), see Weiss 1969, 4-3-9. □

A pairing

$$x, y \mapsto (x, y): M \times N \to P \tag{18}$$

such that

$$g(x, y) = (gx, gy), \quad \text{all } g \in G,$$

defines a homomorphism of G-modules

$$M \otimes N \to P,$$

and hence maps

$$H^r(G, M \otimes N) \to H^r(G, P).$$

The composites of the cup-product pairings with these maps, namely, the pairings

$$H^r(G, M) \times H^s(G, N) \to H^{r+s}(G, P),$$

will be referred to as the cup-product pairings defined by (18).

2 Homology

Definition of the homology groups

For a G-module M, let M_G be the largest quotient of M on which G acts trivially. Thus M_G is the quotient of M by the subgroup generated by

$$\{gm - m \mid g \in G, \quad m \in M\}.$$

Note that this is the dual notion to M^G, which is the largest subobject of M on which G acts trivially. The definition of the cohomology groups dualizes to give us homology groups.

In detail, the functor

$$M \mapsto M_G: \mathbf{Mod}_G \to \mathbf{Ab}$$

is right exact, i.e., if

$$0 \to M' \to M \to M'' \to 0$$

is exact, then

$$M'_G \to M_G \to M''_G \to 0$$

is exact. This can be checked directly, or by observing that passing from M to M_G amounts to tensoring M with $\mathbb{Z}[G]/I_G$, where I_G is the augmentation ideal

$$\mathrm{Ker}\left(\sum n_g g \mapsto \sum n_g: \mathbb{Z}[G] \to \mathbb{Z}\right).$$

An object P of an abelian category is ***projective*** if for any object N and quotient object M, every morphism $P \to M$ lifts to a morphism $P \to N$. For example, every free $\mathbb{Z}[G]$-module is projective as a $\mathbb{Z}[G]$- (equivalently, G-) module.

Let M be a G-module. Let $(m_i)_{i\in I}$ be a family of generators for M as a $\mathbb{Z}[G]$-module, and let $\mathbb{Z}[G]^{(I)}$ be a direct sum of copies of $\mathbb{Z}[G]$ indexed by I. The map $\sum_{i\in I}\gamma_i \mapsto \sum \gamma_i m_i$ is a surjective G-homomorphism $\mathbb{Z}[G]^{(I)} \to M$. This shows that every G-module is a quotient of a free G-module, and hence that the category Mod_G has enough projectives.

Let M be a G-module, and choose a projective resolution

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \longrightarrow 0$$

of M. The complex

$$\cdots \longrightarrow (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \longrightarrow 0$$

need no longer be exact, and we set

$$H_r(G, M) = \frac{\mathrm{Ker}(d_r)}{\mathrm{Im}(d_{r+1})}.$$

These groups have the following basic properties.

2.1 The zeroth group $H_0(G, M) = M_G$, because

$$P_{1G} \to P_{0G} \to M_G \to 0$$

is exact.

2.2 If P is a projective G-module, then $H_r(G, P) = 0$ for all $r > 0$, because

$$\cdots \to 0 \to P \to P \to 0$$

is a projective resolution of P.

2.3 Let $P_\bullet \to M$ and $Q_\bullet \to N$ be projective resolutions of the G-modules M and N. Any homomorphism $\alpha\colon M \to N$ of G-modules extends to a morphism of complexes

$$\begin{array}{ccc} P_\bullet & \longrightarrow & M \\ \downarrow{\scriptstyle \alpha_\bullet} & & \downarrow{\scriptstyle \alpha} \\ Q_\bullet & \longrightarrow & N \end{array}$$

and the homomorphisms

$$H_r(\alpha_\bullet)\colon H_r(P_\bullet) \to H_r(Q_\bullet)$$

are independent of the choice of $\alpha_\bullet$. When we apply this statement to the identity map $\mathrm{id}\colon M \to M$, we find that the groups $H_r(G, M)$ are well-defined up to a well-defined isomorphism. The statement for a general α then shows that $M \mapsto H_r(G, M)$ is a functor from the category of G-modules to the category of abelian groups.

2.4 A short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of G-modules gives rise to a long exact sequence

$$\cdots \to H_r(G, M) \to H_r(G, M'') \xrightarrow{\delta_r} H_{r-1}(G, M') \to \cdots \to H_0(G, M'') \to 0.$$

Moreover, the association

$$\text{short exact sequence} \mapsto \text{ long exact sequence}$$

is functorial, i.e., a morphism of short exact sequences induces a morphism of long exact sequences.

REMARK 2.5 The family of functors $(H_r(G,\cdot))_{r\geq 0}$ and the boundary maps δ_r are uniquely determined by the properties (2.1, 2.2, 2.4).

Just as in the case of cohomology, it is possible to give an explicit description of $H_r(G,M)$ as the quotient of a group of r-cycles by a subgroup of r-boundaries—see the references later in this chapter.

The group $H_1(G,\mathbb{Z})$

Using only the properties of the homology groups listed above, we shall compute $H_1(G,\mathbb{Z})$.

The ***augmentation map*** is

$$\mathbb{Z}[G]\to\mathbb{Z},\quad \sum n_g g\mapsto \sum n_g.$$

Its kernel is called the ***augmentation ideal*** I_G. Clearly I_G is a free $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ with basis $\{g-1 \mid g\in G, g\neq 1\}$, and so

$$M/I_GM = M_G \overset{(2.1)}{\simeq} H_0(G,M).$$

Consider the exact (***augmentation***) sequence:

$$0\to I_G\to\mathbb{Z}[G]\to\mathbb{Z}\to 0. \tag{19}$$

The G-module $\mathbb{Z}[G]$ is projective (because it is a free $\mathbb{Z}[G]$-module), and so $H_1(G,\mathbb{Z}[G])=0$. Therefore we obtain an exact sequence of homology groups

$$0\to H_1(G,\mathbb{Z})\to I_G/I_G^2\to\mathbb{Z}[G]/I_G\to\mathbb{Z}\to 0.$$

The middle map is induced by the inclusion $I_G\hookrightarrow\mathbb{Z}[G]$, and so is zero. Therefore the sequence shows that

$$H_1(G,\mathbb{Z})\xrightarrow{\simeq} I_G/I_G^2 \tag{20}$$

and

$$\mathbb{Z}[G]_G\xrightarrow{\simeq}\mathbb{Z}$$

i.e., $\mathbb{Z}$ is the largest quotient of $\mathbb{Z}[G]$ on which G acts trivially. Note that $I_G^2\overset{\text{def}}{=} I_G\cdot I_G$ is the $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ generated by elements of the form

$$(g-1)(g'-1),\quad g,g'\in G.$$

LEMMA 2.6 *Let G^c be the commutator subgroup of G, so that G/G^c is the largest abelian quotient G^{ab} of G. Then the map $g\mapsto(g-1)+I_G^2$ induces an isomorphism*

$$\frac{G}{G^c}\to\frac{I_G}{I_G^2}. \tag{21}$$

PROOF. Consider the map

$$g \mapsto (g-1) + I_G^2 : G \to I_G/I_G^2.$$

This is a homomorphism because

$$\begin{aligned} gg' - 1 &= (g-1)(g'-1) + (g-1) + (g'-1) \\ &\equiv (g-1) + (g'-1) \bmod I_G^2. \end{aligned}$$

Since I_G/I_G^2 is commutative, the map factors through G^{ab}. To prove that it is an isomorphism, we construct an inverse. Recall that I_G is freely generated as a $\mathbb{Z}$-module by the elements $g-1$. Consider the homomorphism $I_G \to G^{\mathrm{ab}}$ mapping $g-1$ to the class of g. From the identity

$$(g-1)(g'-1) = (gg'-1) - (g-1) - (g'-1)$$

we see that $(g-1)(g'-1)$ maps to 1. Since I_G^2 is generated by elements of this form, this shows that the map factors through I_G/I_G^2. The two maps we have constructed are inverse. □

PROPOSITION 2.7 *There is a canonical isomorphism*

$$H_1(G,\mathbb{Z}) \simeq G^{\mathrm{ab}}.$$

PROOF. Combine the isomorphism (20) with the inverse of (21). □

ASIDE 2.8 For any group G, there exists a topological space BG, called the ***classifying space*** of G, such that $G = \pi_1(BG)$ and $H_r(BG,\mathbb{Z}) = H_r(G,\mathbb{Z})$ for all r (Rosenberg 1994, 5.1.16, 5.1.27). In terms of BG, the proposition simply states that $H_1(BG,\mathbb{Z}) \simeq \pi_1(BG)^{\mathrm{ab}}$.

3 The Tate groups

Throughout this section, G is a finite group.

For a G-module M, the ***norm map*** $\mathrm{Nm}_G : M \to M$ is defined to be

$$m \mapsto \textstyle\sum_{g\in G} gm.$$

Let $g' \in G$. As g runs through the elements of G, so also do $g'g$ and gg', and so $g'(\mathrm{Nm}_G(m)) = \mathrm{Nm}_G(m) = \mathrm{Nm}_G(g'm)$. Hence

$$\mathrm{Im}(\mathrm{Nm}_G) \subset M^G, \qquad I_G M \subset \mathrm{Ker}\,\mathrm{Nm}_G\,.$$

Therefore, we get an exact commutative diagram,

$$\begin{array}{ccccccccc} & & & & M & \xrightarrow{\mathrm{Nm}_G} & M & & \\ & & & & \downarrow & & \uparrow & & \\ 0 & \longrightarrow & \mathrm{Ker}(\mathrm{Nm}_G)/I_G M & \longrightarrow & M/I_G M & \longrightarrow & M^G & \longrightarrow & M^G/\mathrm{Nm}_G(M) \longrightarrow 0. \end{array}$$

As $H_0(G,M) = M/I_G M$ and $H^0(G,M) = M^G$, the bottom row of this can be rewritten

$$0 \to \mathrm{Ker}(\mathrm{Nm}_G)/I_G M \to H_0(G,M) \xrightarrow{\mathrm{Nm}_G} H^0(G,M) \to M^G/\mathrm{Nm}_G(M) \to 0.$$

Tate defined

$$H_T^r(G,M) = \begin{cases} H^r(G,M) & r > 0 \\ M^G/\operatorname{Nm}_G(M) & r = 0 \\ \operatorname{Ker}(\operatorname{Nm}_G)/I_G M & r = -1 \\ H_{-r-1}(G,M) & r < -1. \end{cases}$$

Thus, the exact sequence now becomes

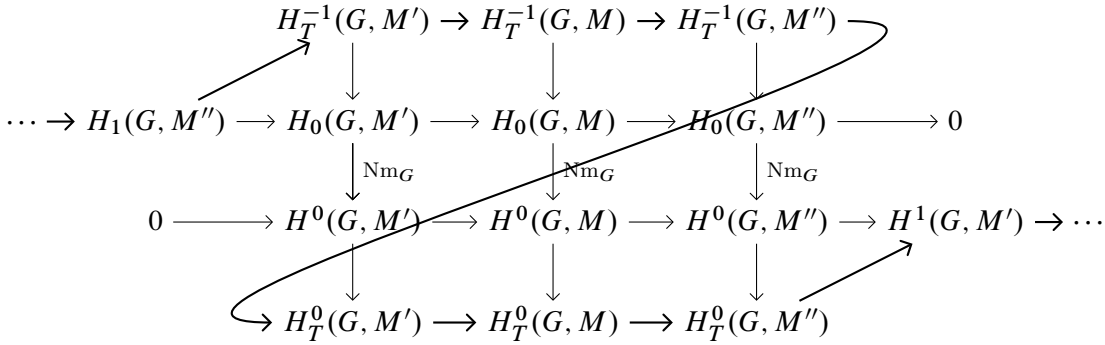
$$0 \to H_T^{-1}(G,M) \to H_0(G,M) \xrightarrow{\operatorname{Nm}_G} H^0(G,M) \to H_T^0(G,M) \to 0.$$

The groups $H_T^r(G,M)$ are known as the ***Tate cohomology groups***. Often $H_T^r(G,M)$ is denoted by $\hat{H}^r(G,M)$. Since it causes no ambiguity, we sometimes omit the subscript T when $r > 0$.

For any short exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

we get a diagram



On applying the extended snake lemma (A.1) to the middle part of the diagram, we get a (very) long exact sequence

$$\cdots \to H_T^r(G,M') \to H_T^r(G,M) \to H_T^r(G,M'') \xrightarrow{\delta} H_T^{r+1}(G,M) \to \cdots \tag{22}$$

$(-\infty < r < \infty)$.

PROPOSITION 3.1 *If M is induced, then $H_T^r(G,M) = 0$ for all $r \in \mathbb{Z}$.*

PROOF. For $r > 0$, this was proved in (1.12).

Case $r = 0$. Recall (1.3) that $M \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ for some abelian group X, and so an element m of M can be written uniquely in the form $m = \sum_g (g \otimes x_g)$ with $x_g \in X$. If m is fixed by $g' \in G$, then $\sum_g (g'g \otimes x_g) = \sum_g (g \otimes x_g)$; in particular,[2] $g' \otimes x_e = g' \otimes x_{g'}$, i.e., $x_e = x_{g'}$. Therefore, if $m \in M^G$, then $x_g = x_e$ for all $g \in G$, and $m = \left(\sum_g g\right) \otimes x_e = \operatorname{Nm}_G(e \otimes x_e)$.

[2]Here, e is the neutral element in G.

Case $r = -1$. If $\mathrm{Nm}_G\left(\sum_g g \otimes x_g\right) = 0$, then $\sum_g x_g = 0$, and so

$$\sum_g \left(g \otimes x_g\right) = \sum_g \left((g-1) \otimes x_g\right) \in I_G M.$$

Case $r < -1$. Let $M = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$. Write X as a quotient $X_0 \twoheadrightarrow X$ of a free abelian group X_0. The kernel of this map will also be a free abelian group,[3] and so we have an exact sequence

$$0 \to X_1 \to X_0 \to X \to 0$$

with X_0 and X_1 free abelian groups. On tensoring this with $\mathbb{Z}[G]$, we obtain an exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to M_1 \to M_0 \to M \to 0. \tag{23}$$

Now

$$H_T^r(G, M_0) = 0 = H_T^r(G, M_1)$$

for $r < -1$ because M_0 and M_1 are free $\mathbb{Z}[G]$-modules and for $r \geq -1$ because M_0 and M_1 are induced. The (very) long exact sequence of (23) now shows that $H_T^r(G, M) = 0$ for all r. □

We know (15), p. 62, that every G-module M is a submodule of an induced module. It is also a quotient of an induced G-module because, on tensoring the augmentation sequence (19) with M, we obtain an exact sequence of G-modules

$$0 \to M' \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to M \to 0.$$

This allows us to prove results by dimension shifting in both directions. Using this, it is possible to extend to all r, most of the results we proved for the groups $H^r(G, M)$ with $r \geq 0$. For example, Shapiro's lemma and its consequences are true, and the restriction and corestriction maps we defined in (1.27) and (1.29) extend to all the Tate cohomology groups. Specifically, there are canonical homomorphisms:[4]

Res: $H_T^r(G, M) \to H_T^r(H, M)$ (H a subgroup of G);
Cor: $H_T^r(H, M) \to H_T^r(G, M)$ (H a subgroup of G).

Moreover, there is a natural action of G/H on $H_T^r(H, M)$ for all $r \in \mathbb{Z}$.

The composite $\mathrm{Res} \circ \mathrm{Cor}$ is still multiplication by $(G\colon H)$. As $H_T^r(\{1\}, M) = 0$ for all r, the argument in the proof of (1.30) shows that $H_T^r(G, M)$ is killed by $|G|$ for all r.

Note that

$$H_T^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) \simeq G/G^c.$$

PROPOSITION 3.2 *Let H be a subgroup of G.*

(a) *The map* Cor: $H_T^{-2}(H, \mathbb{Z}) \to H_T^{-2}(G, \mathbb{Z})$ *corresponds to the map* $H/H^c \to G/G^c$ *induced by the inclusion* $H \hookrightarrow G$.

(b) *The map* Res: $H_T^{-2}(G, \mathbb{Z}) \to H_T^{-2}(H, \mathbb{Z})$ *corresponds to the Verlagerung map* $G/G^c \to H/H^c$ *(V, 3.18).*

[3] We are using that every subgroup of a free abelian group is free abelian. Darij Grinberg points out that this fact is highly nontrivial (and nonconstructive), and that it is possible to avoid using it.

[4] However, the inflation map Inf: $H_T^r(G/H, M^H) \to H_T^r(G, M)$, H a normal subgroup of G, is defined only for $r \geq 1$.

PROOF. See Weiss 1969, 3-5-5, 3-5-7. I'll include the proof in a future version of the notes. □

There is a uniform explicit description of all the groups $H_T^r(G, M)$. In fact, there is an explicit complex $L_\bullet$ of G-modules (infinite in both directions) such that

$$H_T^r(G, M) = H^r(\mathrm{Hom}_G(L_\bullet, M)).$$

For $r > 0$ this leads directly to the description we gave above of $H^r(G, M)$ in terms of inhomogeneous cocycles and coboundaries. See Weiss 1969, Chapter I.

Cup-products

When the group G is finite, the cup-products extend in a unique way to all the cohomology groups, and have the same list of properties. See Weiss 1969, Chapter IV. A future version of the notes will contain a complete list of the properties we need (but not the proofs, which are lengthy but not difficult).

The cohomology of finite cyclic groups

We first compute the cohomology of $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{Q}/\mathbb{Z}$ regarded as G-modules with the trivial action.

LEMMA 3.3 *For every finite group G,*

(a) $H_T^r(G, \mathbb{Q}) = 0$ *all* $r \in \mathbb{Z}$;

(b) $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/(G : 1)\mathbb{Z}$ *and* $H^1(G, \mathbb{Z}) = 0$;

(c) *there is a canonical isomorphism*

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

PROOF. (a) The group $\mathbb{Q}$ is uniquely divisible, i.e., for all nonzero integers m, multiplication by $m\colon \mathbb{Q} \to \mathbb{Q}$ is an isomorphism. Therefore the map $H_T^r(m)\colon H_T^r(G, \mathbb{Q}) \to H_T^r(G, \mathbb{Q})$, which is also multiplication by m, is an isomorphism. When we take $m = (G\colon 1)$, we find that multiplication by m on $H_T^r(G, \mathbb{Q})$ is both zero (see 1.30) and an isomorphism, which is possible only if $H_T^r(G, \mathbb{Q}) = 0$.

(b) Because G acts trivially on $\mathbb{Z}$, $\mathbb{Z}^G = \mathbb{Z}$ and the norm map is multiplication by $(G : 1)$. Hence $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/(G : 1)\mathbb{Z}$. Moreover, $H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z})$ (see 1.18a), but, because $\mathbb{Z}$ is torsion-free, all homomorphisms $G \to \mathbb{Z}$ are zero.

(c) The cohomology sequence of

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

is an exact sequence

$$\begin{array}{ccccccc} H^1(G, \mathbb{Q}) & \longrightarrow & H^1(G, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & H^2(G, \mathbb{Z}) & \longrightarrow & H^2(G, \mathbb{Q}). \\ \| & & \| & & & & \| \\ 0 & & \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) & & & & 0 \end{array}$$

□

Let G be a finite cyclic group of order m, with generator σ. Then, by definition,

$$H_T^0(G,M) = \frac{\mathrm{Ker}(\sigma-1)}{\mathrm{Im}(\mathrm{Nm}_G)}$$
$$H_T^{-1}(G,M) = \frac{\mathrm{Ker}(\mathrm{Nm}_G)}{\mathrm{Im}(\sigma-1)}.$$

Recall that in (1.20) we showed that $H^1(G,M)$ is isomorphic to the same group as $H_T^{-1}(G,M)$. In fact, the cohomology groups of a finite cyclic group are periodic with period 2.

PROPOSITION 3.4 *Let G be a cyclic group of finite order. The choice of a generator for G determines isomorphisms*

$$H_T^r(G,M) \xrightarrow{\simeq} H_T^{r+2}(G,M)$$

for all G-modules M and all $r \in \mathbb{Z}$.

PROOF. Let σ generate G. Then the sequence

$$0 \to \mathbb{Z} \xrightarrow{m\mapsto \sum_{g\in G} gm} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\sigma^i\mapsto 1} \mathbb{Z} \to 0$$

is exact. Because the groups in the sequence and the kernel I_G of $\mathbb{Z}[G] \to \mathbb{Z}$ are free $\mathbb{Z}$-modules, the sequence remains exact after it is tensored with M. Thus

$$0 \to M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to M \to 0$$

is an exact sequence of G-modules. Recall (1.4) that $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M \approx \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$, where M_0 is M regarded as abelian group, and so $H_T^r(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} M) = 0$ for all r by (3.1). Therefore (see 1.13), the sequence defines isomorphisms

$$H_T^r(G,M) \xrightarrow{\simeq} H_T^{r+2}(G,M)$$

for all r. □

REMARK 3.5 Let γ be the element of $H^2(G,\mathbb{Z})$ corresponding under the isomorphism $H^2(G,\mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ to the map sending the chosen generator σ of G to $1/m$. Then the map $H_T^r(G,M) \to H_T^{r+2}(G,M)$ is $x \mapsto x \cup \gamma$. In a future version, I'll prove this. Serre, Local Fields, VIII, Section 4 gives the following hint: "the period isomorphisms are given by cup product with γ: this follows, for example, from the formulas for the cup product given in Cartan-Eilenberg (Homological Algebra) p. 252." Alternatively, see Weiss 1969, 4-5-10.

Let G be a finite cyclic group, and let M be a G-module. When the cohomology groups $H^r(G,M)$ are finite, we define the ***Herbrand quotient*** of M to be

$$h(M) = \frac{\left|H_T^0(G,M)\right|}{\left|H_T^1(G,M)\right|}.$$

PROPOSITION 3.6 *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of G-modules. If any two of the Herbrand quotients $h(M')$, $h(M)$, $h(M'')$ are defined, then so also is the third, and*

$$h(M) = h(M')h(M'').$$

PROOF. We can truncate the (very) long exact cohomology sequence as follows,

$$0 \to K \to H_T^0(M') \to H_T^0(M) \to H_T^0(M'') \to H^1(M') \to H^1(M) \to H^1(M'') \to K' \to 0,$$

where

$$K = \operatorname{Coker}(H_T^{-1}(M) \to H_T^{-1}(M'')) \approx \operatorname{Coker}(H^1(M) \to H^1(M'')) = K'.$$

The first statement is now obvious, and the second follows from the next lemma. □

LEMMA 3.7 *Let*

$$0 \to A_0 \to A_1 \to \cdots \to A_r \to 0$$

be a exact sequence of finite groups. Then

$$\frac{|A_0| \cdot |A_2| \cdot \cdots}{|A_1| \cdot |A_3| \cdot \cdots} = 1.$$

PROOF. For a short exact sequence, that is, $r = 2$, this is obvious, but every exact sequence can be broken up into short exact sequences,

$$\begin{aligned} 0 \to A_0 \to A_1 \to C_1 \to 0 \\ 0 \to C_1 \to A_2 \to C_2 \to 0 \\ \cdots \\ 0 \to C_{r-1} \to A_{r-1} \to A_r \to 0. \end{aligned}$$

Here $C_i = \operatorname{Coker}(A_{i-1} \to A_i) = \operatorname{Ker}(A_{i+1} \to A_{i+2})$. From these sequences we find that

$$1 = \frac{|A_0| \cdot |C_1|}{|A_1|} = \frac{|A_0| \cdot |A_2|}{|A_1| \cdot |C_2|} = \cdots.$$

□

PROPOSITION 3.8 *If M is a finite module, then $h(M) = 1$.*

PROOF. Consider the exact sequences

$$0 \to M^G \to M \xrightarrow{g-1} M \to M_G \to 0$$

and

$$0 \to H_T^{-1}(M) \to M_G \xrightarrow{\operatorname{Nm}_G} M^G \to H_T^0(M) \to 0,$$

where g is any generator of G. From the first sequence we find that M^G and M_G have the same order, and then from the second that $H_T^{-1}(M)$ and $H_T^0(M)$ have the same order. □

COROLLARY 3.9 *Let $\alpha: M \to N$ be a homomorphism of G-modules with finite kernel and cokernel. If either $h(M)$ or $h(N)$ is defined, then so also is the other, and they are equal.*

PROOF. Suppose $h(N)$ is defined, and consider the exact sequences:

$$0 \to \alpha(M) \to N \to \operatorname{Coker}(\alpha) \to 0$$

$$0 \to \operatorname{Ker}(\alpha) \to M \to \alpha(M) \to 0.$$

From the first sequence, we find that $h(\alpha M)$ is defined and equals $h(N)$, and from the second sequence we find that $h(M)$ is defined and equals $h(\alpha M)$. □

Tate's Theorem

For the remainder of this section, all cohomology groups will be the Tate groups, and so we drop the subscript T except in the main statements.

THEOREM 3.10 *Let G be a finite group, and let M be a G-module. If*

$$H^1(H, M) = 0 = H^2(H, M)$$

for all subgroups H of G, then $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$.

PROOF. If G is cyclic, this follows from the periodicity of the cohomology.

Assume now that G is solvable. We shall prove the theorem in this case by induction on the order of G.

Because G is solvable, it contains a proper normal subgroup H such that G/H is cyclic. Because H has order less than that of G, and the pair (H, M) satisfies the hypotheses of the theorem, $H^r(H, M) = 0$ for all r. Therefore (see 1.34), we have exact sequences

$$0 \to H^r(G/H, M^H) \to H^r(G, M) \to H^r(H, M) \qquad (*)$$

for all $r \geq 1$. Because $H^1(G, M) = 0 = H^2(G, M)$, $H^1(G/H, M^H) = H^2(G/H, M^H) = 0$, and because G/H is cyclic, this implies that $H^r(G/H, M^H) = 0$ for all r. Therefore, the sequences $(*)$ show that $H^r(G, M) = 0$ for all $r > 0$. We next show that $H^0(G, M) = 0$. Let $x \in M^G$. Because $H^0(G/H, M^H) = 0$, there exists a $y \in M^H$ such that $\mathrm{Nm}_{G/H}(y) = x$, and because $H^0(H, M) = 0$, there exists a $z \in M$ such that $\mathrm{Nm}_H(z) = y$. Now

$$\mathrm{Nm}_G(z) = (\mathrm{Nm}_{G/H} \circ \mathrm{Nm}_H)(z) = x.$$

Thus, we now know that $H^r(G, M) = 0$ for all $r \geq 0$.

To proceed further, we use the exact sequence

$$0 \to M' \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to M \to 0$$

obtained by tensoring the augmentation sequence (19) with M. Recall that

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}} M \overset{1.4}{\simeq} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 \overset{1.3}{\simeq} \mathrm{Ind}^G(M_0)$$

is induced, and so $H^r(H, \mathbb{Z}[G] \otimes_{\mathbb{Z}} M) = 0$ for all r and all subgroups H of G. Therefore,

$$H^r(H, M) \simeq H^{r+1}(H, M')$$

for all r and all H. In particular, M' satisfies the hypotheses of the theorem, and so (by what we have proved) $H^r(G, M') = 0$ for $r \geq 0$. In particular,

$$0 = H^0(G, M') = H^{-1}(G, M).$$

The argument, when repeated, gives that $H^{-2}(G, M) = 0$, etc.. This proves the theorem when G is solvable.

Now consider the case of an arbitrary finite group G. If G and M satisfy the hypotheses of the theorem, so also do G_p and M, where G_p is a Sylow p-subgroup. Therefore $H^r(G_p, M) = 0$ for all r and p, and so (see 1.33), the p-primary component of $H^r(G, M)$ is zero for all r and p. This implies that $H^r(G, M) = 0$ for all r. □

THEOREM 3.11 (TATE'S THEOREM) *Let G be a finite group and let C be a G-module. Suppose that for all subgroups H of G (including $H = G$),*

(a) $H^1(H, C) = 0$, *and*

(b) $H^2(H, C)$ *is a cyclic group of order equal to* $(H : 1)$.

Then, for all r, there is an isomorphism

$$H_T^r(G, \mathbb{Z}) \to H_T^{r+2}(G, C)$$

depending only on the choice of a generator for $H^2(G, C)$.

PROOF. Choose a generator γ for $H^2(G, C)$. Because $\mathrm{Cor} \circ \mathrm{Res} = (G : H)$, $\mathrm{Res}(\gamma)$ generates $H^2(H, C)$ for any subgroup H of G.

Let φ be a cocycle representing γ. Define $C(\varphi)$ to be the direct sum of C with the free abelian group having as basis symbols x_σ, one for each $\sigma \in G$, $\sigma \neq 1$, and extend the action of G on C to an action on $C(\varphi)$ by setting

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \varphi(\sigma, \tau).$$

The symbol "x_1" is to be interpreted as $\varphi(1, 1)$. This does define an action of G on $C(\varphi)$ because

$$\rho\sigma x_\tau = x_{\rho\sigma\tau} - x_{\rho\sigma} + \varphi(\rho\sigma, \tau),$$

whereas

$$\begin{aligned}\rho(\sigma x_\tau) &= \rho(x_{\sigma\tau} - x_\sigma + \varphi(\sigma, \tau)) \\ &= x_{\rho\sigma\tau} - x_\rho + \varphi(\rho, \sigma\tau) - (x_{\rho\sigma} - x_\rho + \varphi(\rho, \sigma)) + \rho\varphi(\sigma, \tau).\end{aligned}$$

These agree because φ satisfies the cocycle condition

$$\rho\varphi(\sigma, \tau) + \varphi(\rho, \sigma\tau) = \varphi(\rho\sigma, \tau) + \varphi(\rho, \sigma).$$

Note that φ is the coboundary of the 1-cochain $\sigma \mapsto x_\sigma$, and so γ maps to zero in $H^2(G, C(\varphi))$. For this reason, $C(\varphi)$ is called the ***splitting module*** for γ.

We shall first show that the hypotheses imply that

$$H^1(H, C(\varphi)) = 0 = H^2(H, C(\varphi))$$

for all subgroups H of G.

Recall that we have an exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

where I_G is the free abelian group with basis the elements $\sigma - 1$, $\sigma \in G$, $\sigma \neq 1$ Because $\mathbb{Z}[G]$ is induced, $H^r(H, \mathbb{Z}[G]) = 0$ for all r, and so

$$\begin{aligned}H^1(H, I_G) &\simeq H^0(H, \mathbb{Z}) \simeq \mathbb{Z}/(H : 1)\mathbb{Z}, \\ H^2(H, I_G) &\simeq H^1(H, \mathbb{Z}) = 0\end{aligned}$$

Define α to be the additive map $C(\varphi) \to \mathbb{Z}[G]$ such that

$$\begin{aligned}\alpha(c) &= 0 \text{ for all } c \in C \\ \alpha(x_\sigma) &= \sigma - 1.\end{aligned}$$

Clearly,

$$0 \to C \to C(\varphi) \xrightarrow{\alpha} I_G \to 0$$

is an exact sequence of G-modules. Its cohomology sequence reads

$$0 \to H^1(H, C(\varphi)) \to H^1(H, I_G) \to H^2(H, C) \xrightarrow{0} H^2(H, C(\varphi)) \to 0$$

The zeros at the ends use that $H^1(H, C) = 0$ and $H^2(H, I_G) = 0$. The map $H^2(H, C) \to H^2(H, C(\varphi))$ is zero because $H^2(H, C)$ is generated by $\mathrm{Res}(\gamma)$, and this maps to the restriction of the image of γ in $H^2(G, C(\varphi))$, which is zero. Therefore, $H^1(H, I_G) \to H^2(H, C)$ is onto, and hence is an isomorphism (because the two groups have the same order). Its kernel and cokernel, namely, $H^1(H, C(\varphi))$ and $H^2(H, C(\varphi))$, are therefore both zero

We deduce from the Theorem 3.10 that $H^r(H, C(\varphi)) = 0$ for all r. On splicing the two short exact sequences together, we obtain an exact sequence

$$0 \to C \to C(\varphi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \tag{24}$$

with the property that $H^r(G, C(\varphi)) = 0 = H^r(G, \mathbb{Z}[G])$ for all r. Therefore, the double boundary map is an isomorphism (1.13)

$$H^r(G, \mathbb{Z}) \to H^{r+2}(G, C).$$

□

REMARK 3.12 If M is a G-module such that $\mathrm{Tor}_1^{\mathbb{Z}}(M, C) = 0$, for example, if either M or C is torsion-free as a $\mathbb{Z}$-module, then one can tensor the above 4-term sequence with M and obtain isomorphisms

$$H_T^r(G, M) \to H_T^{r+2}(G, M \otimes C).$$

REMARK 3.13 The map $H_T^r(G, \mathbb{Z}) \to H_T^{r+2}(G, C)$ is cup-product with the chosen element $\gamma \in H^2(G, C)$.

EXAMPLE 3.14 Let K be a local field. We shall prove that for any finite Galois extension L of K with Galois group G, $H^2(G, L^\times)$ is cyclic of order $[L\colon K]$ with a canonical generator $u_{L/K}$. Since we know that $H^1(G, L^\times) = 0$ (Hilbert's Theorem 90), Tate's theorem shows that cup-product with $u_{L/K}$ is an isomorphism

$$G^{\mathrm{ab}} = H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, L^\times) = K^\times / \mathrm{Nm}\, L^\times.$$

The inverse isomorphism $K^\times / \mathrm{Nm}\, L^\times \xrightarrow{\simeq} G^{\mathrm{ab}}$ is the local Artin map. The global Artin map can be obtained by a similar argument.

NOTES The book Weiss 1969 gives a complete and very detailed account of the basic theory of Tate cohomology groups. For a recent paper on the Tate sequence (24), its generalizations, and associated boundary maps, see Buckingham, Acta Arith. 149 (2011), no. 4, 383–402.

4 The Cohomology of Profinite Groups

Direct limits

A partially ordered set $(I, \leq)$ is said to be ***directed*** if for any two elements i and j of I, there exists a k such that $i, j \leq k$. Suppose that for every element i of a directed set $(I, \leq)$ we have a set A_i, and for every inequality $i \leq j$ we have a map $\alpha_{ji}: A_i \to A_j$. If

(a) $\alpha_{ii} = \mathrm{id}$ for all $i \in I$, and

(b) $\alpha_{kj} \circ \alpha_{ji} = \alpha_{ki}$ whenever $i \leq j \leq k$,

then the family (A_i, α_{ji}) is called a ***direct system.*** On the disjoint union $\coprod A_i$ of the A_i, introduce the equivalence relation under which $a_i \in A_i$ is related to $a_j \in A_j$ if and only if $\alpha_{ki}(a_i) = \alpha_{kj}(a_j)$ for some $k \geq i, j$. The corresponding quotient set is called the ***direct limit*** of the A_i (relative to the α_{ji}):

$$A = \varinjlim A_i.$$

There is for each i a canonical map

$$\alpha_i: A_i \to A,$$

possessing the following properties:

(a) $\alpha_i = \alpha_j \circ \alpha_{ji}$ for $j \geq i$;

(b) $\alpha_i(a_i) = \alpha_j(a_j) \iff \alpha_{ki}(a_i) = \alpha_{kj}(a_j)$ for some $k \geq i, j$;

(c) $A = \bigcup \alpha_i(A_i)$.

The system (A, α_i) has the following universal property: let T be a set and let (β_i), $\beta_i: A_i \to T$, be a family of maps such that $\beta_i = \beta_j \circ \alpha_{ji}$ for $i \leq j$; then there exists a unique map $\beta: A \to T$ such that $\beta_i = \beta \circ \alpha_i$ for all i.

If the A_i are abelian groups and the α_{ij} are homomorphisms, then A has a unique structure of an abelian group for which the α_i are homomorphisms.

LEMMA 4.1 *For any direct system of exact sequences*

$$A_i \to B_i \to C_i,$$

the sequence

$$\varinjlim A_i \to \varinjlim B_i \to \varinjlim C_i$$

is again exact. Therefore the formation of direct limits commutes with passage to cohomology in complexes.

PROOF. Exercise for the reader. □

Profinite groups

Let G be a profinite group. This means that G is a compact[5] topological group for which the open normal subgroups form a fundamental system of neighbourhoods of 1. Note that every open subgroup is of finite index (because its cosets cover G). For example, a finite group with the discrete topology is profinite, and every discrete profinite group is finite. A Galois

[5] Following Bourbaki, I require compact spaces to be Hausdorff.

group $G = \mathrm{Gal}(L/K)$ is a profinite group — the open subgroups are exactly those fixing a finite extension of K contained in L — and every profinite group occurs as a Galois group. For a profinite group, we use the topology to modify our notion of cohomology group.

First, we consider only those G-modules for which the map

$$G \times M \to M$$

is continuous when M is endowed with the discrete topology, i.e., the topology in which every subset is open. Equivalent conditions:

- $\diamond$ $M = \bigcup M^H$, H runs through the open subgroups of G;
- $\diamond$ the stabilizer in G of any element of M is open.

A module satisfying these conditions is called a ***discrete*** G-module.

The discrete G-modules form an abelian category with enough injectives, and so we can define cohomology groups $H^r_{\mathrm{cts}}(G, M)$, $r \geq 0$, by taking injective resolutions, just as before. Moreover, the groups can be calculated using ***continuous cocycles***: for $r \geq 0$, let $C^r_{\mathrm{cts}}(G, M)$ be the group of continuous maps $G^r \to M$, and define $d^r : C^r_{\mathrm{cts}}(G, M) \to C^{r+1}_{\mathrm{cts}}(G, M)$ as before; then

$$H^r_{\mathrm{cts}}(G, M) = \frac{Z^r_{\mathrm{cts}}(G, M)}{B^r_{\mathrm{cts}}(G, M)},$$

where $Z^r_{\mathrm{cts}}(G, M) = \mathrm{Ker}(d^r)$ and $B^r_{\mathrm{cts}}(G, M) = \mathrm{Im}(d^{r-1})$.

Let $\varphi : G^r \to M$ be a continuous r-cochain. Then $\varphi(G^r)$ is compact (because G^r is compact) and discrete (because M is discrete), and so it is finite, and hence it is contained in M^{H_0} for some open normal subgroup H_0 of G. The inverse image $\varphi^{-1}(m)$ of each point m of $\varphi(G^r)$ is open, and so contains a translate of $H(m)^r$ for some open normal subgroup $H(m)$ of G. Let $H_1 = \bigcap_{m \in \varphi(G^r)} H(m)$.[6] This is again an open subgroup of G, and φ factors through $(G/H_1)^r$. Let $H = H_0 \cap H_1$. Then φ arises by inflation from an r-cocycle on G/H with values in M^H. In other words, the map

$$\varinjlim C^r(G/H, M^H) \to C^r_{\mathrm{cts}}(G, M)$$

is surjective. It is not difficult to see that it is also injective. Because passage to the direct limit commutes with the formation of kernels and cokernels, and hence with the formation of cohomology, we obtain the following proposition:

PROPOSITION 4.2 *The maps* $\mathrm{Inf} : H^r(G/H, M^H) \to H^r_{cts}(G, M)$ *realize* $H^r_{cts}(G, M)$ *as the direct limit of the groups* $H^r(G/H, M^H)$ *as* H *runs through the open normal subgroups* H *of* G*:*

$$\varinjlim H^r(G/H, M^H) = H^r_{cts}(G, M).$$

Explicitly, the statement means that each element of $H^r_{\mathrm{cts}}(G, M)$ arises by inflation from some group $H^r(G/H, M^H)$ and if $a \in H^r(G/H, M^H)$ and $a' \in H^r(G/H', M^{H'})$ map to the same element in $H^r_{\mathrm{cts}}(G, M)$, then they map to the same element in $H^r(G/H'', M^{H''})$ for some open subgroup $H'' \subset H \cap H'$.

[6] This group may not be small enough for φ to factor through $(G/H_1)^r$. Instead, for any point of G^r, take a translate of an open normal subgroup containing the point and fully contained in a fibre of φ. In this way, we get an open covering of G^r, which may be replaced by a finite subcovering because G^r is compact. Now let H_1 be the intesection of all the subgroups whose translates occur in this subcovering.

COROLLARY 4.3 *For every profinite group G and discrete G-module M, $H^r(G,M)$ is a torsion group for all $r>0$.*

PROOF. Each of the groups $H^r(G/H,M^H)$, $r>0$, is torsion (see 1.31). □

Most of the theory concerning the cohomology groups $H^r(G,M)$ for $r\geq 0$ continues to hold for the groups defined by continuous cochains. For example, if H is a closed subgroup of G, there are maps Inf, Res, and Cor (the last requires H to be of finite index), and there are cup-product maps.

In future, all cohomology groups will be defined using continuous cochains (and the subscript cts will be dropped). In practice, this will mean that either G is an infinite profinite group, and it matters that we take continuous cochains, or G is finite, in which case it doesn't (and the groups are defined for all $r\in\mathbb{Z}$).

PROPOSITION 4.4 *Let G be a profinite group, and let M be a discrete G-module. If $M=\varinjlim M_i$, where $M_i\subset M$, then $H^r(G,M)=\varinjlim H^r(G,M_i)$.*

PROOF. Because G is compact and M is discrete, the image of any r-cochain $f:G^r\to M$ is finite. Since the M_i form a directed system of submodules of M (i.e., given M_i and M_j, there is an M_k containing both of them) and $M=\bigcup M_i$, every finite subset of M is contained in an M_i. It follows that $C^r(G,M)=\varinjlim C^r(G,M_i)$, and so Lemma 4.1 shows that

$$H^r(C^\bullet(G,M))=\varinjlim H^r(C^\bullet(G,M_i)).$$

□

ASIDE 4.5 (For the experts.) Let G be a profinite group, let $\mathsf{M}(G)$ be the category of all G-modules, and $\mathsf{C}(G)$ the category of discrete G-modules. Then $\mathsf{C}(G)$ is a full subcategory of $\mathsf{M}(G)$. Moreover, there is a functor

$$M\mapsto M^*\overset{\text{def}}{=}\bigcup_{H\text{ open in }G}M^H:\mathsf{M}(G)\to\mathsf{C}(G).$$

Clearly,

$$\operatorname{Hom}_G(M,N^*)=\operatorname{Hom}_G(M,N)$$

for M a discrete G-module. The inclusion functor $i:\mathsf{C}(G)\to\mathsf{M}(G)$ is exact, but doesn't preserve injectives—hence $H^r(G,M)\neq H^r(G,iM)$ in general. On the other hand, $M\mapsto M^*$ preserves injectives, but is only left exact—hence $\mathsf{C}(M)$ has enough injectives. Again $H^r(G,M)\neq H^r(G,M^*)$ (however, there is a spectral sequence ...).

NOTES In the mid-1930s, Hurewicz showed that the homology groups of an "aspherical space" X depend only on the fundamental group π of the space. Thus one could think of the homology groups $H_r(X,\mathbb{Z})$ of the space as being the homology groups $H_r(\pi,\mathbb{Z})$ of the group π. It was only in the mid-1940s that Hopf, Eckmann, Eilenberg, MacLane, Freudenthal and others gave purely algebraic definitions of the homology and cohomology groups of a group G. It was then found that H^1 coincided with the group of crossed homomorphisms modulo principal crossed homomorphisms, and H^2 with the group of equivalence classes of "factor sets", which had been introduced much earlier (e.g., I. Schur, Über die Darstellung der endlichen..., 1904; O. Schreier, Über die Erweiterungen von Gruppen, 1926; R. Brauer, Über Zusammenhänge..., 1926). For more on the history, see Mac Lane 1978.

Our proof of Tate's theorem follows Tate's original proof (Tate 1952). At that time, there was no published account of the Tate groups, and so Tate proved his theorem only for $r\geq 0$, but ended with an enigmatic promise to extend the result to negative r and to recover the Artin map. The construction of the Tate cohomology groups was first published in Cartan and Eilenberg 1956 following Tate's ideas.

A good source for the material in the first three sections is Serre 1962, Part 3. There is a somewhat abbreviated version of the same material in Atiyah and Wall 1967. See also Iyanaga 1975, Chapter I, and Weiss 1969. For the cohomology of profinite groups, see Serre 1964 and Shatz 1972.

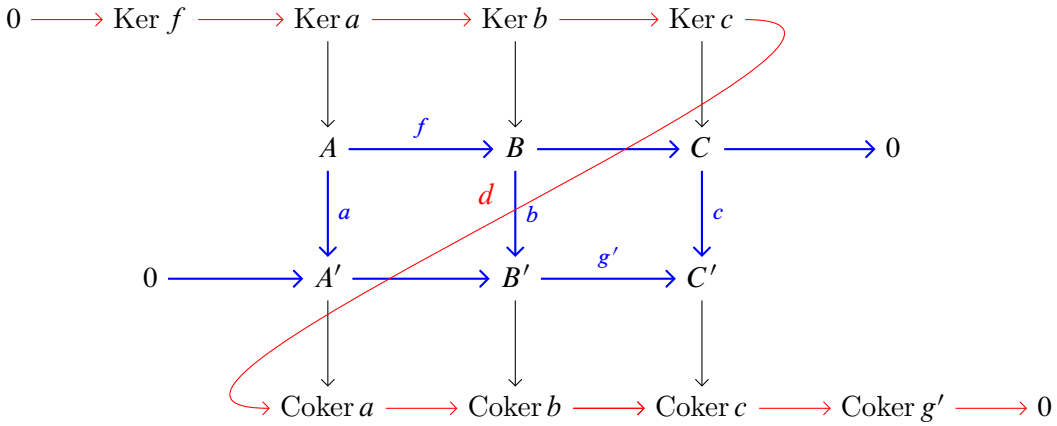
For a discussion of the origins of cohomology in class field theory, see sx857593.

A Appendix: Some Homological Algebra

Ça me semble extrêmement plaisant de ficher comme ça beaucoup de choses, pas drôles quand on les prend séparément, sous le grand chapeau des foncteurs dérivés.
Grothendieck, Letter to Serre, 18.2.1955.[7]

Some exact sequences[8]

LEMMA A.1 (THE EXTENDED SNAKE LEMMA) *The exact commutative diagram in blue gives rise to the exact sequence in red:*



PROOF. Except for the first and last terms, this is standard. A small diagram chase shows that $\operatorname{Ker} f \subset \operatorname{Ker}(a)$, from which exactness at $\operatorname{Ker} a$ follows. The proof of exactness at $\operatorname{Coker} c$ is similarly straightforward. □

LEMMA A.2 (KERNEL-COKERNEL LEMMA) *Every pair of homomorphisms*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

of abelian groups gives rise to an exact sequence

$$0 \to \operatorname{Ker} f \to \operatorname{Ker} g \circ f \xrightarrow{f} \operatorname{Ker} g \to \operatorname{Coker} f \to \operatorname{Coker} g \circ f \to \operatorname{Coker} g \to 0.$$

[7] To me it seems extremely pleasant to stick all sorts of things, which are not much fun when considered separately, under the big hat of derived functors

[8] Based on F. Lemmermeyer, The Snake Lemma.

PROOF. Apply the extended snake lemma to

$$\begin{array}{ccccccc} & & A & \xrightarrow{f} & B & \longrightarrow & \mathrm{Coker}(f) \longrightarrow 0 \\ & & \downarrow{\scriptstyle g\circ f} & & \downarrow{\scriptstyle g} & & \downarrow \\ 0 & \longrightarrow & C & \xrightarrow{\mathrm{id}} & C & \longrightarrow & 0 \end{array}$$

□

The language of category theory

A ***category*** C consists of a nonempty class $\mathrm{ob}(\mathsf{C})$ of objects, a set $\mathrm{Hom}(A, B)$ for each pair of objects A, B (called the set of ***morphisms*** from A to B), and a map

$$(\alpha, \beta) \mapsto \beta \circ \alpha \colon \mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$$

for each triple of objects A, B, C, satisfying the following conditions:

(a) composition of morphisms is associative;

(b) for each object A, $\mathrm{Hom}(A, A)$ has an element id_A that is a left and right identity for composition.

It is to be understood that the sets $\mathrm{Hom}(A, B)$ are disjoint, so that a morphism determines its source and target.

A ***covariant functor*** $F \colon \mathsf{C} \to \mathsf{D}$ is a "map" that attaches to each object A of C an object $F(A)$ of D and to each morphism $\alpha \colon A \to B$ a morphism $F(\alpha) \colon F(A) \to F(B)$ such that $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ and $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.

A functor $F \colon \mathsf{C} \to \mathsf{D}$ is ***left adjoint*** to the functor $G \colon \mathsf{D} \to \mathsf{C}$ if there is a natural isomorphism

$$\mathrm{Hom}_{\mathsf{D}}(F(A), B) \simeq \mathrm{Hom}_{\mathsf{C}}(A, G(B)).$$

If the sets $\mathrm{Hom}(A, B)$ are endowed with the structures of abelian groups in such a way that the composition maps are bi-additive, and every finite collection of objects in C has a direct sum, then C (together with the structures) is called an ***additive category***. To say that A and B admit a direct sum means that there is an object $A \oplus B$ in C and maps $i_A \colon A \to A \oplus B$, $i_B \colon B \to A \oplus B$, $p_A \colon A \oplus B \to A$, $p_B \colon A \oplus B \to B$ such that:

$$\begin{aligned} p_A \circ i_A &= \mathrm{id}_A & \qquad p_B \circ i_B &= \mathrm{id}_B \\ p_A \circ i_B &= 0 & \qquad p_B \circ i_A &= 0 \end{aligned}$$

$$i_A p_A + i_B p_B = 1_{A \oplus B}.$$

Let C be an additive category. A sequence

$$0 \to A \to B \xrightarrow{\alpha} C$$

is ***exact*** if the sequence of abelian groups

$$0 \to \mathrm{Hom}(T, A) \to \mathrm{Hom}(T, B) \to \mathrm{Hom}(T, C)$$

is exact for all objects T. A sequence

$$A \xrightarrow{\beta} B \to C \to 0$$

is ***exact*** if the sequence of abelian groups

$$0 \to \mathrm{Hom}(C, T) \to \mathrm{Hom}(B, T) \to \mathrm{Hom}(A, T)$$

is exact for all objects T. When the first sequence is exact, A is called the ***kernel*** of α, and when the second is exact, C is called the ***cokernel*** of β.

A morphism $A \to B$ is said to be ***injective*** (or a ***monomorphism***) if $0 \to A \to B$ is exact. Similarly, it is ***surjective*** (or an ***epimorphism***) if $A \to B \to 0$ is exact.

Let C be an additive category in which every morphism has both a kernel and a cokernel. Let $\alpha\colon A \to B$ be morphism. The kernel of the cokernel $B \to C$ of α is called the ***image*** of α, and the cokernel of the kernel of α is called the ***coimage*** of α. There is a canonical map from the coimage of α to the image of α, and if this is always an isomorphism, then C is called an ***abelian category***.[9]

Functors between additive categories will be assumed to be additive, i.e., such that the maps $\mathrm{Hom}(A, B) \to \mathrm{Hom}(F(A), F(B))$ are homomorphisms of abelian groups. Such a functor is said to be ***exact*** if it maps exact sequences to exact sequences.

For example, for every ring R, the category of R-modules is an abelian category, and, for every topological space X, the category of sheaves of abelian groups on X is an abelian category.

In the remainder of this section, C will be an abelian category. The reader will lose little (so far as this course is concerned) by taking C to be the category of modules over a ring, for example, the category of modules over a group ring $\mathbb{Z}[G]$.

Injective objects

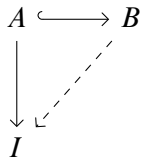
Let C be an abelian category. An object I of C is ***injective*** if $\mathrm{Hom}(\cdot, I)$ is an exact functor, i.e., if

$$0 \to A \to B \to C \to 0$$

exact in C implies that

$$0 \to \mathrm{Hom}(C, I) \to \mathrm{Hom}(B, I) \to \mathrm{Hom}(A, I) \to 0$$

is exact. The last sequence is automatically exact except at $\mathrm{Hom}(A, I)$, and so to say that I is injective means that, whenever A is a subobject of B, every homomorphism $A \to I$ extends to B.



An abelian category C is said to have ***enough injectives*** if every object admits an injective homomorphism into an injective object.

PROPOSITION A.3 *A module M over a principal ideal domain R is injective if and only if it is divisible, i.e., the map $x \mapsto rx$ is surjective for all $r \in R$, $r \neq 0$.*

PROOF. injective $\Longrightarrow$ divisible: Let $m \in M$ and let r be a nonzero element of R. The map $x \mapsto rx\colon R \to R$ is injective, and every extension of $x \mapsto xm\colon R \to M$ to R will send 1 to an element m' such that $rm' = m$.

divisible $\Longrightarrow$ injective: Suppose that M is divisible, and consider a homomorphism $\alpha\colon A \to M$, where A is a submodule of B. On applying Zorn's lemma to the set of pairs

[9] If you are mystified by this paragraph, you may find sx2263197 helpful.

(A', α'), where A' is a submodule of B containing A and α' extends α to A', we obtain a maximal such pair (A_1, α_1). If $A_1 \neq B$, then there exists a $b \in B \smallsetminus A_1$, and we define $I = \{r \in R \mid rb \in A_1\}$. Because M is divisible, the map $r \mapsto \alpha_1(rb)\colon I \to M$ extends[10] to R, but this implies that α_1 extends to $A_1 + Rb$, which contradicts the maximality of (A_1, α_1). □

Therefore, when R is a principal ideal domain, every quotient of an injective module is injective, for example, K/R, where K is the field of fractions of R. In particular, $\mathbb{Q}/\mathbb{Z}$ is an injective abelian group.

PROPOSITION A.4 *The category of modules over a principal ideal domain R has enough injectives.*

PROOF. Write M as a quotient $M \approx F/N$ of a free R-module F, and consider the exact commutative diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N & \longrightarrow & F \otimes_R K & \longrightarrow & (F \otimes_R K)/N & \longrightarrow & 0. \end{array}$$

Because $F \to F \otimes_R K$ is an injective map and $F \otimes_R K$ is an injective object, the map $M \to (F \otimes_R K)/N$ is an injective homomorphism of M into an injective R-module. □

For abelian groups, the proposition can also be proved as follows: for an abelian group M, let $M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$; choose a free abelian group F mapping onto $M^\vee$, $F \twoheadrightarrow M^\vee$; then $M \hookrightarrow M^{\vee\vee} \hookrightarrow F^\vee$, and $F^\vee$ is injective.

PROPOSITION A.5 *A functor that admits an exact left adjoint preserves injectives.*

PROOF. Let F' be an exact left adjoint to the functor $F\colon \mathsf{C} \to \mathsf{D}$. For every injective object I in C, the functor $\mathrm{Hom}_{\mathsf{D}}(\cdot, F(I))$ is isomorphic to the functor $\mathrm{Hom}_{\mathsf{C}}(F'(\cdot), I)$, which is exact because it is the composite of two exact functors, namely, F' and $\mathrm{Hom}_{\mathsf{C}}(\cdot, I)$. □

Right derived functors

Let C be an abelian category with enough injectives, and let $F\colon \mathsf{C} \to \mathsf{D}$ be a left exact functor from C to a second abelian category. Thus, a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

in C gives rise to an exact sequence

$$0 \to F(M') \to F(M) \to F(M'')$$

in D. The theory of derived functors provides a natural extension of this last sequence to a long exact sequence.

Let M be an object of C. A ***resolution*** of M is a long exact sequence

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \to \cdots \to I^r \xrightarrow{d^r} I^{r+1} \to \cdots .$$

If the I^r's are injective objects of C, then it is called an ***injective resolution***. We sometimes denote this complex by $M \to I^\bullet$.

[10] For the moment, this is left as an exercise for the reader.

LEMMA A.6 *An injective resolution $M \to I^\bullet$ of M exists, and if $M \to J^\bullet$ is a second injective resolution, then there exists a homomorphism from $M \to I^\bullet$ to $M \to J^\bullet$, i.e., there exists a commutative diagram,*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & \cdots \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M & \longrightarrow & J^0 & \longrightarrow & J^1 & \longrightarrow & \cdots \end{array}$$

PROOF. By assumption, there exists an injective morphism

$$0 \to M \to I^0$$

with I^0 injective. Let B^1 be the cokernel of the map. Again, there exists an injective morphism

$$0 \to B^1 \to I^1$$

with I^1 injective. Now

$$0 \to M \to I^0 \to I^1$$

is exact. Let $B^2 = \operatorname{Coker}(B^1 \to I^1)$, and continue in this fashion.

Similarly, a morphism of resolutions can be constructed step by step, using the definition of an injective object. □

On applying a left exact functor F to an injective resolution $M \to I^\bullet$ of a object M, we obtain a complex

$$F(I^\bullet)\colon F(I^0) \to F(I^1) \to \cdots \to F(I^r) \xrightarrow{F(d^r)} F(I^{r+1}) \to \cdots$$

which may no longer be exact, and so the cohomology groups

$$H^r(F(I^\bullet)) \stackrel{\text{def}}{=} \frac{\operatorname{Ker}(F(d^r))}{\operatorname{Im}(F(d^{r-1}))}$$

may be nonzero.

REMARK A.7 Because F is left exact, the sequence

$$0 \to F(M) \to F(I^0) \xrightarrow{d^0} F(I^1)$$

is exact. Therefore,

$$H^0(F(I^\bullet)) \stackrel{\text{def}}{=} \operatorname{Ker}(d^0) = F(M).$$

PROPOSITION A.8 *Let $M \to I^\bullet$ and $N \to J^\bullet$ be injective resolutions of objects M and N of C. Every morphism $\alpha\colon M \to N$ extends to a map of complexes*

$$\begin{array}{ccc} M & \longrightarrow & I^\bullet \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^\bullet} \\ N & \longrightarrow & J^\bullet. \end{array}$$

For every left exact functor F, the morphism

$$H^r(F(\alpha^\bullet))\colon H^r(F(I^\bullet)) \to H^r(F(J^\bullet))$$

is independent of the choice of $\alpha^\bullet$.

We discuss the proof below.

The proposition, applied to the identity morphism $M \to M$, implies that the objects $H^r(F(I^\bullet))$ are well-defined up to a well-defined isomorphism: given two injective resolutions $M \to I^\bullet$ and $M \to J^\bullet$ of M, there exists a morphism $\alpha^\bullet: I^\bullet \to J^\bullet$ extending the identity map on M, and the maps $H^r(F(I^\bullet)) \to H^r(F(J^\bullet))$ it defines are isomorphisms independent of the choice of $\alpha^\bullet$. Now, for each object M of C, we choose an injective resolution $M \to I^\bullet$, and we define

$$(R^r F)(M) = H^r(F(I^\bullet)).$$

A morphism $\alpha: M \to N$ gives rise to a well-defined morphism $(R^r F)(M) \to (R^r F)(N)$, and these maps make $R^r F$ into a functor. They are called the ***right derived functors*** of F.

The next two lemmas prove something a little more precise than the proposition.

LEMMA A.9 *Let $M \to I^\bullet$ and $N \to J^\bullet$ be resolutions of objects M and N of C. If $N \to J^\bullet$ is an injective resolution, then every morphism $\alpha: M \to N$ extends to a morphism*

$$\begin{array}{ccc} M & \longrightarrow & I^\bullet \\ \downarrow & & \downarrow \\ N & \longrightarrow & J^\bullet. \end{array}$$

of complexes.

PROOF. Bucur and Deleanu 1968, 7.5. □

Two morphisms $\alpha^\bullet, \beta^\bullet: I^\bullet \to J^\bullet$ of complexes are said to be ***homotopic*** if there exists a family of morphisms $k^r: I^r \to J^{r-1}$ (a ***homotopy***) such that

$$\alpha^r - \beta^r = d^{r-1} \circ k^r + k^{r+1} \circ d^r$$

for all r.

Note that, for every $x \in Z^r(I^\bullet) \stackrel{\text{def}}{=} \operatorname{Ker}(d^r)$,

$$\alpha^r(x) - \beta^r(x) = d^{r-1}(k^r(x)) \in \operatorname{Im}(d^{r-1}) \stackrel{\text{def}}{=} B^r(J^\bullet).$$

Therefore $\alpha^r(x)$ and $\beta^r(x)$ have the same image in $H^r(J^\bullet)$, and so homotopic morphisms define the same morphism on cohomology.

LEMMA A.10 *Let $M \to I^\bullet$ be a resolution of M, and let $N \to J^\bullet$ be an injective resolution N. Any two extensions $\alpha^\bullet$ and $\beta^\bullet$ of morphisms $M \to N$ to $I^\bullet \to J^\bullet$ are homotopic.*

PROOF. Bucur and Deleanu 1968, 7.5. □

This implies the second statement of Proposition A.8, because the family $(F(k^r))$ is a homotopy from $F(\alpha^\bullet)$ to $F(\beta^\bullet)$.

PROPOSITION A.11 *A short exact sequence*

$$0 \to A \to B \to C \to 0$$

in C gives rise to a long exact sequence

$$0 \to F(A) \to F(B) \to F(C) \to R^1F(A) \to \cdots$$
$$\cdots \to R^rF(A) \to R^rF(B) \to R^rF(C) \to \cdots$$

and the association of the long exact sequence to the short exact sequence is functorial.

The second condition means that a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

gives rise to a commutative diagram

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & R^{r-1}F(C) & \longrightarrow & R^rF(A) & \longrightarrow & R^rF(B) & \longrightarrow & R^rF(C) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & R^{r-1}F(C') & \longrightarrow & R^rF(A') & \longrightarrow & R^rF(B') & \longrightarrow & R^rF(C') & \longrightarrow & \cdots \end{array}$$

For the proof of the proposition, see Bucur and Deleanu 1968, 7.6.

REMARK A.12 The right derived functors of F are uniquely characterized (up to a unique isomorphism of functors) by the following three properties:

(a) $R^0F = F$;

(b) $R^rF(I) = 0$ for $r > 0$ when I is injective;

(c) the property in (A.11).

Variants

By reversing the directions of some of the arrows, one obtains variants of some of the above definitions, for example, projective objects, left derived functors, etc.

The Ext groups

Let C be an abelian category.

Let $A \in \mathsf{C}$. If C has enough injectives, then we can define the right derived functors of the left exact functor $\mathrm{Hom}(A, \cdot)$. Denote the rth right derived functor by $\mathrm{Ext}^r(A, \cdot)$. To compute $\mathrm{Ext}^r(A, B)$, we choose an injective resolution $B \to I^\bullet$ of B, and set

$$\mathrm{Ext}^r(A, B) = H^r(\mathrm{Hom}(A, I^\bullet)).$$

Let $B \in \mathsf{C}$. If C has enough projectives, then we can define the right derived functors of the left exact ***contravariant*** functor $\mathrm{Hom}(\cdot, B)$. Denote the rth right derived functor by $\mathrm{Ext}^r(\cdot, B)$. To compute $\mathrm{Ext}^r(A, B)$, we choose a projective resolution $P_\bullet \to A$ of A, and we set

$$\mathrm{Ext}^r(A, B) = H^r(\mathrm{Hom}(P_\bullet, B)).$$

PROPOSITION A.13 *If C has enough injectives and enough projectives, then the two definitions of $\mathrm{Ext}^r(A, B)$ coincide.*

PROOF. We define the Ext^r using projectives, and prove that they have the properties characterizing the right derived functors of $\mathrm{Hom}(A, \cdot)$.

First, certainly $\mathrm{Ext}^0(A, B) = \mathrm{Hom}(A, B)$.

To say that I is injective means that $\mathrm{Hom}(\cdot, I)$ is exact. Therefore $\mathrm{Hom}(P_\bullet, I)$ is exact, and so

$$\mathrm{Ext}^r(A, I) \stackrel{\text{def}}{=} H^r(\mathrm{Hom}(P_\bullet, I)) = 0.$$

Finally, if

$$0 \to B' \to B \to B'' \to 0$$

is exact, then because $P_\bullet \to A$ is a resolution of A by projectives, the sequence of complexes

$$0 \to \mathrm{Hom}(P_\bullet, B') \to \mathrm{Hom}(P_\bullet, B) \to \mathrm{Hom}(P_\bullet, B'') \to 0$$

is exact. By a standard procedure, we get out of this a long exact sequence

$$\cdots \to H^r(\mathrm{Hom}(P_\bullet, B')) \to H^r(\mathrm{Hom}(P_\bullet, B)) \to H^r(\mathrm{Hom}(P_\bullet, B'')) \to \cdots . \qquad \square$$

EXAMPLE A.14 Let G be a group. Then Mod_G has both enough injectives and enough projectives. For every G-module M, $\mathrm{Hom}_G(\mathbb{Z}, M) = M^G$, and so the functors $\mathrm{Hom}(\mathbb{Z}, \cdot)$ and $H^0(G, \cdot)$ agree. Hence, so also do their right derived functors:

$$\mathrm{Ext}^r_G(\mathbb{Z}, M) \simeq H^r(G, M).$$

The last proposition allows us to compute these groups by choosing a projective resolution $P_\bullet \to \mathbb{Z}$ of $\mathbb{Z}$ and setting

$$H^r(G, M) = H^r(\mathrm{Hom}_G(P_\bullet, M)). \tag{25}$$

REMARK A.15 It would shorten the exposition in this chapter a little by adopting the formula (25) as the definition of $H^r(G, M)$. This is the approach taken by Atiyah and Wall (1967), but it is not the natural definition.

References

For the general notion of derived functors, see Chapter 7 of Bucur and Deleanu 1968.

Chapter III

Local Class Field Theory: Cohomology

In this chapter, we develop the cohomological approach to local class field theory. We first prove that there exists a local Artin map (Theorem 3.4). Together with the theorems of Chapter I, §§1–3, this suffices to complete the proofs of the main theorems of local class field theory. For those who skipped the Lubin-Tate theory, we then give a proof of the main theorems that is independent of Chapter I (except for §1).

Throughout this chapter, "local field" means "nonarchimedean local field". As before, K^{al} denotes an algebraic closure of K (or separable algebraic closure in the case that K has characteristic $p \neq 0$), and "extension of K" means "subfield of K^{al} containing K". All cohomology groups will computed using continuous cochains (see II, §4). For a Galois extension of fields L/K (possibly infinite), set

$$H^2(L/K) = H^2(\mathrm{Gal}(L/K), L^\times).$$

For the moment, $H^2(L/K)$ is just a cohomology group, but in the next chapter we shall see that it has an explicit interpretation as the relative Brauer group of L/K.

1 The Cohomology of Unramified Extensions

The cohomology of the units

Let K be a local field.

PROPOSITION 1.1 *Let L/K be a finite unramified extension with Galois group G, and let U_L be the group of units in L. Then*

$$H^r_T(G, U_L) = 0, \quad \text{all } r.$$

PROOF. If π is a prime element of L, then every element of $L^\times$ can be written uniquely in the form $\alpha = u\pi^m$, $u \in U_L$, $m \in \mathbb{Z}$. Thus

$$L^\times = U_L \cdot \pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}. \tag{26}$$

Since L is unramified over K, we can choose $\pi \in K$. Then $\tau\alpha = \tau(u\pi^m) = (\tau u)\pi^m$ for $\tau \in \mathrm{Gal}(L/K)$, and so (26) becomes a decomposition of G-modules when we let

G act trivially on $\pi^{\mathbb{Z}} \simeq \mathbb{Z}$. Therefore, $H^r(G, U_L)$ is a direct summand of $H^r(G, L^\times)$ (see II, 1.25). Since $H^1(G, L^\times) = 0$ by Hilbert's theorem 90 (II, 1.22), this shows that $H^1(G, U_L) = 0$. Because G is cyclic, to complete the proof of the theorem, it suffices (by II, 3.4) to show that $H^0_T(G, U_L) = 0$. This is accomplished by the next proposition. □

PROPOSITION 1.2 *Let L/K be a finite unramified extension. Then the norm map $\mathrm{Nm}_{L/K}: U_L \to U_K$ is surjective.*

We first need some lemmas. Let l and k be the residue fields of L and K. Because L/K is unramified, the action of G on $\mathcal{O}_L$ defines an isomorphism $G \simeq \mathrm{Gal}(l/k)$.

LEMMA 1.3 *For $m > 0$, let $U_L^{(m)} = 1 + \mathfrak{m}_L^m$. Then*

$$U_L/U_L^{(1)} \xrightarrow{\simeq} l^\times$$
$$U_L^{(m)}/U_L^{(m+1)} \xrightarrow{\approx} l$$

as G-modules.

PROOF. Let π be a prime element of K. It remains prime in L, and

$$U_L^{(m)} = \{1 + a\pi^m \mid a \in \mathcal{O}_L\}.$$

The maps

$$u \mapsto u \mod \mathfrak{m}_L: U_L \to l^\times$$
$$1 + a\pi^m \mapsto a \mod \mathfrak{m}_L: U_L^{(m)} \to l$$

induce the required isomorphisms. □

LEMMA 1.4 *For all r, $H^r_T(G, l^\times) = 0$. In particular, the norm map $l^\times \to k^\times$ is surjective.*

PROOF. By Hilbert's Theorem 90 (II, 1.22), $H^1(G, l^\times) = 0$, and because $l^\times$ is finite, its Herbrand quotient $h(l^\times) = 1$ (see II 3.8). Therefore $H^2(G, l^\times) = 0$, and this implies that all the groups are zero (by II, 3.4). □

LEMMA 1.5 *The group $H^r_T(G, l) = 0$ for all r. In particular, the trace map $l \to k$ is surjective.*

PROOF. In (II, 1.24) this is proved for $r > 0$, which implies it for all r (by II, 3.4). □

PROOF (OF PROPOSITION 1.2) There are commutative diagrams ($m > 0$)

$$\begin{array}{ccc} U_L & \longrightarrow & l^\times \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} \\ U_K & \longrightarrow & k^\times \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \longrightarrow & l \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ U_K^{(m)} & \longrightarrow & k. \end{array}$$

Consider $u \in U_K$. Because the norm map $l^\times \to k^\times$ is surjective, there exists a $v_0 \in U_L$ such that $\mathrm{Nm}(v_0)$ and u have the same image in $k^\times$, i.e., such that $u/\mathrm{Nm}(v_0) \in U_K^{(1)}$. Because the trace map $l \to k$ is surjective, there exists a $v_1 \in U_L^{(1)}$ such that $\mathrm{Nm}(v_1) \equiv u/\mathrm{Nm}(v_0) \mod U_K^{(2)}$. Continuing in this fashion, we obtain a sequence of elements $v_0, v_1, v_2, v_3, \ldots, v_i \in U_L^{(i)}$, such that $u/\mathrm{Nm}(v_0 \cdots v_i) \in U_K^{(i+1)}$. Let $v = \lim_{m\to\infty} \prod_{j=0}^m v_j$. Then $u/\mathrm{Nm}(v) \in \bigcap U_K^{(i)} = \{1\}$. □

COROLLARY 1.6 *Let L/K be an infinite unramified extension with Galois group G. Then $H^r(G, U_L) = 0$ for $r > 0$ (continuous cochains).*

PROOF. The field L is a union of finite extensions K' of K, and so (see II, 4.2),

$$H^r(\mathrm{Gal}(L/K), U_L) \simeq \varinjlim_{K'} H^r(\mathrm{Gal}(K'/K), U_{K'}) = 0.$$

□

The invariant map

Let L be an unramified extension of K (possibly infinite), and let $G = \mathrm{Gal}(L/K)$.

As $H^2(G, U_L) = 0 = H^3(G, U_L)$, the cohomology sequence of the short exact sequence

$$0 \to U_L \to L^\times \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \to 0,$$

gives an isomorphism

$$H^2(G, L^\times) \xrightarrow[\simeq]{H^2(\mathrm{ord}_L)} H^2(G, \mathbb{Z}).$$

The groups $H^r(G, \mathbb{Q})$ are torsion for $r > 0$ (see II, 4.3) and uniquely divisible (because $\mathbb{Q}$ is), and hence zero. Therefore the cohomology sequence of the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

(trivial G-actions) gives an isomorphism

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}).$$

Recall that

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z})$$

and that G has a canonical topological generator, namely, the Frobenius element $\sigma = \mathrm{Frob}_{L/K}$. The composite of

$$H^2(L/K) \xrightarrow[\simeq]{\mathrm{ord}_L} H^2(G, \mathbb{Z}) \xleftarrow[\simeq]{\delta} H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}$$

is called the ***invariant map***

$$\mathrm{inv}_{L/K}: H^2(L/K) \to \mathbb{Q}/\mathbb{Z}.$$

Consider a tower of field extensions

$$E \supset L \supset K$$

with both E and L unramified (hence Galois) over K. Then

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Inf}} & & \| \\ H^2(E/K) & \xrightarrow{\mathrm{inv}_{E/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes, because all the maps in the definition of inv are compatible with Inf.

THEOREM 1.7 *There exists a unique isomorphism*

$$\mathrm{inv}_K\colon H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z},$$

with the property that, for every $L \subset K^{\mathrm{un}}$ of finite degree n over K, inv_K induces the isomorphism

$$\mathrm{inv}_{L/K}\colon H^2(L/K) \to \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

PROOF. This is an immediate consequence of the above discussion. □

PROPOSITION 1.8 *Let L be a finite extension of K of degree n, and let K^{un} and L^{un} be the largest unramified extensions of K and L. Then the following diagram commutes:*

$$\begin{array}{ccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\ n\ } & \mathbb{Q}/\mathbb{Z}. \end{array} \tag{27}$$

PROOF. The largest unramified extension of a local field is obtained by adjoining all mth roots of 1 for m not divisible by the residue characteristic. Therefore, $L^{\mathrm{un}} = L \cdot K^{\mathrm{un}}$, and so the map

$$\tau \mapsto \tau|K^{\mathrm{un}}\colon \mathrm{Gal}(L^{\mathrm{un}}/L) \to \mathrm{Gal}(K^{\mathrm{un}}/K)$$

is injective. The map denoted Res in (27) is that defined by the compatible homomorphisms

$$\begin{array}{ccc} \mathrm{Gal}(K^{\mathrm{un}}/K) & \leftarrow & \mathrm{Gal}(L^{\mathrm{un}}/L) \\ K^{\mathrm{un}\times} & \to & L^{\mathrm{un}\times} \end{array}$$

(II, 1.27b).

Let $\Gamma_K = \mathrm{Gal}(K^{\mathrm{un}}/K)$ and $\Gamma_L = \mathrm{Gal}(L^{\mathrm{un}}/L)$, and consider the diagram,

$$\begin{array}{ccccccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow[\simeq]{\mathrm{ord}_K} & H^2(\Gamma_K,\mathbb{Z}) & \xleftarrow[\simeq]{\delta} & H^1(\Gamma_K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle fe} \\ H^2(L^{\mathrm{un}}/L) & \xrightarrow[\simeq]{\mathrm{ord}_L} & H^2(\Gamma_L,\mathbb{Z}) & \xleftarrow[\simeq]{\delta} & H^1(\Gamma_L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Here e is the ramification index for L/K and f is the residue class degree. The first square is obtained from the commutative square

$$\begin{array}{ccc} K^{\mathrm{un}\times} & \xrightarrow{\mathrm{ord}_K} & \mathbb{Z} \\ \downarrow & & \downarrow{\scriptstyle e} \\ L^{\mathrm{un}\times} & \xrightarrow{\mathrm{ord}_L} & \mathbb{Z}. \end{array}$$

The second square expresses the fact that the restriction map commutes with the boundary map. Apart from the factor "e", the third square is

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle g\mapsto g|\Gamma_L} & & \downarrow{\scriptstyle f} \\ \mathrm{Hom}(\Gamma_L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The Frobenius elements σ_K and σ_L are determined by the fact that they induce $x \mapsto x^q$ and $x \mapsto x^{q^f}$ respectively on the residue fields, where $q = |k|$ and $q^f = |l|$, and so $\sigma_L|K^{\text{un}} = \sigma_K^f$. It is now clear that the square commutes, and since $n = ef$, this proves the proposition. □

The local Artin map

Let L be a finite unramified extension of K with Galois group G, and let $n = [L\colon K]$. The ***local fundamental class*** $u_{L/K}$ is the element of $H^2(L/K)$ mapped to the generator $\frac{1}{[L:K]}$ of $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ by the invariant map $\text{inv}_{L/K}\colon H^2(L/K) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. The pair $(G, L^\times)$ satisfies the hypotheses of Tate's theorem (II, 3.11),[1] and so cup-product with the fundamental class $u_{L/K}$ defines an isomorphism

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G, L^\times)$$

for all $r \in \mathbb{Z}$. For $r = -2$, this becomes

$$\begin{array}{ccc} H^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & H^0(G, L^\times) \\ \|_{\text{II, 2.7}} & & \| \\ G & & K^\times/\,\text{Nm}(L^\times). \end{array}$$

We now compute this map explicitly.

A prime element π of K is also a prime element of L, and defines a decomposition

$$L^\times = U_L \cdot \pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}$$

of G-modules. Thus

$$H^r(G, L^\times) \simeq H^r(G, U_L) \oplus H^r(G, \pi^{\mathbb{Z}}).$$

Choose a generator σ of G (e.g., the Frobenius generator), and let

$$f \in H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

be the element such that $f(\sigma^i) = \frac{i}{n} \mod \mathbb{Z}$ for all i. It generates $H^1(G, \mathbb{Q}/\mathbb{Z})$.

From the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and the fact that $H^r(G, \mathbb{Q}) = 0$ for all r, we obtain an isomorphism

$$\delta\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

According to the description of δ in (II, 1.21), to construct δf, we first choose a lifting of f to 1-cochain $\tilde{f}\colon G \to \mathbb{Q}$. We take $\tilde{f}$ to be the map $\sigma^i \mapsto \frac{i}{n}$, where $0 \le i < n-1$. Then

$$d\tilde{f}(\sigma^i, \sigma^j) = \sigma^i \tilde{f}(\sigma^j) - \tilde{f}(\sigma^{i+j}) + \tilde{f}(\sigma^i) = \begin{cases} 0 & \text{if} \quad i + j \le n-1 \\ 1 & \text{if} \quad i + j > n-1. \end{cases}$$

[1] For the condition on H^1, use Hilbert's Theorem 90, and for the condition on H^2, use the invariant map.

When we identify $\mathbb{Z}$ with the subgroup $\pi^{\mathbb{Z}}$ of $L^\times$, we find that the fundamental class $u_{L/K} \in H^2(G, L^\times)$ is represented by the cocycle:

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if} \quad i + j \leq n - 1 \\ \pi & \text{if} \quad i + j > n - 1 \end{cases}$$

From the exact sequences

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

$$0 \to L^\times \to L^\times(\varphi) \to I \to 0$$

(see the proof of II, 3.11) we obtain boundary maps

$$H^{-2}(G, \mathbb{Z}) \to H^{-1}(G, I)$$

$$H^{-1}(G, I) \to H^0(G, L^\times),$$

which are isomorphisms because $\mathbb{Z}[G]$ and $L^\times(\varphi)$ have trivial cohomology. Here $L^\times(\varphi)$ is the splitting module $L^\times \oplus \bigoplus_{\sigma \in G, \sigma \neq 1} \mathbb{Z} x_\sigma$ of φ.

Finally, $H^{-2}(G, \mathbb{Z}) \overset{\text{def}}{=} H_1(G, \mathbb{Z}) \simeq G$ (see II, 2.7).

PROPOSITION 1.9 *Under the composite*

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) & \xrightarrow{\simeq} & H^0(G, L^\times) \\ \| \text{II, 2.7} & & \| \\ G & & K^\times / \operatorname{Nm}(L^\times). \end{array}$$

of the above maps, the Frobenius element $\sigma \in G$ maps to the class of π in $K^\times / \operatorname{Nm}(L^\times)$.

Note that, because all units in K are norms from $L^\times$ (see 1.2), the class of π mod $\operatorname{Nm}(L^\times)$ is independent of the prime element π. On the other hand, the G-module $L^\times(\varphi)$ and the map depend on the choice of the generator σ for G.

PROOF. From the construction of the isomorphism $H^{-2}(G, \mathbb{Z}) \simeq G$, we see that the image of σ under the boundary map $H^{-2}(G, \mathbb{Z}) \to H^{-1}(G, I_G) \subset I_G / I_G^2$ is represented by $\sigma - 1$.

The boundary map $H^{-1}(G, I_G) \to H^0(G, L^\times)$ is that given by the snake lemma from the diagram (we write I for I_G):

$$\begin{array}{ccccccccc} & & & & & & H^{-1}(G, I) & & \\ & & & & & & \downarrow & & \\ & & & & (L^\times)_G & \longrightarrow & L^\times(\varphi)_G & \longrightarrow & (I)_G & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^{\times G} & \longrightarrow & L^\times(\varphi)^G & \longrightarrow & I^G & & & & \\ & & \downarrow & & & & & & & & \\ & & H^0(G, L^\times). & & & & & & & & \end{array}$$

The vertical maps connecting the rows are $\mathrm{Nm}_G = \sum_{i=0}^{n-1} \sigma^i$. The element $(\sigma - 1) + I^2$ is the image of $x_\sigma + I \cdot L^\times(\varphi)$ in $L^\times(\varphi)_G$, and $\mathrm{Nm}_G(x_\sigma + I \cdot L^\times(\varphi))$ is the sum of the elements:

$$\begin{array}{rcl} x_\sigma & = & x_\sigma \\ \sigma x_\sigma & = & x_{\sigma^2} - x_\sigma + \varphi(\sigma,\sigma) \\ \sigma^2 x_\sigma & = & x_{\sigma^3} - x_{\sigma^2} + \varphi(\sigma,\sigma^2) \\ \cdots & & \cdots \\ \sigma^{n-1} x_\sigma & = & \text{`}x_1\text{'} - x_{\sigma^{n-1}} + \varphi(\sigma,\sigma^{n-1}) \end{array} .$$

On summing these, remembering that $\text{`}x_1\text{'} = \varphi(1,1) = 1$ and that $+$ on the factor $L^\times$ of $L(\varphi)$ is actually $\cdot$, we find that

$$\mathrm{Nm}_G(x_\sigma) = \prod_{i=1}^{n-1} \varphi(\sigma,\sigma^i) = \pi.$$

This completes the proof. □

REMARK 1.10 The above proof of Proposition 1.9, using Tate's original definition of the isomorphism $H^r(G,\mathbb{Z}) \to H^{r+2}(G,C)$, is simpler than that found in other references, which uses the description of the map in terms of cup products.

2 The Cohomology of Ramified Extensions

Because of Hilbert's Theorem 90 (II, 1.22), there is an exact sequence

$$0 \to H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(E/K) \xrightarrow{\mathrm{Res}} H^2(E/L)$$

for any tower of Galois extensions $E \supset L \supset K$ (see II, 1.36).

The next theorem extends Theorem 1.7 to ramified extensions.

THEOREM 2.1 *For every local field K, there exists a canonical isomorphism*

$$\mathrm{inv}_K : H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}.$$

Let L be a Galois extension of K of degree $n < \infty$. Then the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \\ & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{28}$$

commutes, and therefore defines an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

The proof will occupy most of the rest of the section.

LEMMA 2.2 *If L/K is Galois of finite degree n, then $H^2(L/K)$ contains a subgroup canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.*

PROOF. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ker}(\mathrm{Res}) & \longrightarrow & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\ 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \end{array}$$

Since the two inflation maps are injective, so also is the first vertical map, but 1.8 shows that the kernel of the restriction map on the top row is canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

To complete the proof of Theorem 2.1, it suffices to prove that the map $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(L/K)$ is an isomorphism. There are two different approaches to proving this. In the next chapter on Brauer groups, we shall show that $H^2(K^{\mathrm{un}}/K) \simeq H^2(K^{\mathrm{al}}/K)$ (every central simple algebra over K is split by an unramified extension; see IV §4), and so the vertical maps in the above diagram are isomorphisms. The second proof, which we now present, shows that $\left|H^2(L/K)\right| \leq n$.

LEMMA 2.3 *Let L be a finite Galois extension of K with Galois group G. Then there exists an open subgroup V of $\mathcal{O}_L$, stable under G, such that $H^r(G, V) = 0$ for all $r > 0$.*

PROOF. Let $\{x_\tau \mid \tau \in G\}$ be a normal basis for L over K (see FT, 5.18). The x_τ have a common denominator d in $\mathcal{O}_K$ (see ANT, 2.6). After replacing each x_τ with $d \cdot x_\tau$, we may suppose that they lie in $\mathcal{O}_L$. Take $V = \sum \mathcal{O}_K x_\tau$. It is stable under G because the normal basis is. Let π be a prime element of $\mathcal{O}_L$. Then $V \supset \pi^m \mathcal{O}_L$ for some $m > 0$, which shows that V is open (it is union of cosets of $\pi^m \mathcal{O}_L$). Finally,

$$V \simeq \mathcal{O}_K[G] \simeq \mathrm{Ind}^G \mathcal{O}_K$$

as G-modules, and so $H^r(G, V) = 0$ for all $r > 0$ (II, 1.12). □

LEMMA 2.4 *Let L, K, and G, be as in the last lemma. Then there exists an open subgroup V of U_L stable under G such that $H^r(G, V) = 0$ for all $r > 0$.*

PROOF. I prove this only for K of characteristic zero.[2] The power series

$$e^x = 1 + x + \cdots + x^n/n! + \cdots$$

converges for $\mathrm{ord}(x) > \mathrm{ord}(p)/(p-1)$ (ANT, 7.29). It defines an isomorphism of an open neighbourhood of 0 in L onto an open neighbourhood of 1 in $L^\times$, with inverse mapping

$$\log(x) = (x-1) - (x-1)^2/2 + (x-1)^3/3 - \cdots .$$

Both maps commute with the actions of G (because G acts continuously). If V' is an open neighbourhood of 0 as in (2.3), then $\pi^M V'$ will have the same properties, and we can take $V = \exp(\pi^M V')$ with M chosen to be sufficiently large that the exponential function is defined and an isomorphism on $\pi^M V'$. □

LEMMA 2.5 *Let L/K be a cyclic extension of degree n; then $h(U_L) = 1$ and $h(L^\times) = n$.*

[2] For a proof of the characteristic p case, see p. 134 of Serre 1967b.

PROOF. Let V be an open subgroup of U_L with $H^r(G,V) = 0$ for all r. Because U_L is compact, the quotient U_L/V is finite, and so $h(U_L) = h(V) = 1$ by II, 3.9. Now $h(L^\times) = h(U_L)\cdot h(\mathbb{Z}) = h(\mathbb{Z})$, and

$$h(\mathbb{Z}) = \left|H_T^0(G,\mathbb{Z})\right| / \left|H^1(G,\mathbb{Z})\right| = \left|H_T^0(G,\mathbb{Z})\right| = |\mathbb{Z}/n\mathbb{Z}| = n. \qquad \square$$

LEMMA 2.6 *Let L be a finite Galois extension of K of order n, then $H^2(L/K)$ has order n.*

PROOF. We know that the order of $H^2(L/K)$ is divisible by n, and that it equals n when L/K is cyclic. We prove the lemma by induction on $[L\colon K]$. Because the group $\mathrm{Gal}(L/K)$ is solvable (ANT, 7.59), there exists a Galois extension K'/K with $L \supsetneq K' \supsetneq K$. From the exact sequence

$$0 \to H^2(K'/K) \to H^2(L/K) \to H^2(L/K')$$

we see that

$$\left|H^2(L/K)\right| \le \left|H^2(K'/K)\right| \cdot \left|H^2(L/K')\right| = n. \qquad \square$$

PROOF (OF THEOREM 2.1) From the diagram in the proof of (2.2) we see that, for every finite Galois extension L of K, the subgroup $H^2(L/K)$ of $H^2(K^{\mathrm{al}}/K)$ is contained in $H^2(K^{\mathrm{un}}/K)$. Since $H^2(K^{\mathrm{al}}/K) = \bigcup H^2(L/K)$, this proves that the inflation map $H^2(K^{\mathrm{un}}/K) \to H^2(K^{\mathrm{al}}/K)$ is an isomorphism. Compose the inverse of this with the invariant map $\mathrm{inv}_K\colon H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ of Theorem 1.7. $\square$

In fact, the diagram in Theorem 2.1 commutes even when L/K is not Galois:

$$\mathrm{inv}_L \circ \mathrm{Res} = [L : K]\,\mathrm{inv}_K\,. \tag{29}$$

(In this setting, we define $H^2(L/K)$ to be the kernel of the restriction map.)

I claim that

$$\mathrm{inv}_K \circ \mathrm{Cor} = \mathrm{inv}_L\,. \tag{30}$$

Because Res is surjective (see diagram (28)), to prove this it suffices to show that

$$\mathrm{inv}_K \circ \mathrm{Cor} \circ \mathrm{Res} = \mathrm{inv}_L \circ \mathrm{Res}\,.$$

But $\mathrm{Cor} \circ \mathrm{Res} = [L : K]$ by (II, 1.30), and so this is the preceding equality (29).

The fundamental class

Let L be a finite Galois extension of K with Galois group G. As in the unramified case, we define the ***fundamental class*** $u_{L/K}$ of L/K to be the element $u_{L/K}$ of $H^2(L/K)$ such that

$$\mathrm{inv}_{L/K}(u_{L/K}) = \frac{1}{[L\colon K]} \bmod \mathbb{Z},$$

or, equivalently, such that

$$\mathrm{inv}_K(u_{L/K}) = \frac{1}{[L : K]} \bmod \mathbb{Z}.$$

LEMMA 2.7 *Let $L \supset E \supset K$ with L/K finite and Galois. Then*

$$\mathrm{Res}(u_{L/K}) = u_{L/E}, \tag{31}$$
$$\mathrm{Cor}(u_{L/E}) = [E:K]u_{L/K}. \tag{32}$$

Moreover, if E/K is also Galois, then

$$\mathrm{Inf}(u_{E/K}) = [L:E]u_{L/K}. \tag{33}$$

PROOF. Consider

$$\begin{array}{ccccc} H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/E) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \\ \simeq\downarrow{\scriptstyle \mathrm{inv}_K} & & \simeq\downarrow{\scriptstyle \mathrm{inv}_E} & & \simeq\downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[E:K]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:E]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

On applying the kernel-cokernel lemma (II, A.2) to the rows (and using that the lemma is functorial), we obtain a commutative diagram,

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(E/K) & \xrightarrow{\mathrm{Inf}} & H^2(L/K) & \xrightarrow{\mathrm{Res}} & H^2(L/E) \\ & & \downarrow{\scriptstyle \mathrm{inv}_{E/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} \\ 0 & \longrightarrow & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{[E:K]} & \frac{1}{[L:E]}\mathbb{Z}/\mathbb{Z}. \end{array}$$

Here $H^2(E/K)$ is defined to be the kernel of $\mathrm{Res}: H^2(K^{\mathrm{al}}/K) \to H^2(K^{\mathrm{al}}/E)$. The equality (31) expresses the fact that the second square commutes. When E/K is Galois, the equality (33) expresses the fact that the first square commutes.

Equality (32) follows from comparing

$$\mathrm{inv}_K(\mathrm{Cor}_{E/K}(u_{L/E})) \overset{(30)}{=} \mathrm{inv}_E(u_{L/E}) = \frac{1}{[L:E]} \bmod \mathbb{Z}$$
$$\mathrm{inv}_K(u_{L/K}) = \frac{1}{[L:K]} \bmod \mathbb{Z}. \qquad \square$$

REMARK 2.8 There are groups $K^\times/\mathrm{Nm}(L^\times)$ and $H^2(L/K)$ attached to every finite extension L/K of local fields. When L/K is cyclic, they are isomorphic, but not otherwise. The first group is always isomorphic to $\mathrm{Gal}(M/K)$, where M is the largest abelian subextension of L/K (see 3.4, 3.5), and the second is always cyclic of order $[L:K]$. Thus, when L/K is abelian but not cyclic, the two groups have the same order but are not isomorphic, and when L/K is not abelian, they have different orders.

3 The Local Artin Map

The pair $(G, L^\times)$ satisfies the hypotheses of Tate's theorem (II, 3.11),and so we have proved the following result.

THEOREM 3.1 *For every finite Galois extension of local fields L/K and $r \in \mathbb{Z}$, the homomorphism*

$$H_T^r(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^{r+2}(\mathrm{Gal}(L/K), L^\times)$$

defined by $x \mapsto x \cup u_{L/K}$ is an isomorphism. When $r = -2$, this becomes an isomorphism

$$G^{\mathrm{ab}} \simeq K^\times / \mathrm{Nm}_{L/K}(L^\times).$$

If $L \supset E \supset K$ with L/K Galois, then the homomorphism in the theorem commutes with both Res and Cor. For example, to prove the statement for Res we must show that

$$\mathrm{Res}(x \cup u_{L/K}) = \mathrm{Res}(x) \cup u_{L/E}$$

for all $x \in H_T^r(\mathrm{Gal}(L/K), L^\times)$. But a standard property of cup-products (II, 1.39c) is that

$$\mathrm{Res}(x \cup u_{L/K}) = \mathrm{Res}(x) \cup \mathrm{Res}(u_{L/K}),$$

and so this follows from (31). The proof for Cor is similar.

If $L \supset E \supset K$ with L/K and E/K Galois and $x \in H^r(\mathrm{Gal}(E/K), E^\times)$ with $r \geq 1$, then

$$\mathrm{Inf}(x \cup u_{E/K}) = [L : E]\,\mathrm{Inf}(x) \cup u_{L/K}.$$

Again, this follows from a standard property of cup-products (1.39e) and the formula (33).

For $r = -2$, the map in the theorem becomes

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\simeq} K^\times / \mathrm{Nm}_{L/K} L^\times.$$

We denote the inverse map by

$$\phi_{L/K} : K^\times / \mathrm{Nm}_{L/K} L^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

and call it the ***local Artin map***, or by $\mathrm{rec}_{L/K}$ and call it the ***local reciprocity map.*** (The second name is more common, but it is hard to see any reciprocity in the map.)

LEMMA 3.2 *Let $L \supset E \supset K$ be local fields with L/K Galois. Then the following diagrams commute:*

$$\begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Nm}_{E/K}} & & \downarrow \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

The unmarked vertical arrows are induced by the inclusions $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$ and $K \subset E$.

PROOF. To be added (the second is not really needed). □

3.3 Let $L \supset E \supset K$ be local fields with both L and E Galois over K. Then the following diagram commutes:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ & {\scriptstyle \phi_{E/K}} \searrow & \downarrow \\ & & \mathrm{Gal}(E/K)^{\mathrm{ab}} \end{array}$$

The unmarked vertical arrow is induced by the surjection $\sigma \mapsto \sigma|E : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(E/K)$.

PROOF. This follows directly from the definition of the local Artin map, using (33).[3] □

In particular, if $L \supset E \supset K$ is a tower of finite abelian extensions of K, then $\phi_{L/K}(a)|E = \phi_{E/K}(a)$ for all $a \in K^\times$, and so we can define $\varphi_K\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ to be the homomorphism such that, for every finite abelian extension L/K, $\phi_K(a)|L = \varphi_{L/K}(a)$.

THEOREM 3.4 *For every local field K, there exists a homomorphism (local Artin map)*

$$\phi_K\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following properties:

(a) *for every prime element π of K, $\phi_K(\pi)|K^{\mathrm{un}} = \mathrm{Frob}_K$;*

(b) *for every finite abelian extension L of K, $\mathrm{Nm}_{L/K}(L^\times)$ is contained in the kernel of $a \mapsto \phi_K(a)|L$, and ϕ_K induces an isomorphism*

$$\phi_{L/K}\colon K^\times/\mathrm{Nm}_{L/K}(L^\times) \to \mathrm{Gal}(L/K).$$

PROOF. Everything is obvious from the above, except (a), which follows from the fact that, for an unramified extension L of K, $\phi_{L/K}$ agrees with that defined in §1, and so we can apply Proposition 1.9. □

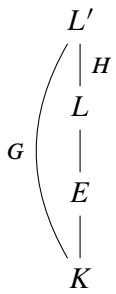
For those who have read §3 of Chapter I, this completes the proof of the main theorems of local class field theory — they can now skip to Chapter V if they wish. Others will need to continue to the end of the chapter.

THEOREM 3.5 (NORM LIMITATION THEOREM) *Let L be a finite extension of K, and let E be the largest abelian extension of K contained in L; then*

$$\mathrm{Nm}_{L/K}(L^\times) = \mathrm{Nm}_{E/K}(E^\times).$$

PROOF. Because of the transitivity of the norm map, $\mathrm{Nm}_{L/K}(L^\times)$ is a subgroup of $\mathrm{Nm}_{E/K}(E^\times)$. If L/K is Galois, then $\mathrm{Gal}(E/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}}$, and so Theorem 3.1 shows that both norm groups have index $[E\colon K]$ in $K^\times$. This implies that they are equal.

In the general case, we let L' be a finite Galois extension of K containing L. Let $G = \mathrm{Gal}(L'/K)$ and $H = \mathrm{Gal}(L'/L)$. Thus:



[3] Hervé Jacquet has pointed out that this doesn't appear to be correct, but that the statement can be proved using Proposition 3.6. I don't know whether it can be proved without using 3.6.

Then E is the largest subfield of L' that is abelian over K and contained in L. Therefore, the subgroup of G fixing it is $G' \cdot H$, where G' is the derived group of G. Let $a \in \mathrm{Nm}(E^\times)$. We have to show that $a \in \mathrm{Nm}(L^\times)$. Consider the commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\phi_{L'/L}} & H/H' \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ K^\times & \xrightarrow{\phi_{L'/K}} & G/G' \\ \| & & \downarrow \\ K^\times & \xrightarrow{\phi_{E/K}} & G/G'H. \end{array}$$

The element $\phi_{L'/K}(a)$ of G/G' maps to 1 in $G/G'H$. As $\phi_{L'/L}$ is surjective, we see from the diagram that there exists a $b \in L^\times$ such $\phi_{L'/K}(a) = \phi_{L'/K}(\mathrm{Nm}(b))$, and hence $a/\mathrm{Nm}(b) \in \mathrm{Nm}(L'^\times)$, say, $a/\mathrm{Nm}(b) = \mathrm{Nm}(c)$. Now

$$a = \mathrm{Nm}_{L/K}(b \cdot \mathrm{Nm}_{L'/L}(c)) \in \mathrm{Nm}_{L/K}(L^\times). \qquad \square$$

Theorem 3.5 shows that there is no hope of classifying nonabelian extensions of a local field in terms of the norm groups.

Alternative description of the local Artin map

Let L/K be a finite abelian extension with Galois group G, and let $u_{L/K} \in H^2(G, L^\times)$ be the fundamental class. The local Artin map $\phi_{L/K}$ is the inverse to the isomorphism

$$x \mapsto x \cup u_{L/K} : H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, L^\times).$$

This definition is difficult to work with because cup-products involving both homology and cohomology groups have no very convenient description. Instead, we re-interprete the map purely in terms of cohomology groups. Consider the cup-product pairing

$$H^0(G, L^\times) \times H^2(G, \mathbb{Z}) \longrightarrow H^2(G, L^\times) \xrightarrow{\mathrm{inv}_{L/K}} \mathbb{Q}/\mathbb{Z}.$$

Given an element $a \in H^0(G, L^\times) = K^\times$ and a class $c \in H^2(G, \mathbb{Z})$ represented by a cocycle $f : G \times G \to \mathbb{Z}$, the cup-product class $a \cup c$ is represented by the cocycle $(\sigma, \tau) \mapsto a^{f(\sigma,\tau)}$. Recall also that we have an isomorphism

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}).$$

PROPOSITION 3.6 *For every $\chi \in \mathrm{Hom}_{cts}(G, \mathbb{Q}/\mathbb{Z})$ and $a \in K^\times$,*

$$\chi(\phi_{L/K}(a)) = \mathrm{inv}_K(a \cup \delta\chi).$$

PROOF. See Serre 1962, "Annexe" to Chapter XI, and Serre 1967a, p. 140. $\square$

Using this, we can get another proof of Proposition 3.4.

LEMMA 3.7 *If L/K is unramified, $\phi_{L/K}$ sends $a \in K^\times$ to $Frob^{\mathrm{ord}_K(a)}$.*

PROOF. Recall that inv_K is defined to be the composite

$$H^2(G, L^\times) \xrightarrow{\text{ord}} H^2(G, \mathbb{Z}) \xleftarrow{\delta} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\chi \mapsto \chi(\sigma)} \mathbb{Q}/\mathbb{Z}.$$

Because of the functoriality of cup-products

$$\mathrm{ord}(a \cup \delta\chi) = \mathrm{ord}(a) \cup \delta\chi, \quad a \in K^\times, \quad \chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

where, on the left ord denotes the map on H^2 induced by $\mathrm{ord}_L\colon L^\times \twoheadrightarrow \mathbb{Z}$, and on the right it is the map itself. Let $a \in H^0(G, L^\times) = K^\times$, and let $m = \mathrm{ord}_L(a)$. For every $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, in the above diagram,

$$a \cup \delta\chi \mapsto \mathrm{ord}(a) \cup \delta\chi \mapsto m\chi \mapsto \chi(\sigma^m), \quad \sigma = \text{Frob},$$

i.e., $\mathrm{inv}_K(a \cup \delta\chi) = \chi(\sigma^m)$. On combining this with the formula in (3.6) we find that

$$\chi(\phi(\alpha)) = \chi(\sigma^{\mathrm{ord}(\alpha)})$$

for all $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, and so $\phi(\alpha) = \sigma^{\mathrm{ord}(\alpha)}$. □

For every character χ of G, we get a character $a \mapsto \mathrm{inv}_K(a \cup \delta\chi)$ of $K^\times$. By duality we get a map $K^\times \to G$. Proposition 3.6 shows that this map is $\phi_{L/K}\colon K^\times \to \mathrm{Gal}(L/K)$.

4 The Hilbert symbol

Since the subgroups of finite index in $K^\times$ intersect in $\{1\}$, the existence theorem implies that the norm groups intersect in 1. The following key result is the starting point in our proof of the existence theorem.

PROPOSITION 4.1 *Let K be a local field containing a primitive nth root of 1. Any element of $K^\times$ that is a norm from every cyclic extension of K of degree dividing n is an nth power.*

This will be a consequence of the theory of the Hilbert symbol.

A VERY SPECIAL CASE

We explain in this subsection how to obtain the proposition in the special case $K = \mathbb{Q}_p$, $n = 2$, by using only elementary results from Serre 1970, Chapter III.

For $a, b \in \mathbb{Q}_p^\times$, define

$$(a, b)_p = \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nontrivial solution in } \mathbb{Q}_p \\ -1 & \text{otherwise.} \end{cases}$$

Clearly, $(a, b)_p$ depends only a and b modulo squares, and so this is a pairing

$$a, b \mapsto (a, b)_p : \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \times \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \{\pm 1\}.$$

Serre shows (ibid. 1.1, 1.2) that this pairing is bi-multiplicative

$$(aa', b)_p = (a, b)_p(a', b)_p, \quad (a, bb')_p = (a, b)_p(a, b')_p,$$

symmetric (which in this case is the same as skew-symmetric)

$$(b,a)_p = (a,b)_p^{-1} = (a,b)_p,$$

and nondegenerate (i.e., the left and right kernels are trivial).

Let a be an element of $\mathbb{Q}_p^\times$ that is not a square. Then

$$\begin{aligned} b \text{ is a norm from } \mathbb{Q}_p[\sqrt{a}] &\iff b = z^2 - ax^2 \text{ has a solution in } \mathbb{Q}_p \\ &\iff z^2 = ax^2 + by^2 \text{ has a nontrivial solution in } \mathbb{Q}_p \\ &\iff (a,b)_p = 1. \end{aligned}$$

Thus,

$$b \text{ is a norm from } \mathbb{Q}_p[\sqrt{a}] \text{ for all } a \implies (a,b)_p = 1 \text{ for all } a \implies b \in \mathbb{Q}_p^{\times 2},$$

by the nondegeneracy of the pairing. This proves the proposition in this case.

ASIDE 4.2 The map $a, b \mapsto (a,b)_p$ is called the ***Hilbert symbol.*** It is defined also for $\mathbb{R}$, and Serre proves ***(Hilbert product formula)***

$$\prod_{p \le \infty} (a,b)_p = 1. \tag{34}$$

The general case

In this subsection, $\mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ denotes the group of *continuous* homomorphisms $G \to \mathbb{Z}/n\mathbb{Z}$.

STEP 1. REVIEW.

Recall that for every cyclic group $\bar{G}$ and $\bar{G}$-module M, there are isomorphisms

$$H_T^r(\bar{G}, M) \to H_T^{r+2}(\bar{G}, M),$$

which become canonical once one chooses a generator σ of $\bar{G}$. More precisely, let $n = (\bar{G} : 1)$ and let χ be the isomorphism $\bar{G} \to \mathbb{Z}/n\mathbb{Z}$ sending σ to 1 mod n. From the cohomology sequence of

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0,$$

we obtain a boundary map $\delta\colon H^1(\bar{G}, \mathbb{Z}/n\mathbb{Z}) \to H^2(\bar{G}, \mathbb{Z})$. The isomorphism

$$H_T^r(\bar{G}, M) \to H_T^{r+2}(\bar{G}, M)$$

is $b \mapsto \delta\chi \cup b$.

Now let K be a field (not necessarily local), and let L/K cyclic extension with Galois group $\bar{G}$ (of order n). When $r = 0$ and $M = L^\times$, the isomorphism becomes

$$b \mapsto \delta\chi \cup b : K^\times / \mathrm{Nm}\, L^\times \to H^2(\bar{G}, L^\times).$$

For $\chi \in \mathrm{Hom}(\bar{G}, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^\times$, define

$$(\chi, b)' = \delta\chi \cup b \in H^2(\bar{G}, L^\times).$$

The above discussion shows that, if χ is an isomorphism $\bar{G} \to \mathbb{Z}/n\mathbb{Z}$, then

$$\boxed{(\chi, b)' = 0 \iff b \text{ is a norm from } L^\times.}$$

STEP 2.

Let K be a field (not necessarily local). If K has characteristic $p \neq 0$, then we require n to be relatively prime to p. Let K^{al} be a separable algebraic closure of K (thus, simply an algebraic closure if K is perfect), and let $G = \mathrm{Gal}(K^{\mathrm{al}}/K)$. Let μ_n be the group of nth roots of 1 in K^{al}, regarded as a G-module. Under our assumption on n, μ_n is a cyclic group of order n.

From the cohomology sequence of

$$0 \longrightarrow \mu_n \longrightarrow K^{\mathrm{al}\times} \xrightarrow{x \mapsto x^n} K^{\mathrm{al}\times} \longrightarrow 0$$

and Hilbert's theorem 90 (II, 1.22) we find that

$$\delta : K^\times/K^{\times n} \xrightarrow{\simeq} H^1(G, \mu_n), \qquad H^2(G, \mu_n) \xrightarrow{\simeq} H^2(G, K^{\mathrm{al}\times})_n.$$

Here $H^2(G, K^{\mathrm{al}\times})_n$ denotes the group of elements in $H^2(G, K^{\mathrm{al}\times})$ killed by n.

Consider the cup-product pairing

$$\begin{array}{ccccc} H^1(G, \mathbb{Z}/n\mathbb{Z}) & \times & H^1(G, \mu_n) & \to & H^2(G, \mu_n) \\ \wr & & \wr & & \wr \\ \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z}) & & K^\times/K^{\times n} & & H^2(G, K^{\mathrm{al}\times})_n. \end{array}$$

For $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^\times/K^{\times n}$, we write (χ, b) for the image of the pair under the above pairing: $(\chi, b) = \chi \cup \delta b$ (as an element of $H^2(G, K^{\mathrm{al}\times})$).

Let $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ and (for simplicity) assume that χ has order n. Let L_χ be the subfield of K^{al} fixed by $\mathrm{Ker}(\chi)$. Thus L_χ is a cyclic extension of K of degree n, and χ induces an isomorphism of its Galois group $\bar{G}$ with $\mathbb{Z}/n\mathbb{Z}$. Let $b \in K^\times$, and let

$$(\chi, b)' = \delta\chi \cup b \in H^2(\bar{G}, L^\times),$$

as in Step 1. Then

$$\mathrm{Inf}((\chi, b)') = (\chi, b).$$

Since the inflation map $H^2(\bar{G}, L_\chi) \to H^2(G, K^{\mathrm{al}\times})$ is injective (see II, 1.36), we deduce that

$$\boxed{(\chi, b) = 0 \iff b \text{ is a norm from } L_\chi^\times.}$$

STEP 3.

Now assume that K is a local field, so that we have a canonical isomorphism

$$\mathrm{inv}_K : H^2(G, K^{\mathrm{al}\times}) \to \mathbb{Q}/\mathbb{Z}.$$

For $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z}) \simeq H^1(G, \mathbb{Z}/n\mathbb{Z})$ and $b \in K^\times/K^{\times n} \simeq H^1(G, \mu_n)$, we now define

$$(\chi, b) = \mathrm{inv}_K(\chi \cup \delta b) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Thus, we have a canonical pairing

$$\chi, b \mapsto (\chi, b) : H^1(G, \mathbb{Z}/n\mathbb{Z}) \times H^1(G, \mu_n) \to H^2(G, \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

PROPOSITION 4.3 *The left kernel of this pairing is zero.*

PROOF. Let $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$; we have to show that if $(\chi, b) = 0$ for all $b \in K^\times/K^{\times n}$, then $\chi = 0$.

Recall that the composite of the local Artin map $\phi_K\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with

$$\tau \mapsto \tau|L\colon \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$$

is surjective for every finite extension L of K contained in K^{ab}. This implies that the image of ϕ_K is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Recall (3.6) that, for $b \in K^\times$,

$$(\chi, b \bmod K^{\times n}) = \chi(\phi_K(b)).$$

Because χ is continuous, if it is zero on $\phi_K(K^\times)$, then it is zero on the whole of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.□

STEP 4.

Now assume that K contains a primitive nth root of 1. Thus, $\mu_n \approx \mathbb{Z}/n\mathbb{Z}$ as a G-module (the isomorphism depends on the choice of a primitive nth root of 1). In particular, $\mu_n \otimes \mu_n \approx \mu_n$, and so $H^2(G, \mu_n \otimes \mu_n) \approx H^2(G, \mu_n)$ (noncanonically). There is a *canonical* isomorphism

$$H^2(G, \mu_n) \otimes \mu_n \xrightarrow{\simeq} H^2(G, \mu_n \otimes \mu_n),$$

which can be defined as $x, y \mapsto x \cup y$. On combining this with the isomorphism $H^2(G, \mu_n) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ given by the invariant map, we obtain an isomorphism

$$H^2(G, \mu_n \otimes \mu_n) \simeq \mu_n.$$

Thus, we have a cup-product pairing

$$\begin{array}{ccccc} H^1(G, \mu_n) & \times & H^1(G, \mu_n) & \to & H^2(G, \mu_n \otimes \mu_n) \\ \wr & & \wr & & \wr \\ K^\times/K^{\times n} & & K^\times/K^{\times n} & & \mu_n. \end{array}$$

For $a, b \in K^\times$, their image in μ_n under this pairing is denoted (a, b). The pairing is called the ***Hilbert symbol***.

THEOREM 4.4 *The Hilbert symbol has the following properties.*

(a) *It is bi-multiplicative, i.e.,*

$$(aa', b) = (a, b)(a', b), \quad (a, bb') = (a, b)(a, b').$$

(b) *It is skew-symmetric, i.e.,*

$$(b, a) = (a, b)^{-1}.$$

(c) *It is nondegenerate, i.e.,*

$$(a, b) = 1 \text{ for all } b \in K^\times/K^{\times n} \implies a \in K^{\times n},$$

$$(a, b) = 1 \text{ for all } a \in K^\times/K^{\times n} \implies b \in K^{\times n}.$$

(d) $(a, b) = 1$ *if and only if* b *is a norm from* $K[\sqrt[n]{a}]$.

PROOF. Statements (a) and (b) are immediate from the definition of the Hilbert symbol in terms of cup-products.

We next prove (c). Choose an nth root of 1, and use it to define isomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ and $\mu_n \to \mu_n \otimes \mu_n$. The diagram defined by these maps,

$$\begin{array}{ccccccc} H^1(G,\mu_n) & \times & H^1(G,\mu_n) & \to & H^2(G,\mu_n\otimes\mu_n) & \simeq & H^2(G,\mu_n)\otimes\mu_n \\ \uparrow & & \| & & \uparrow & & \\ H^1(G,\mathbb{Z}/n\mathbb{Z}) & \times & H^1(G,\mu_n) & \to & H^2(G,\mu_n), & & \end{array}$$

commutes. By Proposition 4.3, the left kernel of the lower pairing is zero. Hence, the left kernel of the upper pairing is also zero, which, by skew-symmetry, implies that the right kernel is zero.

Finally, we prove (d). Assume (for simplicity), that $K[\sqrt[n]{a}]$ has degree n over K. Choose a primitive nth root ζ of 1. Then $K[\sqrt[n]{a}]$ is cyclic of degree n over K, and its Galois group is generated by the map σ sending $\sqrt[n]{a}$ to $\zeta\sqrt[n]{a}$. With this choice of ζ, $a \in K^\times/K^{\times n}$ corresponds to the element of $\chi_a \in \mathrm{Hom}(G,\mathbb{Z}/n\mathbb{Z})$ sending σ to 1 mod $n\mathbb{Z}$. As $K[\sqrt[n]{a}] = L_{\chi_a}$, (d) follows from the boxed formula above. □

PROOF (OF PROPOSITION 4.1) We can deduce Proposition 4.1 from Theorem 4.4 by the same argument as in the case $K = \mathbb{Q}_p$, $n = 2$, namely, if b is a norm from $K[\sqrt[n]{a}]$ for all a, then $(a,b) = 1$ for all a (by 4.4d), and hence $b \in K^{\times n}$ (by 4.4c). □

REMARK 4.5 The Hilbert symbol is related to the local Artin map by the formula

$$\phi_K(b)(a^{\frac{1}{n}}) = (a,b)a^{\frac{1}{n}}.$$

Note that Galois theory tells us that, for every $\tau \in \mathrm{Gal}(K[a^{\frac{1}{n}}]/K)$, $\tau a^{\frac{1}{n}} = \zeta a^{\frac{1}{n}}$ for some nth root of one ζ (remember, we are assuming that K contains the nth roots of 1), and so the point of the formula is that roots of 1 are the same. The proof of the formula is an exercise in cup-products, starting from Proposition 3.6.(a)

REMARK 4.6 The existence theorem will show that ϕ_K defines an isomorphism $K^\times/K^{\times n} \to \mathrm{Gal}(L/K)$, where L/K is the largest abelian extension of K of exponent n (without the existence theorem we know only that the map is surjective). Clearly, $\mathrm{Hom}(G,\mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L/K),\mathbb{Z}/n\mathbb{Z})$, which is the dual of $\mathrm{Gal}(L/K)$. Thus, $K^\times/K^{\times n}$ and $\mathrm{Hom}(G,\mathbb{Z}/n\mathbb{Z})$ have the same order. This shows that the pairing in Step 2,

$$H^1(G,\mathbb{Z}/n\mathbb{Z}) \times H^1(G,\mu_n) \to H^2(G,\mu_n) \simeq \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is nondegenerate. More generally, for every finite G-module M, the cup-product pairing

$$H^r(G,M) \times H^{2-r}(G,\check{M}) \to H^2(G,\mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is nondegenerate — here $\check{M} = \mathrm{Hom}(M,\mu_n)$. This duality theorem was proved by Poitou and Tate in the early 1950s, and was a starting point for the theorems in my book "Arithmetic Duality Theorems". Note that it implies that $H^2(G,\mu_n\otimes\mu_n) \simeq (\mu_n)_G$.

REMARK 4.7 The Hilbert symbol has an interpretation in terms of central simple algebras (see the next chapter). For $a, b \in K^\times$ and ζ a primitive nth root of 1, define $A(a,b;\zeta)$ to be the K-algebra with generators i and j satisfying the relations $i^n = a$, $j^n = b$, and $ij = \zeta ji$. Then, $(a,b)_v$ is the class in $\mathrm{Br}(K)_n$ represented by $A(a,b;\zeta)$. Note that for $n = 2$, we recover the quaternion algebra $H(a,b)$.

REMARK 4.8 The Hilbert symbol

$$(\ ,\ ): K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$$

is defined also for $K = \mathbb{R}$ and $n = 2$. Moreover, the product formula (34) holds for all number fields and all n (see V, 5.4 below).

5 The Existence Theorem

Let K be a local field. Recall that a subgroup N of $K^\times$ is a ***norm group*** if there is a finite abelian extension L/K such that $\mathrm{Nm}_{L/K}(L^\times) = N$. Because $K^\times/N \xrightarrow{\sim} \mathrm{Gal}(L/K)$, such a group N is of finite index in $K^\times$ and hence open (I, 1.3).

THEOREM 5.1 (EXISTENCE THEOREM) *Every open subgroup of finite index in $K^\times$ is a norm group.*

In this draft, I prove this only for K of characteristic zero. Then subgroups of finite index are open, and we can use the theory of the Hilbert symbol.

REMARK 5.2 Before starting the proof of Theorem 5.1, we should consider the abstract situation: Let Z be an infinite abelian group, and let $\mathcal{N}$ be a family of subgroups of finite index; what do we need to know in order to prove that $\mathcal{N}$ contains all subgroups of Z of finite index? Clearly, a start is to know,

(a) if I contains an element of $\mathcal{N}$, then I is in $\mathcal{N}$;

(b) if N_1 and N_2 are in $\mathcal{N}$, then $N_1 \cap N_2$ contains an element of $\mathcal{N}$ (and hence is in $\mathcal{N}$).

We know that the family of norm subgroups of $K^\times$ has these properties (Corollary 1.2), but so also, for example, does the set of subgroups of $\mathbb{Z}$ containing $5\mathbb{Z}$. Clearly, we need to know more. Let D be the intersection of all the groups in $\mathcal{N}$. If every subgroup I of finite index in Z contains an element of $\mathcal{N}$, then it contains D. Conversely, if D is divisible, i.e., $D = nD$ for all integers n, then D is contained in every subgroup of finite index (a subgroup of Z of index n contains nZ, which contains $nD = D$). Therefore, we need that D be divisible, but even this isn't sufficient. For example, let $Z = \mathbb{Z}$ and $\mathcal{N} = \{p^n\mathbb{Z} \mid n \in \mathbb{N}\}$. Then $D = \bigcap p^n\mathbb{Z} = 0$ is divisible, but not every subgroup of finite index in $\mathbb{Z}$ contains an element of $\mathcal{N}$. [Probably I should include a complete list of "axioms" that a family $\mathcal{N}$ should satisfy in order to contain all open subgroups of finite index — see Serre 1962, XI.5, or Artin and Tate 1961, Chapter 14. This may be useful when we come to the global existence theorem.]

Proof of Theorem 5.1

STEP 1. *For all finite extensions L/K, the norm map $L^\times \to K^\times$ has closed image and compact kernel.*

PROOF. Since the image has finite index, it is open (see I, 1.3), and hence closed. The kernel is closed, and the equality

$$\operatorname{ord}_L(\operatorname{Nm}(a)) = [L\colon K]\operatorname{ord}_L(a) = f\cdot\operatorname{ord}_K(a),$$

shows that it contained in U_K, which is compact. □

Let $D_K = \bigcap \operatorname{Nm}_{L/K}(L^\times)$, where L runs over the finite extensions of K (or only the finite abelian extensions — after Theorem 3.5, it is the same).

STEP 2. *For any finite extension K'/K, $\operatorname{Nm}_{K'/K} D_{K'} = D_K$.*

PROOF. Let $a \in D_K$, and consider the sets

$$\operatorname{Nm}_{L/K'} L^\times \cap \operatorname{Nm}^{-1}_{K'/K}(a)$$

for L/K' finite. They are compact and nonempty, and any two contain a third. Therefore their intersection is nonempty (pointset topology). An element in the intersection lies in $D_{K'}$ and has norm a. □

STEP 3. *The group D_K is divisible.*

PROOF. Let $n > 1$ be an integer — we have to show that $nD_K = D_K$. Let $a \in D_K$. For each finite extension L of K containing a primitive nth root of 1, consider the set

$$E(L) = \{b \in K^\times \mid b^n = a, \quad b \in \operatorname{Nm}_{L/K} L^\times\}.$$

It is nonempty: $a = \operatorname{Nm}_{L/K} a'$ for some $a' \in D_L$; according to Proposition 4.1, $a' = c^n$ for some $c \in L$, and

$$\operatorname{Nm}_{L/K}(c)^n = \operatorname{Nm}_{L/K}(a') = a;$$

therefore $b \overset{\text{def}}{=} \operatorname{Nm}_{L/K}(c) \in E(L)$. Moreover, $E(L\cdot L') \subset E(L)\cap E(L')$. Since each set is finite, their intersection is nonempty. An element in their intersection lies in D_K and has nth power a. □

STEP 4. $D_K = \{1\}$. [Actually, we don't use this here.]

PROOF. Choose a prime element of K. Let $V_{m,n} = U^{(m)} \times \pi^{n\mathbb{Z}}$. Then $V_{m,n}$ is an (open) subgroup of finite index in $K^\times$, and therefore contains D_K. Now $D_K \subset \bigcap_{m,n} V_{m,n} = \{1\}$. □

STEP 5. *Every subgroup I of finite index in $K^\times$ that contains U_K is a norm subgroup.*

PROOF. Since $\operatorname{ord}_K\colon K^\times \to \mathbb{Z}$ is surjective with kernel U_K, the subgroups I in question are the subgroups of $K^\times$ of the form $\operatorname{ord}_K^{-1}(n\mathbb{Z})$, $n \geq 1$. Let K_n be the unramified extension of K of degree n. Then $\operatorname{Nm}_{K_n/K}(K_n^\times)$ is a subgroup of $K^\times$ containing U_K (see 1.2) with image $n\mathbb{Z}$ in $\mathbb{Z}$. The statement follows. □

We now prove the theorem. Let $\mathcal{N}$ be the set of norm groups in $K^\times$, so that $D_K = \bigcap_{N\in\mathcal{N}} N$. Let I be a subgroup of $K^\times$ of finite index. Because D_K is divisible, $I \supset D_K$, and so $I \supset \bigcap_{N\in\mathcal{N}} N \supset \bigcap_{N\in\mathcal{N}}(N\cap U_K)$. Therefore the sets $(N\cap U_K)\smallsetminus I$ have empty intersection. As they are compact some finite subfamily has empty intersection, i.e., for

some finite subset $\mathcal{S}$ of $\mathcal{N}$, $I \supset \bigcap_{N\in\mathcal{S}}(N \cap U_K)$. As any two of the sets $N \cap U_K$ contains a third, this implies that $I \supset N \cap U_K$ for some N.

Fix a norm group N such that $N \cap U_K \subset I$. I claim that I contains

$$N \cap (U_K \cdot (N \cap I)).$$

Indeed, every element of the intersection is of the form ab, $a \in U_K$, $b \in N \cap I$, $ab \in N$. The last two statements imply that $a \in N$. Hence $a \in N \cap U_K \subset I$, and so $ab \in I$.

Now $N \cap I$ is of finite index in $K^\times$ because both N and I are and $K^\times/N \cap I$ injects into $(K^\times/N)\times(K^\times/I)$. Hence $U_K\cdot(N\cap I)$ is a subgroup of finite index in $K^\times$ containing U_K, and so is a norm group (Step 5). Now $N\cap(U_K\cdot(N\cap I))$, being the intersection of two norm groups, contains a norm group. Therefore, I contains a norm group, which implies that it is a norm group.

NOTES It follows from Krasner's lemma (ANT, 7.60) that every finite abelian extension of local fields arises by completing a finite abelian extension of global fields. In the 1930s Hasse and F.K. Schmidt[4] were able to deduce the main theorems of local class field theory from those of global class field theory.

From the modern perspective, this seems a strange way to do things. In the 1940s, in his algebraic approach to class field theory Chevalley developed local class field theory directly, and used it in the construction of global class field theory. F. K. Schmidt also showed that local class field theory can be constructed independently of global class field theory.

At that time, there was no good description of the local Artin map, and nor was there an explicit way of constructing the maximal abelian extension of a local field (except for $\mathbb{Q}_p$ of course).

In 1958 Dwork gave an explicit description of the local Artin map, which is reproduced in Serre 1962, but it was not very pleasant.

In 1965 Lubin and Tate introduced the Lubin-Tate formal group laws, and gave an explicit construction of K^{ab} and an explicit description of the local Artin map. However, they made use of the existence of the local Artin map (our Theorem I, 1.1) in their proofs.

In the early 1980s Lubin, Gold, and Rosen independently gave "elementary" proofs that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$. In his book (Iwasawa 1986), Iwasawa develops the whole of local class field theory from the Lubin-Tate perspective, and also gives explicit formulas (due to de Shalit and Wiles) for the Hilbert symbols etc..

Other noncohomological approaches can be found in Hazewinkel 1975, Neukirch 1986, and Fesenko and Vostokov 1993. The disadvantage of the noncohomological approaches is, naturally, that they provide no information about the cohomology groups of local fields, which have important applications to other topics, for example elliptic curves.

For an explicit description of the local Artin map in the case of tame extensions, see Newton, Rachel, Explicit local reciprocity for tame extensions. Math. Proc. Cambridge Philos. Soc. 152 (2012), no. 3, 425–454.

In this chapter, I have largely followed Serre 1962 and Serre 1967a.

[4]H. Hasse, Die Normenresttheorie relative-Abelscher Zahlkörper als Klassenkörper im Kleinen, J. für Mathematik (Crelle) 162 (1930), 145–154.

F. K. Schmidt, Zur Klassenkörpertheorie im Kleinen, ibid. 155–168.

Chapter IV

Brauer Groups

In this chapter, I define the Brauer group of a field, and show that it provides a concrete interpretation of the cohomology group $H^2(K^{\mathrm{al}}/K)$. Besides clarifying the class field theory, Brauer groups have many applications, for example, to the representation theory of finite groups and to the classification of semisimple algebraic groups over nonalgebraically closed fields.

Throughout the chapter, k will be a field, and all vector spaces over k will be finite-dimensional. A ***k-algebra*** is a ring A containing k in its centre and finite dimensional as a k-vector space. We *do not* assume A to be commutative; for example, A could be the ring $M_n(k)$ of $n \times n$ matrices over k. A ***k-subalgebra*** of a k-algebra is a subring containing k. A homomorphism $\varphi\colon A \to B$ of k-algebras is a homomorphism of rings with the property that $\varphi(a) = a$ for all $a \in k$. The ***opposite*** A^{opp} of a k-algebra A is the algebra with the same underlying set and addition, but with multiplication $\cdot$ defined by $\alpha \cdot \beta = \beta\alpha$. Let $e_1, \dots, e_n$ be a basis for A as a k-vector space. Then

$$e_i e_j = \sum_l a_{ij}^l e_l$$

for some $a_{ij}^l \in k$, called the ***structure constants*** of A relative to the basis $(e_i)_i$. Once a basis has been chosen, the algebra A is uniquely determined by its structure constants.

1 Simple Algebras; Semisimple Modules

Semisimple modules

In this section, A is a k-algebra.

By an ***A-module***, we mean a finitely generated left A-module V. In particular, this means that $1v = v$ for all $v \in V$. Such a V is also finite-dimensional when considered as a k-vector space, and so to give an A-module is the same as to give a (finite-dimensional) vector space over k together with a homomorphism of k-algebras $A \to \mathrm{End}_k(V)$, i.e., a ***representation*** of A on V. The module is said to be ***faithful*** if this homomorphism is injective, i.e., if $ax = 0$ for all $x \in V$ implies $a = 0$.

An A-module V is ***simple*** if it is nonzero and contains no proper A-submodule except 0, and it is ***semisimple*** if it is isomorphic to a direct sum of simple A-modules. It is ***indecomposable*** if it can not be written as a direct sum of two nonzero A-modules. Thus a

simple module is semisimple, and an indecomposable module is semisimple if and only if it is simple. [1]

EXAMPLE 1.1 Let $V = k^2$, and let $A = k[\alpha]$ for some $\alpha \in M_2(k)$. The A-submodules of V are the k-subspaces stable under α.

If $\alpha = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, then $\left\{ \begin{pmatrix} * \\ 0 \end{pmatrix} \right\}$ is an A-submodule of V. In fact, it is the only nontrivial submodule, and so V is indecomposable but not semisimple.

If $\alpha = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a \neq b$, then the only lines stable under α are $L_1 \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} * \\ 0 \end{pmatrix} \right\}$ and $L_2 \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 0 \\ * \end{pmatrix} \right\}$. Since $V = L_1 \oplus L_2$ (as an A-module), it is semisimple.

If $\alpha = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, then V again decomposes as the direct sum of two lines, but the decomposition is no longer unique.

Finally, if $A = M_2(k)$, then V is a simple A-module: for every nonzero v in V, $V = M_2(k) \cdot v$.

THEOREM 1.2 *Every A-module V admits a filtration*

$$V = V_0 \supset \cdots \supset V_r = 0$$

whose quotients V_i/V_{i+1} are simple A-modules. If

$$V = W_0 \supset \cdots \supset W_s = 0$$

is a second such filtration, then $r = s$ and there is a permutation σ of $\{0, \dots, r-1\}$ such that $V_i/V_{i+1} \approx W_{\sigma(i)}/W_{\sigma(i)+1}$ for all i.

PROOF. If V is simple, then $V \supset 0$ is such a filtration. Otherwise, V contains a submodule W, $V \neq W \neq 0$, and we can apply the same argument to V/W and to W. This procedure terminates after finitely many steps because V is a finite dimensional k-vector space.

The uniqueness statement can be proved exactly as in the Jordan-Hölder theorem (GT 6.2). □

COROLLARY 1.3 *Suppose that*

$$\begin{aligned} V &\approx V_1 \oplus \cdots \oplus V_r \\ &\approx W_1 \oplus \cdots \oplus W_s \end{aligned}$$

with all the A-modules V_i and W_j simple. Then $r = s$ and there is a permutation σ of $\{1, \dots, r\}$ such that $V_i \approx W_{\sigma(i)}$ for all i.

PROOF. The decompositions define filtrations of the A-module with quotients $\{V_1, \dots, V_r\}$ and $\{W_1, \dots, W_s\}$. □

PROPOSITION 1.4 *Let V be an A-module. If V is a sum of simple submodules (not necessarily direct), say $V = \sum_{i \in I} S_i$, then for any submodule W of V, there is a subset J of I such that*

$$V = W \oplus \bigoplus_{i \in J} S_i.$$

[1] Some authors use "irreducible" and "completely reducible" for "simple" and "semisimple" respectively so, for them "irreducible" implies "completely reducible".

PROOF. Let J be maximal among the subsets of I such that the sum $S_J = \sum_{j\in J} S_j$ is direct and $W \cap S_J = 0$. I claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). To prove this, it suffices to show that every S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals 0 or S_i. In the first case, $W \cap (S_i + S_J) = 0$, because otherwise there exist vectors $w \in W, s_i \in S_i, s_J \in S_J$, such that $w = s_i + s_J \neq 0$; then $s_i = w - s_J \neq 0$, contradicting $S_i \cap (W + S_J) = 0$. Therefore the second case holds, and $S_i \subset W + S_J$. □

COROLLARY 1.5 *The following conditions on an A-module V are equivalent:*

(a) *V is semisimple;*

(b) *V is a sum of simple submodules;*

(c) *every submodule of V has a complement.*

PROOF. Obviously, (a) implies (b), and the proposition shows that (b) implies (c). Assume (c). If V is simple, then it is semisimple. Otherwise it contains a nonzero proper submodule W, which has a complement W', i.e., $V = W \oplus W'$. If W and W' are simple, then V is semisimple. Otherwise, we can continue the argument, which terminates in a finite number of steps because V has finite dimension as a k-vector space. □

COROLLARY 1.6 *Sums, submodules, and quotient modules of semisimple modules are semisimple.*

PROOF. Each is a sum of simple modules: for sums this follows from (1.5); for quotients it follows from (1.4); for submodules it follows from the fact that every submodule has a complement and therefore is also a quotient. □

Every semisimple A-module V can be written as a direct sum

$$V \simeq m_1 S_1 \oplus \cdots \oplus m_r S_r \tag{35}$$

with each S_i simple and no two isomorphic. An A-module is said to be ***isotypic*** (of type the isomorphism class of S) if it isomorphic to a direct sum of copies of a simple module S. The decomposition (35) shows that every semisimple module V is a direct sum of isotypic modules of distinct types, called the ***isotypic components*** of V. The isotypic component of V corresponding to a simple module S is the sum of all simple submodules of V isomorphic to S. From this description, we see that a homomorphism $V \to V'$ of semisimple A-modules maps each isotypic component of V into the isotypic component of V' of the same type.

PROPOSITION 1.7 *Let V be a semisimple A-module. A submodule of V is stable under all endomorphisms of V if and only if it is a sum of isotypic components of V.*

PROOF. Every endomorphism of V preserves its isotypic components, which proves the sufficiency. For the necessity, let W be a submodule of V stable under all endomorphisms of V, and let S be a simple submodule of W. If S' is a submodule of V isomorphic to S, then the endomorphism

$$V \xrightarrow{\text{project}} S \xrightarrow{\approx} S' \hookrightarrow V$$

of V maps W into W, and so $S' \subset W$. Therefore W contains the isotypic component of V of type the isomorphism class of S. □

1.8 Let ${}_AA$ denote A regarded as a left A-module. Right multiplication $x \mapsto xa$ on ${}_AA$ by an element a of A is an A-linear endomorphism of ${}_AA$. Moreover, every A-linear map $\varphi\colon {}_AA \to {}_AA$ is of this form with $a = \varphi(1)$. Thus

$$\varphi \mapsto \varphi(1)\colon \mathrm{End}_A({}_AA) \xrightarrow{\simeq} A \qquad \text{(as } k\text{-vector spaces)}.$$

Let φ_a be the map $x \mapsto xa$. Then

$$(\varphi_a \circ \varphi_b)(1) \overset{\text{def}}{=} \varphi_a(\varphi_b(1)) = \varphi_a(b) = ba = \varphi_{ba}(1),$$

and so

$$\mathrm{End}_A({}_AA) \simeq A^{\mathrm{opp}} \quad \text{(as } k\text{-algebras)}.$$

More generally, if V is a free A-module of rank n, then the choice of a basis for V determines an isomorphism

$$\mathrm{End}_A(V) \to M_n(A^{\mathrm{opp}}).$$

A k-algebra A is said to be ***semisimple*** if every A-module is semisimple. As every A-module is a quotient of a direct sum of copies of ${}_AA$, it suffices to check that the A-module ${}_AA$ is semisimple.

PROPOSITION 1.9 *Let A be a semisimple k-algebra. The isotypic components of the A-module ${}_AA$ are the minimal two-sided ideals of A. Every two-sided ideal of A is a direct sum of minimal two-sided ideals.*

PROOF. The two-sided ideals of A are the submodules of ${}_AA$ stable under right multiplication by the elements of A, i.e., by the endomorphisms of ${}_AA$ (1.8), and so they are the sums of isotypic components of ${}_AA$ (1.7). In particular, the minimal two-sided ideals are exactly the isotypic components of ${}_AA$. The second statement is obvious from the above discussion. □

Simple k-algebras

A k-algebra A is said to be ***simple*** if it contains no proper two-sided ideals other than 0. We shall make frequent use of the following observation:

> The kernel of a homomorphism $f\colon A \to B$ of k-algebras is an ideal in A not containing 1; therefore, if A is simple, then f is injective.

EXAMPLE 1.10 A k-algebra A is said to be a ***division algebra*** if every nonzero element a of A has an inverse, i.e., there exists a b such that $ab = 1 = ba$. Thus a division algebra satisfies all the axioms to be a field except commutativity (and for this reason is sometimes called a ***skew field***). Clearly, a division algebra has no nonzero proper ideals, left, right, or two-sided, and so is simple.

Much of linear algebra does not require that the field be commutative. For example, the usual arguments show that a finitely generated module V over a division algebra D has a basis, and that all bases have the same number n of elements—n is called the dimension of V. In particular, all finitely generated D-modules are free.

EXAMPLE 1.11 Let D be a division algebra over k, and consider the matrix algebra $M_n(D)$. For $A, B \in M_n(D)$, the jth column $(AB)_j$ of AB is AB_j, where B_j is the jth column of B. Therefore, given a matrix B,

$$B_j = 0 \Rightarrow (AB)_j = 0$$
$$B_j \neq 0 \Rightarrow (AB)_j \text{ arbitrary.}$$

It follows that the sets of the form $L(I)$, where I is a subset of $\{1, 2, \dots, n\}$ and $L(I)$ is the set of matrices whose jth columns are zero for $j \notin I$, are left ideals in $M_n(D)$.[2] Moreover, each set $L(\{j\})$ is a minimal ideal in $M_n(k)$. For example, when $n = 4$,

$$L(\{1,3\}) = \left\{ \begin{pmatrix} * & 0 & * & 0 \\ * & 0 & * & 0 \\ * & 0 & * & 0 \\ * & 0 & * & 0 \end{pmatrix} \right\} \text{ and } L(\{3\}) = \left\{ \begin{pmatrix} 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \end{pmatrix} \right\}$$

are, respectively, a left ideal and a minimal left ideal. Similar statements hold for the right ideals. It follows that every nonzero two-sided ideal in $M_n(D)$ is the whole ring, and so $M_n(D)$ is a simple k-algebra.

EXAMPLE 1.12 For $a, b \in k^\times$, let $H(a, b)$ be the k-algebra with basis $1, i, j, ij$ (as a k-vector space) and with the multiplication determined by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Then $H(a, b)$ is a k-algebra, called a ***quaternion algebra*** over k. For example, if $k = \mathbb{R}$, then $H(-1, -1)$ is the usual quaternion algebra. One can show (see Exercise 5.7) that $H(a, b)$ is either a division algebra or it is isomorphic to $M_2(k)$. In particular, it is simple.

Centralizers

Let A be a k-subalgebra of a k-algebra B. The ***centralizer*** of A in B is

$$C_B(A) = \{b \in B \mid ba = ab \text{ for all } a \in A\}.$$

It is again a k-subalgebra of B.

EXAMPLE 1.13 In the following examples, the centralizers are taken in $M_n(k)$.

(a) Let A be the set of scalar matrices in $M_n(k)$, i.e., $A = kI_n$. Clearly $C(A) = M_n(k)$.

(b) Let $A = M_n(k)$. Then $C(A)$ is the centre of $M_n(k)$, which we now compute. Let e_{ij} be the matrix with 1 in the (i, j)th position and zeros elsewhere, so that

$$e_{ij}e_{lm} = \begin{cases} e_{im} & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$

Let $\alpha = (a_{ij}) \in M_n(k)$. Then $\alpha = \sum_{i,j} a_{ij}e_{ij}$, and so $\alpha e_{lm} = \sum_i a_{il}e_{im}$ and $e_{lm}\alpha = \sum_j a_{mj}e_{lj}$. If α is in the centre of $M_n(k)$, then $\alpha e_{lm} = e_{lm}\alpha$, and so $a_{il} = 0$ for $i \neq l$, $a_{mj} = 0$ for $j \neq m$, and $a_{ll} = a_{mm}$. It follows that the centre of $M_n(k)$ is k (identified with the set of scalar matrices).

(c) Let A be the set of diagonal matrices in $M_n(k)$. In this case, $C(A) = A$.

[2] Not all left ideals in $M_n(D)$ are of the form $L(I)$ — for example, imposing a linear relation on the columns defines a left ideal in $M_n(D)$.

Notice that in all three cases, $C(C(A)) = A$.

THEOREM 1.14 (DOUBLE CENTRALIZER THEOREM) *Let A be a k-algebra, and let V be a faithful semisimple A-module. Then $C(C(A)) = A$ (centralizers taken in $\mathrm{End}_k(V)$).*

PROOF. Let $D = C(A)$ and $B = C(D)$. Clearly $A \subset B$, and the reverse inclusion follows from the next lemma when we take $v_1, \dots, v_n$ to generate V as a k-vector space. □

LEMMA 1.15 *For any $v_1, \dots, v_n \in V$ and $b \in B$, there exists an $a \in A$ such that*

$$av_1 = bv_1, \quad av_2 = bv_2, \quad \dots, \quad av_n = bv_n.$$

PROOF. We first prove this for $n = 1$. Note that Av_1 is an A-submodule of V, and so (see 1.5) there exists an A-submodule W of V such that $V = Av_1 \oplus W$. Let $\pi: V \to V$ be the map $(av_1, w) \mapsto (av_1, 0)$ (projection onto Av_1). It is A-linear, hence lies in D, and has the property that $\pi(v) = v$ if and only if $v \in Av_1$. Now

$$\pi(bv_1) = b(\pi v_1) = bv_1,$$

and so $bv_1 \in Av_1$, as required.

We now prove the general case. Let W be the direct sum of n copies of V with A acting diagonally, i.e.,

$$a(v_1, \dots, v_n) = (av_1, \dots, av_n), \quad a \in A, \quad v_i \in V.$$

Then W is again a semisimple A-module (1.6). The centralizer of A in $\mathrm{End}_k(W)$ consists of the matrices $(\gamma_{ij})_{1 \le i,j \le n}$, $\gamma_{ij} \in \mathrm{End}_k(V)$, such that $(\gamma_{ij}\alpha) = (\alpha\gamma_{ij})$ for all $\alpha \in A$, i.e., such that $\gamma_{ij} \in D$. In other words, the centralizer of A in $\mathrm{End}_k(W)$ is $M_n(D)$. An argument as in Example 1.13(b), using the matrices $e_{ij}(\delta)$ with δ in the ijth position and zeros elsewhere, shows that the centralizer of $M_n(D)$ in $\mathrm{End}_k(W)$ consists of the diagonal matrices

$$\begin{pmatrix} \beta & 0 & \cdots & 0 \\ 0 & \beta & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta \end{pmatrix}$$

with $\beta \in B$. We now apply the case $n = 1$ of the lemma to A, W, b, and the vector $(v_1, \dots, v_n)$ to complete the proof. □

Classification of simple k-algebras

LEMMA 1.16 (SCHUR'S LEMMA) *The endomorphism algebra of a simple A-module is a division algebra.*

PROOF. Let γ be an A-linear map $S \to S$. Then $\mathrm{Ker}(\gamma)$ is an A-submodule of S, and so it is either S or 0. In the first case, γ is zero, and in the second it is an isomorphism, i.e., it has an inverse that is also A-linear. □

THEOREM 1.17 *Every simple k-algebra A is isomorphic to $M_n(D)$ for some n and some division k-algebra D.*

PROOF. Choose a simple A-module S, for example, any minimal left ideal of A. Then A acts faithfully on S, because the kernel of $A \to \mathrm{End}_k(S)$ will be a two-sided ideal of A not containing 1, and hence is 0.

Let D be the centralizer of A in the k-algebra $\mathrm{End}_k(S)$ of k-linear maps $S \to S$. According to the double centralizer theorem (1.14), the centralizer of D in $\mathrm{End}_k(S)$ is A, i.e., $A = \mathrm{End}_D(S)$. Schur's lemma implies that D is a division algebra. Therefore, S is a free D-module (1.10), say, $S \approx D^n$, and so $\mathrm{End}_D(S) \approx M_n(D^{\mathrm{opp}})$ (see 1.8). □

Modules over simple k-algebras

Let A be an k-algebra. The submodules of ${}_AA$ are the left ideals in A, and the simple submodules of ${}_AA$ are the minimal left ideals.

PROPOSITION 1.18 *Simple k-algebras are semisimple.*

PROOF. Let A be a simple k-algebra. It suffices to show that the A-module ${}_AA$ is semisimple. After Theorem 1.17, we may assume that $A = M_n(D)$ for some division algebra D. We saw in 1.11 that the sets $L(i)$ are minimal left ideals in $M_n(D)$, and that $M_n(D) = L(1) \oplus \cdots \oplus L(n)$ as an $M_n(D)$-module. This shows that ${}_AA$ is semisimple. □

THEOREM 1.19 *Let A be a semisimple k-algebra. The following conditions on A are equivalent:*

(a) *A is simple;*

(b) *the A-module ${}_AA$ is isotypic;*

(c) *any two simple A-modules are isomorphic.*

PROOF. The equivalence of (a) and (b) follows from Proposition 1.9, and (c) obviously implies (b). Finally (b) implies (c) because, if ${}_AA$ is isotypic, so also is a direct sum of copies of ${}_AA$, and every A-module is a quotient of such a direct sum. □

COROLLARY 1.20 *Let A be a simple k-algebra. Any two minimal left ideals of A are isomorphic as left A-modules, and A is a direct sum of its minimal left ideals.*

PROOF. Minimal left ideals are simple A-modules, and so the first statement follows from (c) of the theorem. The second statement was proved in the proof of 1.18. □

COROLLARY 1.21 *Let A be a simple k-algebra, and let S be a simple A-module. Every A-module is isomorphic to a direct sum of copies of S. Any two A-modules having the same dimension over k are isomorphic.*

PROOF. As A is semisimple, the first assertion follows from (c) of the theorem, and the second assertion follows from the first. □

COROLLARY 1.22 *The integer n in Theorem 1.17 is uniquely determined by A, and D is uniquely determined up to isomorphism.*

PROOF. If $A \approx M_n(D)$, then $D^{\mathrm{opp}} \approx \mathrm{End}_A(S)$ for any simple A-module S, and n is the dimension of S as a D-vector space. Since any two simple A-modules are isomorphic (1.19), this implies the statement. □

2 Definition of the Brauer Group

Tensor products of algebras

Let A and B be k-algebras, and let $A \otimes_k B$ be the tensor product of A and B as k-vector spaces. There is a unique k-bilinear multiplication on $A \otimes_k B$ such that

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb', \quad a, a' \in A, \quad b, b' \in B.$$

When we identify k with $k \cdot (1 \otimes 1) \subset A \otimes_k B$, then $A \otimes_k B$ becomes a k-algebra. If $(e_i)_i$ and $(f_j)_j$ are bases of A and B as k-vector spaces, then $(e_i \otimes f_j)_{i,j}$ is a basis for $A \otimes_k B$, and the structure constants for $A \otimes_k B$ can be obtained from those of A and B by an obvious formula. We shall use that tensor products are commutative in the sense that, for any two k-algebras A and B, the map $a \otimes b \mapsto b \otimes a$ extends to an isomorphism of k-algebras

$$A \otimes_k B \to B \otimes_k A,$$

and that they are associative in the sense that, for any three k-algebras A, B, and C, the map $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$ extends to an isomorphism of k-algebras

$$A \otimes_k (B \otimes_k C) \to (A \otimes_k B) \otimes_k C.$$

EXAMPLE 2.1 For every k-algebra A,

$$A \otimes_k M_n(k) \simeq M_n(A).$$

To see this, note that a ring B containing a subring R in its centre is isomorphic to $M_n(R)$ if and only if it admits a basis $(e_{ij})_{1 \le i,j \le n}$ as a left R-module such that

$$e_{ij}e_{lm} = \begin{cases} e_{im} & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$

If (e_{ij}) is the standard basis for $M_n(k)$, then $(1 \otimes e_{ij})$ is an A-basis for $A \otimes M_n(k)$ with the correct property.

More generally,

$$A \otimes_k M_n(A') \simeq M_n(A \otimes_k A') \tag{36}$$

for any k-algebras A and A'.

EXAMPLE 2.2 For any m, n, $M_m(k) \otimes M_n(k) \simeq M_{mn}(k)$. To see this, note that according to the preceding example, $M_m(k) \otimes_k M_n(k) \simeq M_m(M_n(k))$, and an $m \times m$-matrix whose entries are $n \times n$-matrices is an $mn \times mn$-matrix (delete the inner parentheses). Alternatively, let (e_{ij}) and $(f_{i'j'})$ be standard bases for $M_m(k)$ and $M_n(k)$, and check that $(e_{ij} \otimes f_{i'j'})$ has the correct multiplication properties.

Centralizers in tensor products

The next proposition shows that the centralizer of a tensor product of subalgebras is the tensor product of their centralizers.

PROPOSITION 2.3 *Let A and A' be k-algebras, with subalgebras B and B', and let $C(B)$ and $C(B')$ be the centralizers of B and B' in A and A' respectively. Then the centralizer of $B \otimes_k B'$ in $A \otimes_k A'$ is $C(B) \otimes_k C(B')$, i.e.,*

$$C_{A \otimes_k A'}(B \otimes_k B') = C_A(B) \otimes_k C_{A'}(B').$$

PROOF. Certainly $C(B \otimes_k B') \supset C(B) \otimes_k C(B')$.

Let $(f_i)_i$ be a basis for A' as a k-vector space. Then $(1 \otimes f_i)_i$ is a basis for $A \otimes_k A'$ as an A-module, and so an element α of $A \otimes_k A'$ can be written uniquely in the form $\alpha = \sum_i \alpha_i \otimes f_i$, $\alpha_i \in A$. Let $\beta \in B$. Then α commutes with $\beta \otimes 1$ if and only if $\beta\alpha_i = \alpha_i\beta$ for all i. Therefore, the centralizer of $B \otimes 1$ in $A \otimes A'$ is $C(B) \otimes A'$. Similarly, the centralizer of $1 \otimes B'$ in $C(B) \otimes A'$ is $C(B) \otimes C(B')$.

Certainly, $C(B \otimes B') \subset C(B \otimes 1)$, and so $C(B \otimes B')$ is contained in $C(B) \otimes A'$, and, in fact, is contained in the centralizer of $1 \otimes B'$ in $C(B) \otimes A'$, which is $C(B) \otimes C(B')$. This completes the proof. □

In particular, the centre of the tensor product of two k-algebras is the tensor product of their centres: $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$.

COROLLARY 2.4 *The centre of a simple k-algebra is a field.*

PROOF. Obviously, the centre of a division algebra is a field, but Wedderburn's theorem (1.17) shows that every simple k-algebra is isomorphic to $M_n(D)$ for some division algebra D. Now $M_n(D) \simeq M_n(k) \otimes_k D$, and so $Z(M_n(D)) \simeq k \otimes_k Z(D) \simeq Z(D)$. □

A k-algebra A is said to be ***central*** if its centre is k, and a k-algebra that is both central and simple is said to be ***central simple.*** The corollary shows that every simple k-algebra is central simple over a finite extension of k.

Primordial elements

Before continuing, it will be useful to review a little linear algebra from the second edition of Bourbaki's Algebra.

Let V be a k-vector space, possibly infinite dimensional, and let $(e_i)_{i\in I}$ be a basis for V. Any $v \in V$ can be written uniquely $v = \sum a_i e_i$, and we define

$$J(v) = \{i \in I \mid a_i \neq 0\};$$

it is a finite subset of I, which is empty if and only if $v = 0$.

Let W be a subspace of V. A nonzero element w of W is said to be ***primordial*** (relative to V and the basis $(e_i)_{i\in I}$) if $J(w)$ is minimal among the sets $J(w')$ for w' a nonzero element of W and, in the expression $w = \sum a_i e_i$, at least one $a_i = 1$.

PROPOSITION 2.5 *(a) Let w be a nonzero element of W such that $J(w)$ is minimal, and let w' be a second nonzero element of W. Then $J(w') \subset J(w)$ if and only if $w' = cw$ for some nonzero $c \in k$, in which case $J(w') = J(w)$.*

(b) The set of primordial elements of W spans it.

PROOF. (a) If $w' = cw$, $c \neq 0$, then certainly $J(w') = J(w)$. For the converse, let $w = \sum_{i\in J(w)} a_i e_i$ and $w' = \sum_{i\in J(w')} b_i e_i$ be nonzero elements of W with $J(w') \subset J(w)$. Let $j \in J(w')$. Then $J(w - a_j b_j^{-1} w') \subset J(w) \smallsetminus \{j\}$, and so $w - a_j b_j^{-1} w' = 0$ by the minimality of $J(w)$.

(b) Let $w = \sum_{i\in J(w)} a_i e_i \in W$. We have to show that w lies in the subspace spanned by primordial elements. We may assume that $w \neq 0$. Among the nonzero elements w' of W with $J(w') \subset J(w)$, there is one for which $J(w')$ has the fewest possible elements. Some scalar multiple w_0 of w' will be primordial, say, $w_0 = \sum_{i\in J(w_0)} b_i e_i$ with $b_j = 1$.

Now $w = a_j w_0 + (w - a_j w_0)$ with $w - a_j w_0 \in W$ and $\left|J(w - a_j w_0)\right| < |J(w)|$. If $w - a_j w_0$ is a k-linear combination of primordial elements, so is w; if not, repeat the process. As $|J(w)|$ is finite, it will terminate in a finite number of steps. □

The results (and proofs) of this section do not require k to be commutative, i.e., k can be a division algebra.

Simplicity of tensor products

PROPOSITION 2.6 *The tensor product of two simple k-algebras, at least one of which is central, is again simple.*

PROOF. After 1.17, we may suppose that one of the algebras is $M_n(D)$, where D is a division algebra with centre k. Let A be the second simple k-algebra. In the next lemma, we show that $A \otimes_k D$ is simple. Therefore, $A \otimes_k D \approx M_m(D')$ with D' a division algebra, and so

$$A \otimes_k M_n(D) \simeq M_n(A \otimes_k D) \approx M_n(M_m(D')) \simeq M_{mn}(D'),$$

which is simple. □

LEMMA 2.7 *Let A be a k-algebra, and let D be a division algebra with centre k. Then any two-sided ideal $\mathfrak{A}$ in $A \otimes D$ is generated as a left D-module by $\mathfrak{a} \stackrel{\text{def}}{=} \mathfrak{A} \cap (A \otimes 1)$.*

PROOF. We make $A \otimes_k D$ into a left D-module by the rule,

$$\delta(\alpha \otimes \delta') = \alpha \otimes \delta\delta', \quad \alpha \in A, \quad \delta, \delta' \in D.$$

The ideal $\mathfrak{A}$ of $A \otimes_k D$ is, in particular, a D-submodule of $A \otimes_k D$.

Let (e_i) be a basis for A as a k-vector space. Then $(e_i \otimes 1)$ is a basis for $A \otimes_k D$ as a left D-vector space. Let $\alpha \in \mathfrak{A}$ be primordial with respect to this basis, say

$$\alpha = \sum_{i \in J(\alpha)} \delta_i (e_i \otimes 1) = \sum_{i \in J(\alpha)} e_i \otimes \delta_i .$$

For any nonzero $\delta \in D$, $\alpha\delta \in \mathfrak{A}$, and $\alpha\delta = \sum e_i \otimes \delta_i\delta = \sum_{i \in I} (\delta_i\delta)(e_i \otimes 1)$. In particular, $J(\alpha\delta) = J(\alpha)$, and so $\alpha\delta = \delta'\alpha$ for some $\delta' \in D$ (see 2.5a). As some $\delta_i = 1$, this implies that $\delta = \delta'$, and so each δ_i commutes with every $\delta \in D$. Hence δ_i lies in the centre k of D, and $\alpha \in A \otimes 1$. We have shown that every primordial element of $\mathfrak{A}$ is in $A \otimes 1$, which completes the proof because $\mathfrak{A}$ is generated as a D-module by its primordial elements (see 2.5b). □

COROLLARY 2.8 *The tensor product of two central simple k-algebras is again central simple.*

PROOF. Combine Proposition 2.3 with Proposition 2.6. □

Let A be a central simple algebra over k, and let V denote A regarded as a k-vector space. Then left multiplication makes V into a left A-module, and right multiplication makes it into a right A-module, or, what is the same thing, a left A^{opp}-module. These actions identify A and A^{opp} with commuting subalgebras of $\text{End}_k(V)$. From the universality of the tensor product, we obtain a homomorphism

$$a \otimes a' \mapsto (v \mapsto ava') : A \otimes_k A^{\text{opp}} \to \text{End}_k(V).$$

As $A \otimes_k A^{\mathrm{opp}}$ is simple and the kernel of the homomorphism does not contain 1, it is injective. On counting degrees, we find that

$$[A \otimes_k A^{\mathrm{opp}} : k] = [A : k]^2 = (\dim V)^2 = [\mathrm{End}_k(V) : k],$$

and so the homomorphism is an isomorphism. We have proved the following result.

COROLLARY 2.9 *For a central simple k-algebra A,*

$$A \otimes_k A^{\mathrm{opp}} \simeq \mathrm{End}_k(A) \approx M_n(k), \quad n = [A : k].$$

The Noether-Skolem Theorem

THEOREM 2.10 (SKOLEM, NOETHER) *Let $f, g: A \to B$ be homomorphisms from a k-algebra A to a k-algebra B. If A is simple and B is central simple, then there exists an invertible element $b \in B$ such that $f(a) = b \cdot g(a) \cdot b^{-1}$ for all $a \in A$, i.e., f and g differ by an inner automorphism of B.*

PROOF. If $B = M_n(k) = \mathrm{End}_k(k^n)$, then the homomorphisms define actions of A on k^n—let V_f and V_g denote k^n with the actions defined by f and g. According to (1.21), two A-modules with the same dimension are isomorphic, but an isomorphism $b: V_g \to V_f$ is an element of $M_n(k)$ such that $f(a) \cdot b = b \cdot g(a)$ for all $a \in A$.

In the general case, we consider the homomorphisms

$$f \otimes 1, g \otimes 1: A \otimes_k B^{\mathrm{opp}} \to B \otimes_k B^{\mathrm{opp}}.$$

Because $B \otimes_k B^{\mathrm{opp}}$ is a matrix algebra over k, the first part of the proof shows that there exists a $b \in B \otimes_k B^{\mathrm{opp}}$ such that

$$(f \otimes 1)(a \otimes b') = b \cdot (g \otimes 1)(a \otimes b') \cdot b^{-1}$$

for all $a \in A$, $b' \in B^{\mathrm{opp}}$. On taking $a = 1$ in this equation, we find that $(1 \otimes b') = b \cdot (1 \otimes b') \cdot b^{-1}$ for all $b' \in B^{\mathrm{opp}}$. Therefore (see 2.3), $b \in C_{B \otimes_k B^{\mathrm{opp}}}(k \otimes B^{\mathrm{opp}}) = B \otimes_k k$, i.e., $b = b_0 \otimes 1$ with $b_0 \in B$. On taking $b' = 1$ in the equation, we find that

$$f(a) \otimes 1 = (b_0 \cdot g(a) \cdot b_0^{-1}) \otimes 1$$

for all $a \in A$, and so b_0 is the element sought. □

COROLLARY 2.11 *Let A be a central simple algebra over k, and let B_1 and B_2 be simple k-subalgebras of A. Any isomorphism $f: B_1 \to B_2$ is induced by an inner automorphism of A, i.e., there exists an invertible $a \in A$ such that $f(b) = aba^{-1}$ for all $b \in B_1$.*

PROOF. This is the special case of the theorem in which the two maps are $B_1 \xrightarrow{f} B_2 \hookrightarrow A$ and $B_1 \xrightarrow{\mathrm{id}} B_1 \hookrightarrow A$. □

COROLLARY 2.12 *All automorphisms of a central simple k-algebra are inner.*

For example, the automorphism group of $M_n(k)$ is $\mathrm{PGL}_n(k) \stackrel{\mathrm{def}}{=} \mathrm{GL}_n(k)/k^\times I_n$.

Definition of the Brauer group

Let A and B be central simple algebras over k. We say that A and B are ***similar,*** $A \sim B$, if $A \otimes_k M_n(k) \approx B \otimes_k M_m(k)$ for some m and n. This is an equivalence relation: it is obviously reflexive and symmetric, and 2.2 implies that it is transitive. Define $\mathrm{Br}(k)$ to be the set of similarity classes of central simple algebras over k, and write $[A]$ for the similarity class of A. For classes $[A]$ and $[B]$, define

$$[A][B] = [A \otimes_k B].$$

This is well-defined (i.e., if $A \sim A'$ and $B \sim B'$, then $A \otimes_k B \sim A' \otimes_k B'$), and the associativity and commutativity of tensor products show that it is associative and commutative. For every n, $[M_n(k)]$ is an identity element, and because $A \otimes_k A^{\mathrm{opp}} \approx M_n(k)$ (see 2.9) $[A]$ has $[A^{\mathrm{opp}}]$ as inverse. Therefore $\mathrm{Br}(k)$ is an abelian group, called the ***Brauer group*** of k.

REMARK 2.13 (a) Wedderburn's theorem (1.17, 1.22) shows that every central simple algebra over k is isomorphic to $M_n(D)$ for some central division algebra D and that D is uniquely determined by A (even by the similarity class of A) up to isomorphism. Therefore, each similarity class is represented by a central division algebra, and two central division algebras represent the same similarity class if and only if they are isomorphic.

(b) We should verify[3] that the similarity classes form a set, and not merely a class. For each $n > 0$, consider the families $(a_{ij}^l)_{1\le i,j,l\le n}$, $a_{ij}^l \in k$, that are structure constants for central division algebras over k. Clearly, these families form a set, each family defines a central division algebra over k, and these division algebras contain a set of representatives for the Brauer group of k.

EXAMPLE 2.14 (a) If k is algebraically closed, then $\mathrm{Br}(k) = 0$. To prove this, we have to show that any central division algebra D over k equals k. Let $\alpha \in D$, and let $k[\alpha]$ be the subalgebra of D generated by k and α. Then $k[\alpha]$ is a commutative field of finite degree over k (because it is an integral domain of finite degree over k). Hence $k[\alpha] = k$, and $\alpha \in k$. Since α was arbitrary, this shows that $D = k$.

(b) Frobenius showed that Hamilton's quaternion algebra is the only central division algebra over $\mathbb{R}$. Therefore, the Brauer group of $\mathbb{R}$ is cyclic of order 2, equal to $\{[\mathbb{R}], [\mathbb{H}]\}$ (see §4 below).

(c) Wedderburn showed that all finite division algebras are commutative. Therefore, the Brauer group of a finite field is zero (Theorem 4.1 below).

(d) Hasse showed that the Brauer group of a nonarchimedean local field is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$ (see p. 138 below).

(e) Albert, Brauer, Hasse, and Noether showed that, for a number field K, there is an exact sequence

$$0 \to \mathrm{Br}(K) \to \bigoplus\nolimits_v \mathrm{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0.$$

[3] I once heard Brauer, who normally had a gentle manner, deliver a tirade against "modern" mathematicians who ignored the distinction between sets and classes. As he pointed out, if you ignore the distinction, then you obtain a contradiction (Russell's paradox), and once you have one contradiction in your system, you can prove anything.

The sum is over all the primes of K (including the infinite primes). This statement is of the same depth as that of the main theorems of class field theory (see Chapters VII and VIII).

Extension of the base field

PROPOSITION 2.15 *Let A be a central simple algebra over k, and let K be a field containing k (not necessarily of finite degree over k). Then $A \otimes_k K$ is a central simple algebra over K.*

PROOF. The same argument as in the proof of Proposition 2.3 shows that the centre of $A \otimes_k K$ is $k \otimes_k K = K$ (the argument does not require K to have finite degree over k). Also, the proof of Lemma 2.7 does not use that D is finite-dimensional over k. Therefore, when A is a division algebra, every two-sided ideal in $A \otimes_k K$ is generated as an A-module by its intersection with K, and therefore is 0 or $A \otimes_k K$. In the general case, $A \approx M_n(D)$, and so

$$\begin{aligned} A \otimes_k K \approx M_n(D) \otimes_k K &\simeq (M_n(k) \otimes_k D) \otimes_k K \\ &\simeq M_n(k) \otimes_k (D \otimes_k K) \\ &\simeq M_n(D \otimes_k K) \\ &\simeq M_n(K) \otimes_K (D \otimes_k K) \end{aligned}$$

which is simple. □

COROLLARY 2.16 *For a central simple algebra A over k, $[A : k]$ is a square.*

PROOF. Clearly $[A : k] = [A \otimes_k k^{\mathrm{al}} : k^{\mathrm{al}}]$, and $A \otimes_k k^{\mathrm{al}} \approx M_n(k^{\mathrm{al}})$ for some n. □

Let L be a field containing k (not necessarily of finite degree). Then

$$M_n(k) \otimes L \simeq M_n(L),$$

and

$$(A \otimes_k L) \otimes_L (A' \otimes_k L) = A \otimes_k (L \otimes_L (A' \otimes_k L)) = (A \otimes_k A') \otimes_k L.$$

Therefore the map $A \mapsto A \otimes_k L$ defines a homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(L).$$

We denote the kernel of this homomorphism by $\mathrm{Br}(L/k)$ — it consists of the similarity classes represented by central simple k-algebras A such that the L-algebra $A \otimes_k L$ is a matrix algebra.

A central simple algebra A (or its class in $\mathrm{Br}(k)$) is said to be ***split*** by L, and L is called a ***splitting field*** for A, if $A \otimes_k L$ is a matrix algebra over L. Thus $\mathrm{Br}(L/k)$ consists of the elements of $\mathrm{Br}(k)$ split by L.

PROPOSITION 2.17 *For every field k, $\mathrm{Br}(k) = \bigcup \mathrm{Br}(K/k)$, where K runs over the finite extensions of k contained in some fixed algebraic closure k^{al} of k.*

PROOF. We have to show that every central simple algebra A over k is split by a finite extension of k. We know that $A \otimes_k k^{\mathrm{al}} \approx M_n(k^{\mathrm{al}})$, i.e., that there exists a basis $(e_{ij})_{1 \le i,j \le n}$ for $A \otimes_k k^{\mathrm{al}}$ such that $e_{ij}e_{lm} = \delta_{jl}e_{im}$ for all i, j, l, m. Because $A \otimes_k k^{\mathrm{al}} = \bigcup_{[K:k]<\infty} A \otimes_k K$, the e_{ij} all lie in $A \otimes_k K$ for some K, and it follows that $A \otimes_k K \approx M_n(K)$. □

3 The Brauer Group and Cohomology

For a Galois extension L/k of fields, let $H^2(L/k) = H^2(\mathrm{Gal}(L/k), L^\times)$. We shall show that there is a natural isomorphism $H^2(L/k) \simeq \mathrm{Br}(L/k)$, but first we need to investigate the maximal subfields of a central simple algebra.

Maximal subfields

We need a variant of the double centralizer theorem in which $M_n(k)$ is replaced by a central simple algebra.

THEOREM 3.1 *Let B be a simple k-subalgebra of a central simple k-algebra A. Then the centralizer $C = C(B)$ of B in A is simple, and B is the centralizer of C. Moreover,*

$$[B : k][C : k] = [A : k].$$

PROOF. Let V denote B regarded as a k-vector space. Then B and B^{opp} act on V, by right and left multiplication respectively, and each is the centralizer of the other (see 1.8).

Consider the central simple algebra $A \otimes_k \mathrm{End}_k(V)$. Proposition 2.3 shows that the centralizer of $B \otimes 1$ in this algebra is $C \otimes \mathrm{End}_k(V)$ and that of $1 \otimes B$ is $A \otimes B^{\mathrm{opp}}$. On applying the Noether-Skolem theorem (2.10, 2.11) to the two embeddings $b \mapsto b \otimes 1$ and $b \mapsto 1 \otimes b$ of B into $A \otimes_k \mathrm{End}_k(V)$, we obtain an invertible element u of this k-algebra such that $b \otimes 1 = u(1 \otimes b)u^{-1}$ for all $b \in B$. Clearly then

$$C(B \otimes 1) = u \cdot C(1 \otimes B) \cdot u^{-1}$$

(centralizers in $A \otimes_k \mathrm{End}_k(V)$), which shows that these centralizers are isomorphic. Therefore $C \otimes_k \mathrm{End}_k(V)$ is simple because $A \otimes_k B^{\mathrm{opp}}$ is simple (see 2.6), and this implies that C itself is simple because, for every ideal $\mathfrak{a}$ of C, $\mathfrak{a} \otimes_k \mathrm{End}_k(V)$ is an ideal in $C \otimes_k \mathrm{End}_k(V)$. As $\mathrm{End}_k(V)$ has degree $[B : k]^2$ over k,

$$[C \otimes_k \mathrm{End}(V) : k] = [C : k][B : k]^2,$$

and obviously

$$[A \otimes B^{\mathrm{opp}} : k] = [A : k][B : k].$$

On comparing these equalities, we find that

$$[A : k] = [B : k][C : k].$$

If B' denotes the centralizer of C in A, then $B' \supset B$. But after the above, $[A : k] = [C : k][B' : k]$; so $[B : k] = [B' : k]$ and $B = B'$. □

REMARK 3.2 In the case that $A = \mathrm{End}_k(V)$ for V a k-vector space, Theorem 3.1 follows from Theorem 1.14 because V will be a faithful semisimple B-module. This observation can be used to give an alternative proof of the theorem, because A becomes of this form after a finite extension of the base field (see 2.17).

COROLLARY 3.3 *If in the statement of the theorem, B has centre k, then so also does C, and the canonical homomorphism $B \otimes_k C \to A$ is an isomorphism.*

PROOF. The centres of B and C both equal $B \cap C$, and so B central implies C central. Therefore the k-algebra $B \otimes_k C$ is central simple, which implies that $B \otimes_k C \to A$ is injective. It is surjective because the algebras have the same dimension over k. □

COROLLARY 3.4 *Let A be a central simple algebra over k, and let L be a subfield of A containing k. The following are equivalent:*

(a) *L equals its centralizer in A;*

(b) *$[A : k] = [L : k]^2$;*

(c) *L is a maximal commutative k-subalgebra of A.*

PROOF. (a) $\iff$ (b). Because L is commutative, it is contained in its centralizer $C(L)$, but

$$[A : k] = [L : k][C(L) : k],$$

and so $C(L) = L$ if and only if $[A : k] = [L : k]^2$.

(b) $\implies$ (c). Let L' be a maximal commutative subalgebra containing L. Then $L' \subset C(L)$, and so

$$[A:k] \geq [L:k][L':k] \geq [L:k]^2.$$

Thus (b) implies that $[L':k] = [L:k]$.

(c) $\implies$ (a). If $L \neq C(L)$, then there exists a $\gamma \in C(L) \smallsetminus L$. Now $L[\gamma]$ is a commutative subalgebra of A, contradicting the maximality of L. □

COROLLARY 3.5 *The maximal subfields containing k of a central division k-algebra D are exactly those with degree $\sqrt{[D : k]}$ over k.*

PROOF. Any commutative k-subalgebra of D is an integral domain of finite degree over k, and hence is a field. □

COROLLARY 3.6 *Let A be a central simple algebra over k. A field L of finite degree over k splits A if and only if there exists an algebra B similar to A containing L and such that*

$$[B : k] = [L : k]^2. \tag{37}$$

In particular, every subfield L of A of degree $[A:k]^{1/2}$ over k splits A.

PROOF. Suppose L splits A. Then L also splits A^{opp}, say, $A^{\mathrm{opp}} \otimes_k L = \mathrm{End}_L(V)$. This equality states that $A^{\mathrm{opp}} \otimes_k L$ is the centralizer of L in $\mathrm{End}_k(V)$, and so L is the centralizer of $A^{\mathrm{opp}} \otimes_k L$ in $\mathrm{End}_k(V)$ (see 3.1). Let B be the centralizer of A^{opp} in $\mathrm{End}_k(V)$. I claim that B satisfies the required conditions. Certainly, $B \supset L$, and Corollary 3.3 shows that B is central simple and that $B \otimes_k A^{\mathrm{opp}} \simeq \mathrm{End}_k(V)$. On tensoring both sides with A and using that $A \otimes_k A^{\mathrm{opp}}$ is a matrix algebra, we find that $B \sim A$.

For the converse, it suffices to show that L splits B. Because L is commutative, $L = L^{\mathrm{opp}} \subset B^{\mathrm{opp}}$, and because $[L : k] = \sqrt{[B : k]}$, L is equal to its centralizer in B^{opp}. Therefore the centralizer of $1 \otimes L$ in $B \otimes_k B^{\mathrm{opp}}$ is $B \otimes_k L$. When we identify $B \otimes_k B^{\mathrm{opp}}$ with $\mathrm{End}_k(B)$ (endomorphisms of B as a k-vector space—see 2.9), the centralizer of L becomes identified with $\mathrm{End}_L(B)$ (endomorphisms as an L-vector space). This completes the proof. □

COROLLARY 3.7 *Let D be a central division algebra of degree n^2 over k, and let L be a field of degree n over k. Then L splits D if and only if L can be embedded in D (i.e., there exists a homomorphism of k-algebras $L \to D$).*

PROOF. If L embeds into D, then the last corollary shows that it splits D. Conversely, if L splits D, then there exists a central simple algebra B over k containing L, similar to D, and of degree $[L:k]^2$. But $B \sim D$ implies $B \approx M_m(D)$ for some m (see Remark 2.13a), and the condition on the degrees implies that $m = 1$. □

PROPOSITION 3.8 *Every central division algebra over k contains a maximal subfield separable over k.*

PROOF. Let D be a central division algebra over k, and let L be a subfield that is maximal among the separable subfields of D. If L is not a maximal subfield of D, then its centralizer D' is a central division algebra over L not equal to L (see 3.1). The next lemma shows that D' contains a separable subfield properly containing L, which contradicts the definition of L. □

LEMMA 3.9 *Every central division algebra over k and not equal to it contains a subfield separable over k and not equal to it.*

PROOF. Let D be a central division algebra over k. Choose a basis $(e_i)_{1\le i\le n^2}$ for D with $e_1 = 1$, and let $x = \sum_i a_i e_i$ be an element of D. For every integer m, $x^m = \sum_i P_i(m; a_1, \dots, a_{n^2})e_i$, where the P_i are polynomials in the a_j's with coefficients in k that depend only on the structure constants for D. Therefore, if K is a field containing k and

$$x = \sum a_i(e_i \otimes 1), \quad a_i \in K,$$

is an element of $D \otimes_k K$, then $x^m = \sum_i P_i(m; a_1, \dots a_{n^2})e_i \otimes 1$ with the same polynomials P_i.

When k is perfect we know the lemma, and so we may assume that k has characteristic $p \neq 0$ and is infinite. Suppose that $k[a]$ is purely inseparable over k for every $a \in D$. Then $a^{p^r} \in k$ for some $r > 0$, and one sees easily that there exists an r that works for every element of D. For this particular r and $i \neq 1$, $P_i(p^r; a_1, \dots, a_{n^2}) = 0$ for all $a_1, \dots, a_{n^2} \in k$, which implies that $P_i(p^r; X_1, \dots, X_{n^2})$ is the zero polynomial (see FT, proof of 5.18). Therefore, $a^{p^r} \in k^{\mathrm{al}}$ for every element a of $D \otimes_k k^{\mathrm{al}}$. But $D \otimes_k k^{\mathrm{al}} \approx M_n(k^{\mathrm{al}})$, and so

$$\mathrm{diag}(1, 0, \dots, 0) = \mathrm{diag}(1, 0, \dots, 0)^{p^r} \in k^{\mathrm{al}},$$

which implies that $n = 1$. □

COROLLARY 3.10 *The Brauer group $\mathrm{Br}(k) = \bigcup \mathrm{Br}(L/k)$, where L/k runs over the finite Galois extensions of k contained in a fixed separable algebraic closure of k.*

PROOF. The proposition shows that every element of $\mathrm{Br}(k)$ is split by a finite separable extension, and therefore by a finite Galois extension. □

Central simple algebras and 2-cocycles

Fix a finite Galois extension L of k, and let $G = \mathrm{Gal}(L/k)$. Define $\mathcal{A}(L/k)$ to be the class of central simple algebras A over k containing L and of degree $[A : k] = [L : k]^2$ (hence, L equals its centralizer in A).

Fix an $A \in \mathcal{A}(L/k)$. For every $\sigma \in G$, Corollary 2.11 of the Noether-Skolem theorem shows that there exists an element $e_\sigma \in A$ such that

$$\sigma a = e_\sigma a e_\sigma^{-1} \text{ for all } a \in L. \tag{38}$$

Moreover, e_σ is determined by (38) up to multiplication by an element of $L^\times$, because if f_σ has the same property, then $f_\sigma^{-1} e_\sigma$ centralizes L. Note that (38) can be written as

$$e_\sigma \cdot a = \sigma a \cdot e_\sigma \text{ for all } a \in L, \tag{39}$$

which says that moving e_σ past $a \in L$ replaces it with σa. Clearly $e_\sigma e_\tau$ has the property (38) for $\sigma\tau$, and so

$$e_\sigma e_\tau = \varphi(\sigma, \tau) e_{\sigma\tau} \tag{40}$$

for some $\varphi(\sigma, \tau) \in L^\times$. Note that

$$e_\rho(e_\sigma e_\tau) = e_\rho(\varphi(\sigma, \tau)e_{\sigma\tau}) = \rho\varphi(\sigma, \tau) \cdot \varphi(\rho, \sigma\tau) \cdot e_{\rho\sigma\tau}$$

and

$$(e_\rho e_\sigma)e_\tau = \varphi(\rho, \sigma)e_{\rho\sigma}e_\tau = \varphi(\rho, \sigma)\varphi(\rho\sigma, \tau) \cdot e_{\rho\sigma\tau}.$$

Therefore the associative law implies that φ is a 2-cocycle. It is even a normalized 2-cocycle if we choose $e_1 = 1$. A different choice of e_σ's leads to a cohomologous 2-cocycle, and so we have a well-defined map $A \mapsto \gamma(A)\colon \mathcal{A}(L/k) \to H^2(L/k)$.

THEOREM 3.11 *The map $\gamma\colon \mathcal{A}(L/k) \to H^2(L/k)$ is surjective, and its fibres are the isomorphism classes.*

We first need a lemma.

LEMMA 3.12 *Let $A \in \mathcal{A}(L/k)$, and define e_σ to satisfy (38). Then the set $(e_\sigma)_{\sigma\in G}$ is a basis for A as a left vector space over L.*

PROOF. Note that

$$\dim_L(A) = \frac{\dim_k(A)}{\dim_k(L)} = n,$$

and so it suffices to show that the e_σ are linearly independent. Suppose not, and let $(e_\sigma)_{\sigma\in J}$ be a maximal linearly independent set. If $\tau \notin J$, then

$$e_\tau = \sum a_\sigma e_\sigma$$

for some $a_\sigma \in L$. Let $a \in L$. When we compute $e_\tau a$ in two different ways,

$$e_\tau a = \tau a \cdot e_\tau = \sum_{\sigma\in J} \tau a \cdot a_\sigma e_\sigma,$$

$$e_\tau a = \sum_{\sigma\in J} a_\sigma e_\sigma \cdot a = \sum_{\sigma\in J} a_\sigma \cdot \sigma a \cdot e_\sigma$$

we find that $\tau a \cdot a_\sigma = \sigma a \cdot a_\sigma$ for all $\sigma \in J$. For at least one $\sigma \in J$, $a_\sigma \neq 0$, and then the equation shows that $\tau = \sigma$, contradicting the fact that $\tau \notin J$. Therefore $J = G$. □

Now A is uniquely determined by the following properties: $A \supset L$; $(e_\sigma)_{\sigma\in G}$ is a basis for A as an L-vector space; multiplication in A satisfies the equation (38) and (40).

Let $A' \in \mathcal{A}(L/k)$ and suppose that $\gamma(A) = \gamma(A')$. The condition implies that we can choose bases (e_σ) and (e'_σ) for A and A' satisfying (38) and (40) with the *same* 2-cocycle φ. The map $\sum a_\sigma e_\sigma \mapsto \sum a_\sigma e'_\sigma : A \to A'$ is an isomorphism of k-algebras.

Next suppose that A and A' are isomorphic elements of $\mathcal{A}(L/k)$. The Noether-Skolem theorem allows us to choose the isomorphism $f : A \to A'$ so that $f(L) = L$ and $f|L$ is the identity map. If e_σ satisfies condition (40) for A, then $f(e_\sigma)$ satisfies (40) for A'. With the choices (e_σ) and $(f(e_\sigma))$, A and A' define the same cocycle.

These remarks show that the map $A \mapsto \gamma(A)$ defines a injection

$$\mathcal{A}(L/k)/\approx \to H^2(L/k).$$

To show that the map is surjective, we construct an inverse.

Let $\varphi : G \times G \to L^\times$ be a normalized 2-cocycle. Define $A(\varphi)$ to be the L-vector space with basis $(e_\sigma)_{\sigma\in G}$ endowed with the multiplication given by (38) and (40). Then e_1 is an identity element for multiplication, and the cocycle condition (exactly) shows that

$$e_\rho(e_\sigma e_\tau) = (e_\rho e_\sigma)e_\tau.$$

It follows that $A(\varphi)$ is a k-algebra. We identify L with the subfield Le_1 of $A(\varphi)$.

LEMMA 3.13 *The algebra $A(\varphi)$ is central simple over K.*

PROOF. Let $\alpha = \sum a_\sigma e_\sigma$ centralize L, and let $a \in L$. On comparing $a\alpha = \sum aa_\sigma \cdot e_\sigma$ with $\alpha a = \sum a_\sigma(\sigma a) \cdot e_\sigma$, we find that $a_\sigma = 0$ for $\sigma \neq 1$, and so $\alpha = a_1 e_1 \in L$. Therefore, the centralizer of L in $A(\varphi)$ is L.

Let α lie in the centre of $A(\varphi)$. Then α centralizes L, and so $\alpha \in L$, say $\alpha = ae_1$, $a \in L$. On comparing $e_\sigma \cdot \alpha = (\sigma a)e_\sigma$ with $\alpha \cdot e_\sigma = ae_\sigma$, we see that $\alpha \in k$. Thus $A(\varphi)$ is central.

Let $\mathfrak{A}$ be a two-sided ideal in $A(\varphi)$; in particular, $\mathfrak{A}$ is an L-subspace of $A(\varphi)$. If $\mathfrak{A}$ contains one element e_σ, then (40) shows that it contains all, and so equals $A(\varphi)$. Suppose $\mathfrak{A} \neq 0$, and let $\alpha = \sum a_\sigma e_\sigma$ be a primordial element of $\mathfrak{A}$, with say $a_{\sigma_0} = 1$. If $a_{\sigma_1} \neq 0$, $\sigma_1 \neq \sigma_0$, then for every $a \in L$,

$$(\sigma_1 a) \cdot \alpha - \alpha \cdot a = \sum a_\sigma(\sigma_1 a - \sigma a)e_\sigma \in \mathfrak{A}.$$

If a is chosen so that $\sigma_1 a \neq \sigma_0 a$, then this element is nonzero but has fewer nonzero coefficients than α, contradicting its primordality. Therefore, $\alpha = e_{\sigma_0}$, and we have shown that $\mathfrak{A} = A(\varphi)$. □

Let φ and φ' be cohomologous 2-cocycles, say,

$$a(\sigma) \cdot \sigma a(\tau) \cdot \varphi'(\sigma, \tau) = a(\sigma\tau) \cdot \varphi(\sigma, \tau)$$

for some map $a : G \to L^\times$. One checks immediately that the L-linear map $A(\varphi) \to A(\varphi')$ sending e_σ to $a(\sigma)e'_\sigma$ is an isomorphism of k-algebras. Therefore $\varphi \mapsto A(\varphi)$ defines a map $H^2(L/K) \to \mathcal{A}(L/k)/\approx$, which is clearly inverse to $A \mapsto \gamma(A)$. This completes the proof of Theorem 3.11.

The algebras $A(\varphi)$ are called ***crossed-product algebra.*** Before group cohomology existed, 2-cocycles $\varphi : G \times G \to L^\times$ were called ***factor sets*** (and sometimes still are).

THEOREM 3.14 *For every finite Galois extension L/k, the map $\varphi \mapsto [A(\varphi)]$ defines an isomorphism of abelian groups $H^2(L/k) \to \mathrm{Br}(L/k)$.*

To show that this map is bijective, it suffices (after Theorem 3.11) to show that the map $A \mapsto [A]: \mathcal{A}(L/k)/\approx \to \mathrm{Br}(L/k)$ is bijective.

If A and A' are similar central simple algebras over k, then (see 2.13) there exists a central division algebra D such that $A \sim D \sim A'$, say, $A \approx M_n(D)$, $A' \approx M_{n'}(D)$. But if $[A : k] = [A' : k]$, then $n = n'$, and so $A \approx A'$. This proves that the map $\mathcal{A}(L/k)/\approx \to \mathrm{Br}(L/k)$ is injective, and 3.6 proves that it is surjective.

LEMMA 3.15 *For any two 2-cocycles φ and φ', $A(\varphi + \varphi') \sim A(\varphi) \otimes_k A(\varphi')$.*

PROOF. The proof is a little messy because we have to recognize $A(\varphi) \otimes_k A(\varphi')$, not as a crossed-product algebra, but as matrix algebra over a crossed-product algebra. I merely sketch the proof.[4]

Set $A = A(\varphi)$, $B = A(\varphi')$, and $C = A(\varphi + \varphi')$. Regard A and B as left L-modules (using left multiplication), and define

$$V = A \otimes_L B.$$

Concretely, V is the largest quotient space of $A \otimes_k B$ such that

$$la \otimes_L b = a \otimes_L lb$$

holds for all $a \in A, b \in B, l \in L$.

The k-vector space V has a unique right $A \otimes_k B$-module structure such that

$$(a' \otimes_L b')(a \otimes_k b) = a'a \otimes_L b'b \text{ , all } a', a \in A \text{ , } b', b \in B,$$

and a unique left C-module structure such that

$$(le''_\sigma)(a \otimes_L b) = le_\sigma a \otimes_L e'_\sigma b \text{ , all } l \in L, \sigma \in G, a \in A, b \in B.$$

Here (e_σ), (e'_σ), and (e''_σ) are the standard bases for $A = A(\varphi)$, $B = A(\varphi')$, and $C = A(\varphi + \varphi')$ respectively.

The two actions commute, and so the right action of $A \otimes_k B$ on V defines a homomorphism of k-algebras

$$f: (A \otimes_k B)^{\mathrm{opp}} \to \mathrm{End}_C(V).$$

This homomorphism is injective because $A \otimes_k B$ (and hence its opposite) is simple. Since both $(A \otimes_k B)^{\mathrm{opp}}$ and $\mathrm{End}_C(V)$ have degree n^4 over k, where $n = [L : k]$, f is an isomorphism. As we showed in (1.21), any two modules over a simple ring of the same k-dimension are isomorphic, and it follows that $V \approx C^n$ as a C-module. Hence

$$\mathrm{End}_C(V) \approx \mathrm{End}_C(C^n) = M_n(C^{\mathrm{opp}}),$$

and on composing this isomorphism with f we obtain an isomorphism of k-algebras

$$(A \otimes_k B)^{\mathrm{opp}} \to M_n(C)^{\mathrm{opp}}.$$

The same map can be interpreted as an isomorphism

$$A \otimes_k B \to M_n(C).$$

□

[4] See Blanchard 1972, pp. 94–95, or Farb and Dennis 1993, p. 126–128, for the details.

COROLLARY 3.16 *For every separable algebraic closure k^{al} of k, there is a canonical isomorphism $\mathrm{Br}(k) \to H^2(k^{\mathrm{al}}/k)$.*

PROOF. For every tower of fields $E \supset L \supset k$ with E and L finite and Galois over k, the diagram

$$\begin{array}{ccc} H^2(L/k) & \xrightarrow{\mathrm{Inf}} & H^2(E/k) \\ \downarrow & & \downarrow \\ \mathrm{Br}(L/k) & \hookrightarrow & \mathrm{Br}(E/k) \end{array}$$

commutes (the vertical maps send φ to $[A(\varphi)]$).[5] Now use that

$$\begin{aligned} \mathrm{Br}(k) &= \bigcup \mathrm{Br}(L/k) \qquad (3.10), \\ H^2(k^{\mathrm{al}}/k) &= \bigcup H^2(L/k), \end{aligned}$$

where both unions run over the finite Galois extensions L of k contained in k^{al}. □

COROLLARY 3.17 *For every field k, $\mathrm{Br}(k)$ is torsion, and for every finite extension L/k, $\mathrm{Br}(L/k)$ is killed by $[L : k]$.*

PROOF. The same statements are true for the cohomology groups. □

4 The Brauer Groups of Special Fields

The results of the last section allow us to interpret some of the results of Chapter III as statements concerning the Brauer group of a field. In this section, we shall derive the same results independently of Chapter III (but not quite of Chapter II).

Finite fields

Let k be a finite field. We saw in III, 1.4 that, for every finite extension L of k, $H^2(L/k) = 0$, and hence $\mathrm{Br}(k) = 0$. The following is a more direct proof of this fact.

THEOREM 4.1 (WEDDERBURN) *Every finite division algebra is commutative.*

PROOF. Let D be a finite division algebra with centre k, and let $[D : k] = n^2$. Every element of D is contained in a subfield $k[\alpha]$ of D, and hence in a maximal subfield. Every maximal subfield of D has q^n elements. They are therefore isomorphic, and hence conjugate (Noether-Skolem). Therefore, for every maximal subfield L, $D^\times = \bigcup \alpha L^\times \alpha^{-1}$, but a finite group can not equal the union of the conjugates of a proper subgroup (because the union has too few elements), and so $D = L$. □

[5] Should add a proof that the diagram commutes.

The real numbers

Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. Then

$$H^2(\mathbb{C}/\mathbb{R}) \simeq H_T^0(G, \mathbb{C}^\times) = \mathbb{R}^\times / \mathrm{Nm}_G(\mathbb{C}^\times) = \{\pm\},$$

and so $\mathrm{Br}(\mathbb{C}/\mathbb{R})$ is a cyclic group of order 2. The nonzero element of $H^2(\mathbb{C}/\mathbb{R})$ is represented by the 2-cocycle $\varphi: G \times G \to \mathbb{C}^\times$,

$$\varphi(\rho, \tau) = \begin{cases} -1 & \text{if } \rho = \sigma = \tau \\ 1 & \text{otherwise} \end{cases}.$$

Let $\mathbb{H}$ be the usual quaternion algebra over $\mathbb{R}$. Then the $\mathbb{C}$-linear map $A(\varphi) \to \mathbb{H}$ sending x_σ to j is an isomorphism of $\mathbb{R}$-algebras. It follows that every central simple algebra over $\mathbb{R}$ is isomorphic either to a matrix algebra over $\mathbb{R}$ or to a matrix algebra over $\mathbb{H}$.

A nonarchimedean local field

Let K be a nonarchimedean local field. In Chapter III, Theorem 2.1, we defined an isomorphism $H^2(K^{\mathrm{al}}/K) \simeq \mathbb{Q}/\mathbb{Z}$, and hence an isomorphism $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$. In this subsection, we explain how to construct this isomorphism more directly.

Let D be a central division algebra over K, and let $n^2 = [D : K]$. For every subfield L of D containing K, the absolute value $|\cdot|$ has a unique extension to L. Since every element α of D is contained in such a subfield of D, for example, in $K[\alpha]$, the absolute value $|\cdot|$ has a unique extension to D. It is possible to verify that $|\cdot|$ is a nonarchimedean absolute value on D in the obvious sense, i.e.,

(a) $|\alpha| = 0 \iff \alpha = 0$;

(b) for all $\alpha, \beta \in D$, $|\alpha\beta| = |\alpha||\beta|$;

(c) for all $\alpha, \beta \in D$, $|\alpha + \beta| \le \max\{|\alpha|, |\beta|\}$.

Let q be the number of elements in the residue field k of K, and define $\mathrm{ord}(\alpha)$ for $\alpha \in D$ by the formula:

$$|\alpha| = (1/q)^{\mathrm{ord}(\alpha)}.$$

Then ord extends the additive valuation ord_K on K (normalized to map $K^\times$ onto $\mathbb{Z}$) to D. For any subfield L of D containing K, $[L : K] \le n$, and so $\mathrm{ord}(L^\times) \subset n^{-1}\mathbb{Z}$. Hence also $\mathrm{ord}(D^\times) \subset n^{-1}\mathbb{Z}$.

Let

$$\mathcal{O}_D = \{\alpha \in D \mid \mathrm{ord}(\alpha) \ge 0\}$$

$$\mathfrak{P} = \{\alpha \in D \mid \mathrm{ord}(\alpha) > 0\}.$$

Then $\mathcal{O}_D$ is a subring in D, called the ***ring of integers.*** For every subfield L of D containing K, $\mathcal{O}_D \cap L = \mathcal{O}_L$, and so $\mathcal{O}_D$ consists precisely of the elements of D that are integral over $\mathcal{O}_K$. Moreover $\mathfrak{P}$ is a maximal 2-sided ideal in $\mathcal{O}_D$ (obviously), and the powers of it are the only 2-sided ideals in D (the proof is the same as in the commutative case). Hence $\mathfrak{P}^e = \mathfrak{p}\mathcal{O}_D$ for some e. Then $\mathrm{ord}(D^\times) = e^{-1}\mathbb{Z}$, and therefore $e \le n$.

Clearly, the elements of $\mathcal{O}_D$ not in $\mathfrak{P}$ are units. Therefore $d \overset{\text{def}}{=} \mathcal{O}_D/\mathfrak{P}$ is again a division algebra, and hence a field (4.1). Let f be its degree over k. Write $d = k[a]$. We can lift a to an element α of $\mathcal{O}_D$. Because $[K[\alpha] : K] \le n$, we have $f \le n$.

The same argument as in the commutative case shows that $n^2 = ef$, namely, $\mathcal{O}_D$ is a free $\mathcal{O}_K$-module of some rank m. Because $\mathcal{O}_D \otimes_{\mathcal{O}_K} K = D$, $m = n^2$. Moreover, because $\mathcal{O}_D \otimes_{\mathcal{O}_K} k = \mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$, it also is free of dimension of n^2 over k. Now consider the filtration of k-vector spaces

$$\mathcal{O}_D \supset \mathfrak{P} \supset \mathfrak{P}^2 \supset \cdots \supset \mathfrak{P}^e = \mathfrak{p}\mathcal{O}_D.$$

From our definition of f, $\mathcal{O}_D/\mathfrak{P} = d$ has dimension f as a k-vector space, and the successive quotients are one-dimensional vector spaces over d. Hence $\mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$ has dimension ef over k, and so $ef = n^2$.

Because $e \le n$, $f \le n$, the equality $ef = n^2$ implies that $e = f = n$. In particular, every central division algebra $\neq K$ is ramified. Again write $d = k[a]$, and lift a to an element $\alpha \in D$. Then $K[\alpha]$ is a field with residue field d, and so $[K[\alpha] : K] \ge [d : k] = n$. Therefore $K[\alpha]$ has degree n over K and is unramified. It is a maximal subfield, and hence splits D. We have shown that every element of $\mathrm{Br}(K)$ is split by an unramified extension, i.e., $\mathrm{Br}(K)$ is equal to its subgroup $\mathrm{Br}(K^{\mathrm{un}}/K)$.

We next define the map

$$\mathrm{inv}_K\colon \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

An element of $\mathrm{Br}(K)$ is represented by a central division algebra D over K (unique up to isomorphism). According to what we have just proved, there is a maximal subfield L of D that is unramified over K. Let σ be the Frobenius automorphism of L. According to the Noether-Skolem theorem, there is an element $\alpha \in D$ such that $\sigma x = \alpha x \alpha^{-1}$ for all $x \in L$. If α' also has this property, then $\alpha' = c\alpha$ for some $c \in L$, and so

$$\mathrm{ord}(\alpha') = \mathrm{ord}(c) + \mathrm{ord}(\alpha) \equiv \mathrm{ord}(\alpha) \mod \mathbb{Z}.$$

We define

$$\mathrm{inv}_K(D) = \mathrm{ord}(\alpha) \mod \mathbb{Z}.$$

It depends only on the isomorphism class of D.

EXAMPLE 4.2 Let L be the unramified extension of K of degree n, and let σ be the Frobenius automorphism of L/K, so that $G \overset{\text{def}}{=} \mathrm{Gal}(L/K) = \{\sigma^i \mid 0 \le i \le n-1\}$. Let φ be the 2-cocycle

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if} \quad i + j \le n-1 \\ \pi & \text{if} \quad i + j > n-1, \end{cases}$$

where π is a prime element of K (see the discussion preceding III 1.9). The crossed-product algebra $A(\varphi)$ equals $\bigoplus_{0 \le i \le n-1} Le_i$ with the multiplication determined by

$$e_i \cdot a = \sigma^i a \cdot e_i \text{ all } a \in L,$$

and

$$e_i e_j = \begin{cases} e_{i+j} & \text{if} \quad i + j \le n-1 \\ \pi e_{i+j-n} & \text{if} \quad i + j > n-1, \end{cases}$$

We identify L with a subfield of $A(\varphi)$ by identifying e_0 with 1. Because $e_1 a e_1^{-1} = \sigma a$ for $a \in L$, we can use e_1 to compute the invariant of $A(\varphi)$. According to the above rules, $e_1^n = e_{n-1}e_1 = \pi e_0 = \pi$. Hence

$$\mathrm{inv}_K(A(\varphi)) = \mathrm{ord}(e_1) = \tfrac{1}{n}\,\mathrm{ord}(e_1^n) = \tfrac{1}{n}\,\mathrm{ord}(\pi) = \tfrac{1}{n},$$

as expected.

PROPOSITION 4.3 *The map* $\mathrm{inv}_K\colon \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ *just defined is a bijection.*

PROOF. Let L be the unramified extension of K of degree n (contained in a fixed algebraic closure K^{al} of K), and let l/k be the corresponding extension of residue fields. Because the norm maps $l \to k$, $l^\times \to k^\times$ are surjective, and U_L has a filtration whose quotients are $l^\times$ or l one finds that the norm map $U_L \to U_K$ is surjective (see III, 1.2). Therefore, $H^0_T(G, U_L) = 0$, and (because the cohomology of cyclic groups is periodic) this implies that $H^2(G, U_L) = 0$. As $L^\times = U_L \times \pi^{\mathbb{Z}}$ for any prime element π of K,

$$H^2(L/K) = H^2(G, \pi^{\mathbb{Z}}).$$

Consideration of the cohomology sequence of

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

shows that $H^2(G, \pi^{\mathbb{Z}})$ is cyclic of order n and is generated by the class of the cocycle φ considered in the last example (see the discussion preceding III, 1.9). Therefore, $\mathrm{Br}(L/K)$ is cyclic of order n, and it is generated by $[A(\varphi)]$. It now follows that $\mathrm{inv}_K\colon \mathrm{Br}(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ is an isomorphism, and we saw above that $\mathrm{Br}(K^{\mathrm{un}}/K) = \mathrm{Br}(K^{\mathrm{al}}/K)$. □

REMARK 4.4 (a) The calculation in Example 4.2 shows that the invariant map defined in this chapter agrees with that in the preceding chapter using cohomology. In particular, this shows that the map defined here is a homomorphism.

(b) A calculation as in Example 4.2 shows that $\mathrm{inv}_K(A(\varphi^i) = \frac{i}{n} \mod \mathbb{Z}$. I claim that if i is relatively prime to n, then $A(\varphi^i)$ is a central division algebra. If not, then $A(\varphi^i) \sim M_r(D)$ for a central division algebra D of degree m^2 some $m < n$, and $\mathrm{inv}_K(A(\varphi^i)) = \mathrm{inv}_K(D) \in \frac{1}{m}\mathbb{Z}/\mathbb{Z}$, which is a contradiction. It follows that each central division algebra over K is isomorphic to exactly one division algebra of the form $A(\varphi^i)$ for some $n \geq 1$ and some i relatively prime to n. In particular, for a central division algebra D, the order of $[D]$ in $\mathrm{Br}(K)$ is $\sqrt{[D : K]}$.

(c) Let D be a central division algebra of degree n^2 over K. Because the map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ multiplies the invariant by $[L : K]$ (see III, 2.1), D is split by every extension L of K of degree n. Therefore every such L can be embedded into D (by 3.7). In other words, *every* irreducible polynomial in $K[X]$ of degree n has a root in D!

NOTES The results for finite fields, the real numbers, and nonarchmidean local fields are due respectively to Wedderburn, Frobenius, and Hasse. The calculation of the Brauer group of a nonarchimedean local field is essentially the original (pre-cohomological) proof of Hasse.

5 Complements

Semisimple algebras

Recall that a k-algebra A is semisimple if every A-module is semisimple. Simple k-algebras are semisimple (1.18) and Maschke's theorem (GT, 7.4) shows that the group algebra $k[G]$ is semisimple when the order of G is not divisible by the characteristic of k.

EXAMPLE 5.1 Let A be a finite product of simple k-algebras. Every minimal left ideal of a simple factor of A is a simple A-submodule of ${}_AA$. Therefore, ${}_AA$ is a sum of simple A-modules, and so is semisimple. Since every A-module is a quotient of a direct sum of copies of ${}_AA$, this shows that A is semisimple.

Before stating the main result of this section, we recall some elementary module theory.

5.2 Let A be an k-algebra, and consider modules

$$M = M_1 \oplus \cdots \oplus M_n$$
$$N = N_1 \oplus \cdots \oplus N_m.$$

Let α be an A-linear map $M \to N$. For $x_j \in M_j$, let

$$\alpha(0, \dots, 0, x_j, 0, \dots, 0) = (y_1, \dots, y_m).$$

Then $x_j \mapsto y_i$ is an A-linear map $M_j \to N_i$, which we denote α_{ij}. Thus, α defines an $m \times n$ matrix whose ijth coefficient is an A-linear map $M_j \to N_i$. Conversely, every such matrix (α_{ij}) defines an A-linear map $M \to N$, namely,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1j} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{i1} & \cdots & \alpha_{ij} & \cdots & \alpha_{jn} \\ \vdots & & \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mj} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} \alpha_{11}(x_1) + \cdots + \alpha_{1n}(x_n) \\ \vdots \\ \alpha_{i1}(x_1) + \cdots + \alpha_{in}(x_n) \\ \vdots \\ \alpha_{m1}(x_1) + \cdots + \alpha_{mn}(x_n) \end{pmatrix}.$$

Thus, we see

$$\operatorname{Hom}_A(M, N) \simeq \big(\operatorname{Hom}_A(M_j, N_i)\big)_{1 \le j \le n,\ 1 \le i \le m} \tag{41}$$

(isomorphism of k-vector spaces). When $M = N$, this becomes an isomorphism of k-algebras. For example, if M is a direct sum of m copies of M_0, then

$$\operatorname{End}_A(M) \simeq M_m(\operatorname{End}_A(M_0)) \tag{42}$$

($m \times m$ matrices with coefficients in the ring $\operatorname{End}_A(M_0)$).

THEOREM 5.3 *Let V be a finite-dimensional k-vector space and A a k-subalgebra of $\operatorname{End}_k(V)$. If V is semisimple as an A-module, then the centralizer of A in $\operatorname{End}_k(V)$ is a product of simple k-algebras (hence it is a semisimple k-algebra).*

PROOF. By assumption, we can write $V \approx \bigoplus_i r_i S_i$, where the S_i are simple A-modules, no two of which are isomorphic. The centralizer of A in $\operatorname{End}_k(V)$ is $\operatorname{End}_A(V)$, and $\operatorname{End}_A(V) \approx \operatorname{End}_A(\bigoplus_i r_i S_i)$. Because $\operatorname{Hom}_A(S_j, S_i) = 0$ for $i \ne j$,

$$\begin{aligned} \operatorname{End}_A(\textstyle\bigoplus r_i S_i) &\simeq \prod_i \operatorname{End}_A(r_i S_i) \quad \text{by (41)} \\ &\simeq \prod_i M_{r_i}(D_i) \quad \text{by (42)} \end{aligned}$$

where $D_i = \operatorname{End}_A(S_i)$. According to Schur's lemma (1.16), D_i is a division algebra, and therefore $M_{r_i}(D_i)$ is a simple k-algebra (1.11). □

THEOREM 5.4 *Every semisimple k-algebra is isomorphic to a product of simple k-algebras.*

PROOF. Choose an A-module V on which A acts faithfully, for example, $V = {}_AA$. Then A is equal to its double centralizer $C(C(A))$ in $\operatorname{End}_k(V)$ (see 1.14). According to Theorem 5.3, $C(A)$ is semisimple, and so $C(C(A))$ is a product of simple algebras (5.3). □

Modules over a semisimple k-algebra

Let $A = B \times C$ be a product of k-algebras. A B-module M becomes an A-module with the action $(b,c)m = bm$.

THEOREM 5.5 *Let A be a semisimple k-algebra, say, $A = A_1 \times \cdots \times A_t$ with the A_i simple. For each A_i, let S_i be a simple A_i-module.*

(a) *Each S_i is a simple A-module, and every simple A-module is isomorphic to exactly one of the S_i.*

(b) *Every A-module is isomorphic to $\bigoplus r_i S_i$ for some $r_i \in \mathbb{N}$, and two modules $\bigoplus r_i S_i$ and $\bigoplus r_i' S_i$ are isomorphic if and only if $r_i = r_i'$ for all i.*

PROOF. (a) It is obvious that each S_i is simple when regarded as an A-module, and that no two of them are isomorphic. It follows from 1.20 that ${}_AA \approx \bigoplus r_i S_i$ for some $r_i \in \mathbb{N}$. Let S be a simple A-module, and let x be a nonzero element of S. Then the map $a \mapsto ax\colon {}_AA \to S$ is surjective, and so its restriction to some S_i in ${}_AA$ is nonzero, and hence an isomorphism.

(b) The first part follows from (a) and the definition of a semisimple ring, and the second part follows from 1.3. □

PROPOSITION 5.6 *Let A be a semisimple k-algebra and k' a separable extension of k. Then $A \otimes_k F$ is semisimple.*

PROOF. We may suppose that it is simple. Then the centre F of A is a field. Because k'/k is separable, $F \otimes_k k'$ is a product of fields F_i. Now

$$A \otimes_k k' \simeq A \otimes_F (F \otimes_k k') \simeq A \otimes_F (\prod F_i) \simeq \prod A \otimes_F F_{\mathrm{i}},$$

and each algebra $A \otimes_F F_i$ is simple (2.15). □

Algebras, cohomology, and group extensions

Let A be a central simple algebra of degree n^2 over k, and assume that A contains a field L that is Galois of degree n over k. Let E be the set of invertible elements $\alpha \in A$ such that $\alpha L \alpha^{-1} = L$. Then each $\alpha \in E$ defines an element $x \mapsto \alpha x \alpha^{-1}$ of $\mathrm{Gal}(L/k)$, and the Noether-Skolem theorem implies that every element of $\mathrm{Gal}(L/k)$ arises from an $\alpha \in E$. Because $[L : k] = \sqrt{[A : k]}$, the centralizer of L is L itself, and so the sequence

$$1 \to L^\times \to E^\times \to \mathrm{Gal}(L/k) \to 1$$

is exact. It is not difficult to show that the map sending A to this sequence defines an isomorphism from $\mathcal{A}(L/k)$ to the set of isomorphism classes of extensions of $\mathrm{Gal}(L/k)$ by $L^\times$, and hence to $H^2(L/k)$ (see II, 1.18). See Serre 1950/51.

Brauer groups and K-theory

Let k be a field containing a primitive nth root ζ of 1. To any elements $a, b \in k^\times$, one attaches the k-algebra $A(a,b;\zeta)$ having generators i and j and relations

$$i^n = a, \quad j^n = b, \quad ij = \zeta ji.$$

It is a central simple algebra over k.

The ***Milnor K-group*** K_2F of a field F is the quotient of $F^\times \otimes_{\mathbb{Z}} F^\times$ by the abelian group generated by the elements of the form $u \otimes (1-u)$ with u an element of $F^\times$ such that $1-u \in F^\times$. Thus K_2F has as generators pairs $\{a,b\}$, one for each pair of elements in $F^\times$, and relations

$$\begin{aligned} \{ab,c\} &= \{a,c\}\{b,c\} \\ \{a,bc\} &= \{a,b\}\{a,c\} \\ \{u,1-u\} &= 1. \end{aligned}$$

It is known that these relations imply that

$$\begin{aligned} \{u,v\} &= \{v,u\}^{-1} \\ \{u,-u\} &= 1 \end{aligned}$$

(see Rosenberg 1994, p. 214).

It is not difficult to show that the $A(a,b;\zeta)$, considered as elements of $\mathrm{Br}(k)$ satisfy these relations, and so there is a well-defined homomorphism

$$K_2k \to \mathrm{Br}(k).$$

Remarkably, it has been proved (Theorem of Merkuryev-Suslin, early 1980s) that this map defines an isomorphism from K_2k/nK_2k onto the subgroup of $\mathrm{Br}(k)$ of elements killed by n, and so we have an explicit description of $\mathrm{Br}(k)_n$ in terms of generators and relations.[6]

EXERCISE 5.7 Let F be a field of characteristic $\neq 2$, and define the quaternion algebra $H(a,b)$ as in (1.12). Thus $H(a,b)$ has basis $1,i,j,k$ and $i^2=a$, $j^2=b$, $k=ij=-ji$. It is a central simple algebra over F.

(a) Show that every 4-dimensional central simple algebra over k is isomorphic to $H(a,b)$ for some $a,b \in F^\times$.

(b) According to Wedderburn's theorem, either $H(a,b) \approx M_2(F)$ or $H(a,b)$ is a division algebra. Show that the first case occurs if and only if $w^2-ax^2-by^2+abz^2$ has a nontrivial zero in F. (Hint: for $\alpha = w+xi+yj+zk$, let $\bar{\alpha} = w-xi-yj-zk$, and note that $\alpha\bar{\alpha} = w^2-ax^2-\cdots$)

(c) Show that $H(1,1) \approx M_2(F)$. (Hint: consider the matrices $e_{12}+e_{21}$ and $e_{11}-e_{22}$.)

(d) Show that $H(a,b) \approx H(ax^2,by^2)$ any $x,y \in F^\times$.

(e) Show that $H(a,b) \otimes_F L$ is the quaternion algebra over L defined by a,b regarded as elements of L.

(f) Verify that $H(a,b)$ is in fact central simple over F.

(g) Show that $H(a,1-a) \approx M_2(F)$, provided $a, 1-a \in F^\times$.

(h) Show that $H(1,b) \approx H(a,-a) \approx M_2(F)$ (Hint: consider $j+k$ and $i+j$.)

(i) Show that $H(a,b) \approx H(a,b)^{\mathrm{opp}}$.

[6] See: Merkurjev, A. S.; Suslin, A. A. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), no. 5, 1011–1046, 1135–1136.

The theorem is discussed in the book: Kersten, Ina. Brauergruppen von Körpern. (German) [Brauer groups of fields] Aspects of Mathematics, D6. Friedr. Vieweg & Sohn, Braunschweig, 1990.

(j) Show that $H(a,b) \approx M_2(F)$ if and only if $a \in \mathrm{Nm}(F[\sqrt{b}])$.

(k) Show that the map $\{a,b\} \mapsto [H(a,b)]: K_2F \to \mathrm{Br}(F)$ is well-defined.

EXERCISE 5.8 For a given central division algebra D over $\mathbb{Q}$, determine the number fields that admit an embedding into D.

EXERCISE 5.9 Determine the number fields that admit an embedding into some central division algebra over $\mathbb{Q}$.

For a solution to Exercises 5.8 and 5.9, see sx178999.

Notes

Brauer groups were introduced and studied by R. Brauer, and studied by Albert, Brauer, Noether, Hasse, and others, starting in the nineteen-twenties. The classic accounts are:
Deuring, M., Algebren, Springer, 1935.
Artin, E., Nesbitt, C., and Thrall, R., Rings with Minimum Condition, University of Michigan. Press, 1944.
Apart from the quaint terminology (e.g., Kronecker products for tensor products), the latter is still an excellent book.

Other books include Blanchard 1972, Farb and Dennis 1993, and Herstein 1968. These books include the Brauer group, but also cover much more (but no number theory). The second has lots of exercises.

I found the following especially useful when I was writing the first version of this chapter:
Serre, J-P., Applications algébriques de la cohomologie des groupes, I, II, Séminaire Henri Cartan, 1950/51 (now available at www.numdam.org).

Chapter V

Global Class Field Theory: Statements of the Main Theorems

> *La théorie du corps de classes a une réputation de difficulté qui est en partie justifiée. Mais il faut faire une distinction: il n'est peut-être pas en effet dans la science de théorie où tout à la fois les démonstrations soient aussi ardues, et les résultats d'une aussi parfaite simplicité et d'une aussi grande puissance.*
> J. Herbrand, 1936, p. 2.[1]

In this chapter, I state and explain the main theorems of global class field theory. They will be proved in Chapter VII

Throughout this chapter, K is a number field, although most of the results hold also for finite extensions of $\mathbb{F}_p(T)$.

Recall that for a number field K, we define a ***prime*** of K to be an equivalence class of nontrivial absolute values of K. There are two types of primes: the ***finite primes***, which can be identified with the prime ideals of $\mathcal{O}_K$, and the ***infinite primes.*** A ***real*** infinite prime can be identified with an embedding of K into $\mathbb{R}$, and a ***complex*** infinite prime can be identified with a conjugate pair of embeddings of K into $\mathbb{C}$. We use $\mathfrak{p}$ or v to denote a prime, finite or infinite. We use S to denote a finite set of primes of K, and also the set of primes of a finite extension L of K lying over K. The set of infinite primes is denoted by S_∞.

The completion of K at a prime $\mathfrak{p}$ (resp. v) is denoted by $K_\mathfrak{p}$ (resp. K_v), and the inclusion $K \hookrightarrow K_\mathfrak{p}$ (resp. $K \hookrightarrow K_v$) is denoted $a \mapsto a_\mathfrak{p}$ (resp. $a \mapsto a_v$).

1 Ray Class Groups

Ideals prime to S

Let $I = I_K$ be the group of fractional ideals in K. For a finite set S of primes of K, we define I^S to be the subgroup of I generated by the prime ideals not in S. Each element $\mathfrak{a}$

[1] Class field theory has a reputation for being difficult, which is partly justified. But it is necessary to make a distinction: there is perhaps nowhere in science a theory in which the proofs are so difficult but at the same time the results are of such perfect simplicity and of such great power.

of I^S factors uniquely as

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, \quad \mathfrak{p}_i \notin S, \quad n_i \in \mathbb{Z},$$

and so I^S can be identified with the free abelian group generated by the prime ideals not in S. Define

$$K^S = \{a \in K^\times \mid (a) \in I^S\} = \{a \in K^\times \mid \operatorname{ord}_\mathfrak{p}(a) = 0 \text{ all finite } \mathfrak{p} \in S\}.$$

Let $i\colon K^S \to I^S$ be the map sending an element a of K^S to the ideal $a\mathcal{O}_K$.

For example, when $K = \mathbb{Q}$ and S is the set of prime numbers dividing and integer n, I^S is the set of fractional ideals

$$\{(r/s) \mid r, s \in \mathbb{Z}\,,\ \gcd(r,n) = 1 = \gcd(s,n)\}$$

and

$$\mathbb{Q}^S = \{r/s \mid r, s \in \mathbb{Z}\,,\ \gcd(r,n) = 1 = \gcd(s,n)\}.$$

In this case, the natural map $\mathbb{Q}^S \to I^S$ is surjective with kernel $\{\pm 1\}$.

LEMMA 1.1 *For every finite set S of prime ideals in $\mathcal{O}_K$, the sequence*

$$0 \to U_K \to K^S \to I^S \to C \to 0$$

is exact. (Here $U_K = \mathcal{O}_K^\times$ and C is the full ideal class group $I/i(K^\times)$.)

PROOF. To show that $I^S \to C$ is surjective, we have to show that every ideal class $\mathcal{C}$ is represented by an ideal in I^S. Let $\mathfrak{a}$ represent $\mathcal{C}$. Then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals, and for any $c \in \mathfrak{c}$, $\mathfrak{a}\cdot(c) = \mathfrak{b}\cdot\mathfrak{c}^{-1}\cdot(c)$ is integral, and so we may suppose that $\mathfrak{a}$ itself is an integral ideal. Write $\mathfrak{a} = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}$, where $\mathfrak{b} \in I^S$. For each $\mathfrak{p} \in S$, choose a $\pi_\mathfrak{p} \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$, so that $\operatorname{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. By the Chinese Remainder Theorem, there exists an $a \in \mathcal{O}_K$ such that

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} \bmod \mathfrak{p}^{n(\mathfrak{p})+1}$$

for all $\mathfrak{p} \in S$. These congruences imply that $\operatorname{ord}_\mathfrak{p}(a) = n(\mathfrak{p})$ for all $\mathfrak{p} \in S$, and so $(a) = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}'$ with $\mathfrak{b}' \in I^S$. Now $a^{-1}\mathfrak{a} \in I^S$ and represents the same class as $\mathfrak{a}$ in C.

Next, if $\mathfrak{a} \in I^S$ maps to zero in C, then $\mathfrak{a} = (\alpha)$ for some $\alpha \in K^S$, and α is uniquely determined up to a unit. This proves the exactness at the remaining places. □

REMARK 1.2 In fact, every class in C is represented by an *integral* ideal $\mathfrak{a}$ in I^S: suppose the class is represented by $\mathfrak{a} \in I^S$; write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals in I^S, choose a nonzero $c \in \mathfrak{c} \cap K^S$ (exists by the Chinese remainder theorem), and note that $c\mathfrak{a}$ is integral.

Moduli

DEFINITION 1.3 A ***modulus*** for K is a function

$$m\colon \{\text{ primes of } K\} \to \mathbb{Z}$$

such that

(a) $m(\mathfrak{p}) \geq 0$ for all primes $\mathfrak{p}$, and $m(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$;

(b) if $\mathfrak{p}$ is real, then $m(\mathfrak{p}) = 0$ or 1;

(c) if $\mathfrak{p}$ is complex, then $m(\mathfrak{p}) = 0$.

Traditionally, one writes

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}.$$

A modulus $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ is said to ***divide*** a modulus $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ if $m(\mathfrak{p}) \leq n(\mathfrak{p})$ for all $\mathfrak{p}$. In particular, a prime $\mathfrak{p}$ divides a modulus $\mathfrak{m}$ if and only if $m(\mathfrak{p}) > 0$.

A modulus $\mathfrak{m}$ can be written

$$\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0,$$

where $\mathfrak{m}_\infty$ is a product of real primes and $\mathfrak{m}_0$ is product of positive powers of prime ideals, and hence can be identified with an ideal in $\mathcal{O}_K$.

The ray class group

For a modulus $\mathfrak{m}$, define $K_{\mathfrak{m},1}$ to be the set of $a \in K^\times$ such that

$$\begin{cases} \operatorname{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}) & \text{all finite } \mathfrak{p} \text{ dividing } \mathfrak{m} \\ a_{\mathfrak{p}} > 0 & \text{all real } \mathfrak{p} \text{ dividing } \mathfrak{m}. \end{cases}$$

Note that

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}) &\iff \pi^{m(\mathfrak{p})} | (a_{\mathfrak{p}} - 1) \\ &\iff a \mapsto 1 \text{ in } (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{m(\mathfrak{p})})^\times \simeq (\hat{\mathcal{O}}_{\mathfrak{p}}/\hat{\mathfrak{p}}^{m(\mathfrak{p})})^\times, \end{aligned}$$

where π is a prime element in the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$. Let

$$S(\mathfrak{m}) = \{ \text{primes dividing } \mathfrak{m} \}.$$

For any $a \in K_{\mathfrak{m},1}$ and prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}$, $\operatorname{ord}_{\mathfrak{p}}(a-1) > 0 = \operatorname{ord}_{\mathfrak{p}}(1)$, and so

$$\operatorname{ord}_{\mathfrak{p}}(a) = \operatorname{ord}_{\mathfrak{p}}((a-1)+1) = 0.$$

Therefore, for any $a \in K_{\mathfrak{m},1}$, the ideal (a) lies in $I^{S(\mathfrak{m})}$. Let i denote the map $a \mapsto (a)\colon K_{\mathfrak{m},1} \to I^{S(\mathfrak{m})}$. The quotient

$$C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$$

is called the ***(ray) class group modulo*** $\mathfrak{m}$.

EXAMPLE 1.4 The expression $\mathfrak{m} = (2)^3 \cdot (17)^2 \cdot (19) \cdot \infty$ is a modulus for $\mathbb{Q}$ with $\mathfrak{m}_0 = (2)^3 \cdot (17)^2 \cdot (19)$ and $\mathfrak{m}_\infty = \infty$ (here ∞ denotes the unique infinite prime of $\mathbb{Q}$). Moreover, $\mathbb{Q}_{\mathfrak{m},1}$ consists of the positive rational numbers a such that

$$\begin{cases} \operatorname{ord}_2(a-1) \geq 3 \\ \operatorname{ord}_{17}(a-1) \geq 2 \\ \operatorname{ord}_{19}(a-1) \geq 1 \end{cases}.$$

The condition at 2 says that a is the quotient of two odd integers, $a = b/c$, and that the image of bc^{-1} in $(\mathbb{Z}/8\mathbb{Z})^\times$ is 1. The other conditions can be expressed similarly.

LEMMA 1.5 *Let S be a finite set of prime ideals of K. Then every element $\alpha \in K^S$ can be written $\alpha = a/b$ with $a, b \in \mathcal{O}_K \cap K^S$.*

PROOF. Because $\alpha \in K^S$, $(\alpha) = \mathfrak{a}/\mathfrak{b}$ with $\mathfrak{a}, \mathfrak{b}$ integral ideals in I^S. Clearly $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element $\mathcal{C}$ of the ideal class group, and according to Remark 1.2 we can choose an integral ideal $\mathfrak{c}$ in I^S to represent $\mathcal{C}^{-1}$. Now $(\alpha) = \mathfrak{ac}/\mathfrak{bc} = (a)/(b)$ for some $a, b \in \mathcal{O}_K \cap K^S$. □

PROPOSITION 1.6 *Every class in $C_\mathfrak{m}$ is represented by an integral ideal $\mathfrak{a}$, and two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same class in $C_\mathfrak{m}$ if and only if there exist nonzero $a, b \in \mathcal{O}_K$ such that $a\mathfrak{a} = b\mathfrak{b}$ and*

$$a \equiv b \equiv 1 \bmod \mathfrak{m}_0$$

a and b have the same sign for every real prime dividing $\mathfrak{m}$.

PROOF. Suppose that the class is represented by $\mathfrak{a} \in I^S$, and let $\mathfrak{a} = \mathfrak{bc}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals in I^S. The Chinese remainder theorem shows that there exists a nonzero $c \in \mathfrak{c} \cap K_{\mathfrak{m}_0,1}$, and the strong approximation theorem shows that c can be chosen to be > 0 at the real primes. Now $c\mathfrak{a}$ is integral and represents the same class as $\mathfrak{a}$ in $C_\mathfrak{m}$. The second part of the statement follows from Lemma 1.5. □

Thus, for example, the usual ideal class group can be identified with the set of integral ideals modulo the equivalence relation: $\mathfrak{a} \sim \mathfrak{b}$ if and only if $a\mathfrak{a} = b\mathfrak{b}$ for some nonzero $a, b \in \mathcal{O}_K$.

THEOREM 1.7 *For every modulus $\mathfrak{m}$ of K, there is an exact sequence*

$$0 \to U/U_{\mathfrak{m},1} \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to C_\mathfrak{m} \to C \to 0$$

and canonical isomorphisms

$$K_\mathfrak{m}/K_{\mathfrak{m},1} \simeq \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p}|\mathfrak{m}}} \{\pm\} \times \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p}|\mathfrak{m}}} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \simeq \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p}|\mathfrak{m}}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times,$$

where

$$\begin{aligned} K_\mathfrak{m} &= K^{S(\mathfrak{m})} = \{\alpha \in K^\times \mid \operatorname{ord}_\mathfrak{p}(\alpha) = 0 \text{ for all } \mathfrak{p}|\mathfrak{m}_0\} \\ U &= \mathcal{O}_K^\times \text{, the group of units in } K, \\ U_{\mathfrak{m},1} &= U \cap K_{\mathfrak{m},1}. \end{aligned}$$

Therefore, $C_\mathfrak{m}$ is a finite group of order

$$h_\mathfrak{m} = h \cdot (U : U_{\mathfrak{m},1})^{-1} \cdot 2^{r_0} \cdot \mathbb{N}(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \frac{1}{\mathbb{N}\mathfrak{p}}\right),$$

where r_0 is the number of real primes dividing $\mathfrak{m}$ and h is the class number of K (order of C).

PROOF. The inclusion $I^{S(\mathfrak{m})} \to I$ defines a homomorphism $C_\mathfrak{m} \to C$. Consider the pair of maps

$$K_{\mathfrak{m},1} \xrightarrow{f} K_\mathfrak{m} \xrightarrow{g} I^{S(\mathfrak{m})}.$$

According to the Lemma 1.1, the kernel and cokernel of g are U and C respectively. The cokernel of $g \circ f$ is $C_\mathfrak{m}$ (by definition) and its kernel is $K_{\mathfrak{m},1} \cap U = U_{\mathfrak{m},1}$. Finally, f is injective. Therefore, the kernel-cokernel sequence (see II, A.2) of the pair of maps is

$$0 \to U_{\mathfrak{m},1} \to U \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to C_\mathfrak{m} \to C \to 0.$$

We next prove that $K_\mathfrak{m}$ is canonically isomorphic to the given groups. Let $\mathfrak{p}$ be a prime dividing $\mathfrak{m}$. If $\mathfrak{p}$ is real, we map $\alpha \in K_\mathfrak{m}$ to the sign of $\alpha_\mathfrak{p}$ (recall that a real prime is an embedding $K \hookrightarrow \mathbb{R}$, and that $\alpha_\mathfrak{p}$ denotes the image of α under the embedding). If $\mathfrak{p}$ is finite, i.e., it is a prime ideal in $\mathcal{O}_K$, then we map $\alpha \in K_\mathfrak{m}$ to $[a][b]^{-1} \in (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$, where a, b are as in the lemma. As a and b are relatively prime to $\mathfrak{p}$, their classes $[a]$ and $[b]$ in $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$ are invertible, and so this makes sense. The weak approximation theorem (ANT, 7.20) shows that the map $K_\mathfrak{m} \to \prod\{\pm\} \times \prod(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$ is surjective, and its kernel is obviously $K_{\mathfrak{m},1}$.

The Chinese Remainder Theorem shows that there is an isomorphism of rings

$$\mathcal{O}_K/\mathfrak{m}_0 \simeq \prod_{\mathfrak{p}|\mathfrak{m}} \mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})},$$

and hence an isomorphism of groups

$$(\mathcal{O}_K/\mathfrak{m}_0)^\times \simeq \prod(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times.$$

This completes proof of the isomorphisms.

It remains to compute the orders of the groups. Note that $\mathcal{O}_K/\mathfrak{p}^m$ is a local ring with maximal ideal $\mathfrak{p}/\mathfrak{p}^m$ (because its ideals correspond to the ideals of $\mathcal{O}_K$ containing $\mathfrak{p}^m$), and so its units are the elements not in $\mathfrak{p}/\mathfrak{p}^m$. The filtration

$$(\mathcal{O}_K/\mathfrak{p}^m)^\times \supset (1+\mathfrak{p})/\mathfrak{p}^m \supset \cdots \supset (1+\mathfrak{p}^{m-1})/\mathfrak{p}^m \supset 0$$

has quotients isomorphic to

$$k^\times, k, \dots, k, \quad k \stackrel{\text{def}}{=} \mathcal{O}_K/\mathfrak{p},$$

and so $(\mathcal{O}_K/\mathfrak{p}^m)^\times$ has order $(q-1)q^{m-1}$, $q = (\mathcal{O}_K : \mathfrak{p}) \stackrel{\text{def}}{=} \mathbb{N}\mathfrak{p}$. This shows that

$$(C_\mathfrak{m} : 1) = (C : 1) \cdot (K_\mathfrak{m} : K_{\mathfrak{m},1}) \cdot (U_\mathfrak{m} : U_{\mathfrak{m},1})^{-1}$$

is equal to the expression in the statement of the theorem. □

EXAMPLE 1.8 (a) If $\mathfrak{m} = 1$, then $C_\mathfrak{m} = C$.

(b) When $\mathfrak{m}$ is the product of the real primes, $C_\mathfrak{m}$ is the narrow-class group and there is an exact sequence

$$0 \to U/U_+ \to K^\times/K_+ \to C_\mathfrak{m} \to C \to 1,$$

where K_+ is the group of totally positive elements (i.e., positive under all real embeddings) and U_+ is the group of all totally positive units. Moreover, $K^\times/K_+ \simeq \prod_{\mathfrak{p}\text{ real}}\{\pm\}$, and so the kernel of $C_\mathfrak{m} \to C$ is the set of possible signs modulo those arising from units.

For $\mathbb{Q}$, the narrow-class group is trivial. For $\mathbb{Q}[\sqrt{d}]$, $d > 0$, there are two real primes, and $U = \{\pm\varepsilon^m \mid m \in \mathbb{Z}\} \approx (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$, where ε is a fundamental unit. Let $\bar{\varepsilon}$ be the conjugate of ε. Then $h_{\mathfrak{m}} = 2h$ or h according as ε and $\bar{\varepsilon}$ have the same or different signs. Note that $\mathrm{Nm}(\varepsilon) = +1$ if the signs are the same and -1 if they differ. For small values of d we have

d	h	ε	$\mathrm{Nm}(\varepsilon)$
2	1	$1+\sqrt{2}$	-1
3	1	$2+\sqrt{3}$	1
5	1	$(1+\sqrt{5})/2$	-1
6	1	$5+2\sqrt{6}$	1

Therefore, $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{6}]$ have class number 1 but narrow-class number 2, whereas for $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{5}]$ both class numbers are 1.

(c) For the field $\mathbb{Q}$ and the modulus (m), the sequence becomes

$$0 \to \{\pm 1\} \to (\mathbb{Z}/m\mathbb{Z})^\times \to C_{\mathfrak{m}} \to 0.$$

For the modulus $\infty(m)$, the sequence becomes

$$0 \to \{\pm 1\} \to \{\pm\} \times (\mathbb{Z}/m\mathbb{Z})^\times \to C_{\mathfrak{m}} \to 0.$$

Here -1 maps to $(-, [-1])$, and the subgroup $(\mathbb{Z}/m\mathbb{Z})^\times$ of the product maps isomorphically onto the quotient $C_{\mathfrak{m}}$.

The Frobenius element

We review the theory of the Frobenius element (ANT, Chapter 8). Let K be a number field, and let L be a finite Galois extension of K with group G. Let $\mathfrak{p}$ be an ideal of K, and let $\mathfrak{P}$ be an ideal of L lying over it. The decomposition group $D(\mathfrak{P})$ (or $G(\mathfrak{P})$) is defined to be

$$\{\tau \in G \mid \tau\mathfrak{P} = \mathfrak{P}\}.$$

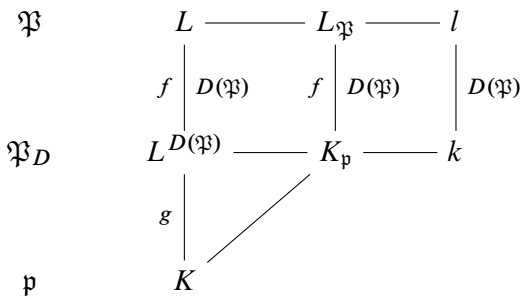
Equivalently, it is the set of elements of G that act continuously for the $\mathfrak{P}$-adic topology, and so extend to the completion $L_{\mathfrak{P}}$. In this way we obtain an isomorphism

$$D(\mathfrak{P}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

Assume $\mathfrak{P}$ is unramified over $\mathfrak{p}$. Then the action of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ on $\mathcal{O}_L$ induces an isomorphism

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(l/k),$$

where l and k are the residue fields. Pictorially:



The group $\mathrm{Gal}(l/k)$ is cyclic with a canonical generator, namely, the Frobenius element $x \mapsto x^q$, where q is the number of elements of k. Hence $D(\mathfrak{P})$ is cyclic, and the generator of $D(\mathfrak{P})$ corresponding to the Frobenius element in $\mathrm{Gal}(l/k)$ is called the ***Frobenius element*** $(\mathfrak{P}, L/K)$ at $\mathfrak{P}$. It is the unique element σ of $\mathrm{Gal}(L/K)$ satisfying the following two conditions:

(a) $\sigma \in D(\mathfrak{P})$, i.e., $\sigma\mathfrak{P} = \mathfrak{P}$;

(b) for all $\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^q \bmod \mathfrak{P}$, where q is the number of elements the residue field $\mathcal{O}_K/\mathfrak{p}$, $\mathfrak{p} = \mathfrak{P} \cap K$.

We now list the basic properties of $(\mathfrak{P}, L/K)$.

1.9 *Let $\tau\mathfrak{P}$ be a second prime dividing $\mathfrak{p}$. Then $D(\tau\mathfrak{P}) = \tau D(\mathfrak{P})\tau^{-1}$, and*

$$(\tau\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}.$$

PROOF. If $\rho \in D(\mathfrak{P})$, then

$$\tau\rho\tau^{-1}(\tau\mathfrak{P}) = \tau\rho\mathfrak{P} = \tau\mathfrak{P},$$

and so $\tau\rho\tau^{-1} \in D(\tau\mathfrak{P})$. Thus $\tau D(\mathfrak{P})\tau^{-1} \subset D(\tau\mathfrak{P})$, and since they have the same order, they must be equal.

Let $\alpha \in \mathcal{O}_L$ and let $\sigma = (\mathfrak{P}, L/K)$; then

$$\tau\sigma\tau^{-1}(\alpha) = \tau\left((\tau^{-1}\alpha)^q + a\right) \text{ , some } a \in \mathfrak{P} \text{ , and}$$

$$\tau\left((\tau^{-1}\alpha)^q + a\right) = \alpha^q + \tau a \equiv \alpha^q \bmod \tau\mathfrak{P}.$$

□

As G acts transitively on the primes dividing $\mathfrak{p}$, this implies that

$$\{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}$$

is a conjugacy class in G, which we denote $(\mathfrak{p}, L/K)$. When L/K is abelian, $(\mathfrak{p}, L/K)$ contains a single element, and we regard it as an element of $\mathrm{Gal}(L/K)$ (rather than a set consisting of a single element).

1.10 *Consider a tower of fields*

$$\begin{array}{cc} M & \mathfrak{Q} \\ | & \\ L & \mathfrak{P} \\ | & \\ K & \mathfrak{p} \end{array}$$

and assume that $\mathfrak{Q}$ is unramified over $\mathfrak{p}$; then

$$(\mathfrak{Q}, M/L) = (\mathfrak{Q}, M/K)^{f(\mathfrak{P}/\mathfrak{p})}.$$

PROOF. Let $k(\mathfrak{Q}) \supset k(\mathfrak{P}) \supset k(\mathfrak{p})$ be the tower of residue fields. Then $f(\mathfrak{P}/\mathfrak{p}) \overset{\text{def}}{=} [k(\mathfrak{P}) : k(\mathfrak{p})]$, and the Frobenius element in $\mathrm{Gal}(k(\mathfrak{Q})/k(\mathfrak{P}))$ is the $f(\mathfrak{P}/\mathfrak{p})$th power of the Frobenius element in $\mathrm{Gal}(k(\mathfrak{Q})/k(\mathfrak{p}))$. The rest is straightforward. □

1.11 *In 1.10, assume that L is Galois over K; then*

$$(\mathfrak{Q}, M/K)|L = (\mathfrak{P}, L/K).$$

PROOF. Clearly $(\mathfrak{Q}, M/K)|L$ satisfies the conditions characterizing $(\mathfrak{P}, L/K)$. □

Let L_1 and L_2 be Galois extensions of K contained in some field Ω, and let $M = L_1 \cdot L_2$. Then M is Galois over K, and there is an injective homomorphism

$$\sigma \mapsto (\sigma|L_1, \sigma|L_2)\colon \mathrm{Gal}(M/K) \to \mathrm{Gal}(L_1/K)) \times \mathrm{Gal}(L_2/K).$$

1.12 *Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_M$, and let $\mathfrak{P}_i = \mathfrak{Q} \cap \mathcal{O}_{L_i}$. Under the above map,*

$$(\mathfrak{Q}, M/K) \mapsto (\mathfrak{P}_1, L_1/K) \times (\mathfrak{P}_2, L_2/K).$$

PROOF. Apply 1.11. □

Note that $\mathfrak{p}$ splits completely in L if and only if $(\mathfrak{P}, L/K) = 1$ for one (hence all) primes $\mathfrak{P}$ lying over it. Hence, in the situation of 1.12, $\mathfrak{p}$ splits completely in M if and only if it splits completely in L_1 and L_2.

2 L-Series and the Density of Primes in Arithmetic Progressions

We begin by briefly reviewing the elementary theory of Dirichlet L-series (see, for example, Serre 1970, Chapter VI).

Let m be an integer. A ***Dirichlet character modulo*** m is a homomorphism $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. Because $(\mathbb{Z}/m\mathbb{Z})^\times$ is finite, $\chi([n])$ is a root of 1 for all n. A Dirichlet character modulo m can be regarded as a multiplicative function on the set of integers prime to m whose value at n depends only on n modulo m. Often one extends χ to a function on all the integers by setting $\chi(n) = 0$ when $\gcd(m, n) \neq 1$. The trivial Dirichlet character modulo m, taking the value 1 for all integers prime to m, is called the ***principal Dirichlet character*** χ_0.

To a Dirichlet character χ modulo m, one attaches a Dirichlet series

$$L(s, \chi) = \prod_{p \nmid m} \frac{1}{1 - \chi(p)p^{-s}} = \sum_{n>0} \chi(n)/n^s.$$

Both expressions converge for s a complex number with $\Re(s) > 1$—their equality is the analytic expression of the unique factorization. Note that $L(s, \chi_0)$ differs from the Riemann zeta function $\zeta(s)$ only in that it is missing the factors $\frac{1}{1-p^{-s}}$ for p dividing m.

THEOREM 2.1 *(a) The zeta function $\zeta(s)$ extends to a meromorphic function on the half-plane $\Re(s) > 0$, and*

$$\zeta(s) = \frac{1}{s-1} + \varphi(s),$$

where $\varphi(s)$ is holomorphic for $\Re(s) > 0$.

(b) If $\chi \neq \chi_0$, then the series for $L(s, \chi)$ converges for $\Re(s) > 0$ and $L(1, \chi) \neq 0$.

PROOF. Serre 1970, Chapter VI, Propositions 10, 12, Théoŕeme 1. □

On applying log to the equality in (a), one finds using the approximation $-\log(1-x) \sim x$ that

$$\sum 1/p^s \sim \log \frac{1}{1-s} \text{ as } s \downarrow 1.$$

By this we mean that the quotient $\frac{\sum 1/p^s}{-\log(1-s)}$ converges to 1 as s approaches 1 through real numbers > 1. This result makes reasonable the definition that a set T of primes has ***Dirichlet (or analytic) density*** δ if

$$\sum_{p\in T} 1/p^s \sim \delta \log \frac{1}{1-s} \text{ as } s \downarrow 1.$$

Define $f_\chi(s) = \sum_{p\nmid m} \chi(p)/p^s$. Then (2.1b) shows that, for $\chi \neq \chi_0$, $f_\chi(s)$ is bounded near $s = 1$. An elementary argument (Serre 1970, Chapter VI, Lemme 9) shows that, for every a prime to m,

$$\sum_{p\equiv a \bmod m} 1/p^s = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s),$$

where $\varphi(m) \overset{\text{def}}{=} |(\mathbb{Z}/m\mathbb{Z})^\times|$ and the sum is over all Dirichlet characters modulo m.

THEOREM 2.2 *For every a prime to m, the primes in the arithmetic progression*

$$\ldots, a-2m, a-m, a, a+m, a+2m, \ldots$$

have Dirichlet density $1/\varphi(m)$.

PROOF. For $\chi \neq \chi_0$, $f_\chi(s)$ remains bounded near $s = 1$, and so

$$\sum_{p\equiv a \bmod m} 1/p^s \sim \frac{1}{\varphi(m)} \chi_0(a)^{-1} f_{\chi_0}(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{1-s} \text{ as } s \downarrow 1.$$

□

COROLLARY 2.3 *For every m, the set of primes splitting in the cyclotomic field $\mathbb{Q}[\zeta_m]$ has Dirichlet density $1/\varphi(m)$.*

PROOF. A prime ideal (p) splits in $\mathbb{Q}[\zeta_m]$ if and only if $p \equiv 1 \mod m$. □

We now explain how the above results generalize from $\mathbb{Q}$ to arbitrary number fields. Proofs will be given in Chapter VI.

Let K be a number field, and let $\mathfrak{m}$ be modulus for K. A ***(Dirichlet or Weber) character modulo*** $\mathfrak{m}$ is a homomorphism $\chi: C_\mathfrak{m} \to \mathbb{C}^\times$—again, its values are roots of 1. Alternatively, such a character is a multiplicative function $I^S \to \mathbb{C}^\times$ that is zero on $i(K_{\mathfrak{m},1})$ for some modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$. The ***principal character*** modulo $\mathfrak{m}$ is the function $\chi_0: C_\mathfrak{m} \to \mathbb{C}^\times$ taking only the value 1.

To a character χ modulo $\mathfrak{m}$, one attaches a Dirichlet series

$$L(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}} = \sum_{(\mathfrak{a},\mathfrak{m}_0)=\mathcal{O}_K} \chi(\mathfrak{a})/\mathbb{N}\mathfrak{a}^s.$$

The product is over the prime ideals relatively prime to $\mathfrak{m}_0$, and the sum is over the integral ideals relatively prime to $\mathfrak{m}_0$. Again, both expressions converge for $\Re(s) > 1$, and their equality is the analytic expression of the unique factorization of ideals. The L-series $L(s,\chi_0)$ differs by only a finite number of factors from the ***Dedekind zeta function***

$$\zeta_K(s) \overset{\text{def}}{=} \prod_\mathfrak{p} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}} = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \mathbb{N}\mathfrak{a}^{-s}.$$

THEOREM 2.4 *(a) The zeta function $\zeta_K(s)$ extends to a meromorphic function on the half-plane $\Re(s) > 0$, and*

$$\zeta_K(s) \sim \frac{2^{r_1}(2\pi)^{r_2}\ Reg(K)}{w_K|\Delta_{K/\mathbb{Q}}|^{1/2}} h_K \frac{1}{s-1} \text{ as } s \downarrow 1,$$

where r_1 and r_2 are the numbers of real and complex primes of K respectively, $Reg(K)$ is the regulator of K (see ANT, Chapter 5), w_K is the number of roots of 1 in K, $\Delta_{K/\mathbb{Q}}$ is the discriminant of $K/\mathbb{Q}$, and h_K is the class number.

(b) If $\chi \neq \chi_0$, then the series for $L(s,\chi)$ converges for $\Re(s) > 0$ and $L(1,\chi) \neq 0$.

The proof of (b) uses the Existence Theorem (see 3.6).

Again, on applying log to the equality in (a), one finds that

$$\sum_{\mathfrak{p}} 1/\mathbb{N}\mathfrak{p}^s \sim \log \frac{1}{s-1} \text{ as } s \downarrow 1,$$

and one says that a set T of prime ideals in K has ***Dirichlet (or natural) density*** δ if

$$\sum_{\mathfrak{p}\in T} 1/\mathbb{N}\mathfrak{p}^s \sim \delta \log \frac{1}{s-1} \text{ as } s \downarrow 1.$$

A similar argument to that in the previous case proves:

THEOREM 2.5 *For every ideal $\mathfrak{a}$ relatively prime to $\mathfrak{m}_0$, the prime ideals in $\mathcal{O}_K$ whose class in $C_\mathfrak{m}$ is $[\mathfrak{a}]$ have Dirichlet density $1/h_\mathfrak{m}$.*

The analysis in the proofs of Theorems 2.4 and 2.5 is the same as in the case $K = \mathbb{Q}$, but the number theory is much more difficult.

3 The Main Theorems in Terms of Ideals

The Artin map

Let L/K be a finite abelian extension Galois group G. Recall that, for a prime ideal $\mathfrak{p}$ of K that is unramified in L, there is a Frobenius automorphism $\sigma = (\mathfrak{p}, L/K)$ of L uniquely determined by the following condition: for every prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$, $\sigma\mathfrak{P} = \mathfrak{P}$, and $\sigma\alpha \equiv \alpha^{\mathbb{N}\mathfrak{p}} \mod \mathfrak{P}$.

For every finite set S of primes of K containing all primes that ramify in L, we have a homomorphism

$$\psi_{L/K}\colon I^S \to \mathrm{Gal}(L/K), \quad \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_t^{n_t} \mapsto \prod(\mathfrak{p}_i, L/K)^{n_i}$$

called the ***global Artin map (or reciprocity map)***.

EXAMPLE 3.1 Let $K = \mathbb{Q}[\sqrt{m}]$, where m is a square-free integer. The set S of finite primes ramifying in K consists of the primes dividing m if $m \equiv 1 \bmod 4$ and the primes dividing m together with 2 otherwise. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with $\{\pm 1\}$. The Artin map is the homomorphism determined by

$$p \mapsto \left(\frac{m}{p}\right) : I^S \to \mathrm{Gal}(K/\mathbb{Q}),$$

where $(\frac{m}{p})$ is the quadratic residue (Legendre) symbol.

EXAMPLE 3.2 Let $L = \mathbb{Q}[\zeta_m]$, where ζ_m is a primitive mth root of 1. Assume that m is odd or divisible by 4 (so that the primes ramifying in L are precisely the primes dividing m). The map sending an integer n prime to m to the automorphism $\zeta \mapsto \zeta^n$ of L defines an isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$. For p not dividing n, $(p, L/K) = [p]$. If r and s are positive integers prime to m, then r/s defines a class $[r/s] = [r][s]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$, and the Artin map is the composite of

$$I^S \xrightarrow{(r/s)\mapsto[r/s]} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{[n]\mapsto(\zeta\mapsto\zeta^n)} \mathrm{Gal}(L/\mathbb{Q}).$$

Recall (ANT, p. 68) that for any finite extension of number fields L/K, the norm map $\mathrm{Nm}_{L/K}\colon I_L \to I_K$ from the group of fractional ideals of L to the similar group for K, is the unique homomorphism such that for any prime ideal $\mathfrak{P}$ of L, $\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. For any $\alpha \in L$, $\mathrm{Nm}_{L/K}((\alpha)) = (\mathrm{Nm}_{L/K}\,\alpha)$.

PROPOSITION 3.3 *Let L be an abelian extension of K, and let K' be an intermediate field: $L \supset K' \supset K$. Then the following diagram commutes:*

$$\begin{array}{ccc} I_{K'}^S & \xrightarrow{\psi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow \\ I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Here S is any finite set of prime ideals of K containing all those that ramify in L, and also the set of primes of K' lying over a prime in S.

PROOF. Let $\mathfrak{p}'$ be any prime ideal of K' lying over a prime ideal $\mathfrak{p}$ of K not in S. Then $\mathrm{Nm}_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$, and we have to show that $\psi_{L/K'}(\mathfrak{p}') = \psi_{L/K}(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})})$, i.e., that $(\mathfrak{P}, L/K') = (\mathfrak{P}, L/K)^{f(\mathfrak{p}'/\mathfrak{p})}$ for every prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$. But this was proved in 1.10. □

COROLLARY 3.4 *For every finite abelian extension L of K, $\mathrm{Nm}_{L/K}(I_L^S)$ is contained in the kernel of $\psi_{L/K}\colon I^S \to \mathrm{Gal}(L/K)$.*

PROOF. Take $K' = L$ in the above diagram. □

Thus the Artin map induces a homomorphism

$$\psi_{L/K}\colon I_K^S/\,\mathrm{Nm}(I_L^S) \to \mathrm{Gal}(L/K)$$

whenever L/K is a finite abelian extension. The group $I^S/\,\mathrm{Nm}(I_L^S)$ is infinite (because infinitely many primes don't split), and so $\psi_{L/K}$ can not be injective.

The main theorems of global class field theory

Let S be a finite set of primes of K. We shall say that a homomorphism $\psi\colon I^S \to G$ ***admits a modulus*** if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \supset S$ such that $\psi(i(K_{\mathfrak{m},1})) = 0$. Thus ψ admits a modulus if and only if it factors through $C_{\mathfrak{m}}$ for some $\mathfrak{m}$ with $S(\mathfrak{m}) \supset S$.

THEOREM 3.5 (RECIPROCITY LAW) *Let L be a finite abelian extension of K, and let S be the set of primes of K ramifying in L. Then the Artin map $\psi\colon I^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, and it defines an isomorphism*

$$I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})\cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})}) \to \mathrm{Gal}(L/K).$$

A modulus as in the statement of the theorem is called a ***defining modulus for*** L.

Note that the theorem does not imply that K has even a single nontrivial abelian extension. Write $I_K^{\mathfrak{m}}$ for the group of $S(\mathfrak{m})$-ideals in K, and $I_L^{\mathfrak{m}}$ for the group of $S(\mathfrak{m})'$-ideals in L, where $S(\mathfrak{m})'$ contains the primes of L lying over a prime in $S(\mathfrak{m})$. Call a subgroup H of $I_K^{\mathfrak{m}}$ a ***congruence subgroup modulo*** $\mathfrak{m}$ if

$$I_K^{\mathfrak{m}} \supset H \supset i(K_{\mathfrak{m},1}).$$

THEOREM 3.6 (EXISTENCE THEOREM) *For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K, unramified at the primes not dividing $\mathfrak{m}$ such that $H = i(K_{\mathfrak{m},1})\cdot \mathrm{Nm}_{L/K}(I_L^{\mathfrak{m}})$.*

Note that, for H and L as in the theorem, the Artin map $\psi_{L/K}$ induces an isomorphism

$$I^{S(\mathfrak{m})}/H \to \mathrm{Gal}(L/K).$$

In particular, for each modulus $\mathfrak{m}$ there is a field $L_{\mathfrak{m}}$, called the ***ray class field modulo*** $\mathfrak{m}$ such that the Artin map defines an isomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L_{\mathfrak{m}}/K)$. For a field $L \subset L_{\mathfrak{m}}$, set

$$\mathrm{Nm}(C_{L,\mathfrak{m}}) = i(K_{\mathfrak{m},1})\cdot \mathrm{Nm}(I_L^{\mathfrak{m}}) \mod i(K_{\mathfrak{m},1}).$$

COROLLARY 3.7 *Fix a modulus $\mathfrak{m}$. Then the map $L \mapsto \mathrm{Nm}(C_{L,\mathfrak{m}})$ is a bijection from the set of abelian extensions of K contained in $L_{\mathfrak{m}}$ to the set of subgroups of $C_{\mathfrak{m}}$. Moreover,*

$$\begin{aligned} L_1 \subset L_2 &\iff \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \supset \mathrm{Nm}(C_{L_2,\mathfrak{m}});\\ \mathrm{Nm}(C_{L_1\cdot L_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cap \mathrm{Nm}(C_{L_2,\mathfrak{m}});\\ \mathrm{Nm}(C_{L_1\cap L_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cdot \mathrm{Nm}(C_{L_2,\mathfrak{m}}). \end{aligned}$$

REMARK 3.8 Let L/K be an abelian extension with Galois group G. According to the Reciprocity Law, there is a modulus $\mathfrak{m}$ with support the set of primes of K ramifying in L such that the Artin map $\psi_{L/K}\colon I^{S(\mathfrak{m})} \to G$ takes the value 1 on $i(K_{\mathfrak{m},1})$. Consider the map in Theorem 1.7

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \hookrightarrow K_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{i} C_{\mathfrak{m}} \xrightarrow{\psi_{L/K}} G.$$

Clearly, there will be a smallest integer $f(\mathfrak{p}) \le m(\mathfrak{p})$ such that this map factors through $(\mathcal{O}_K/\mathfrak{p}^{f(\mathfrak{p})})^\times$. The modulus $\mathfrak{f}(L/K) = \mathfrak{m}_\infty \prod \mathfrak{p}^{f(\mathfrak{p})}$ is then the smallest modulus such that $\psi_{L/K}$ factors through $C_{\mathfrak{f}}$—it is called the ***conductor***[2] of L/K. The conductor $\mathfrak{f}(L/K)$ is divisible exactly by the primes ramifying in L.

The subfields of the ray class field $L_{\mathfrak{m}}$ containing K are those with conductor $\mathfrak{f}|\mathfrak{m}$.[3] Every abelian extension of K is contained in $L_{\mathfrak{m}}$ for some $\mathfrak{m}$.

[2]Führer in German—in Germany in the 1930s, conversations in public on class field theory could be hazardous.

[3]Let L be an abelian extension of K whose conductor divides $\mathfrak{m}$. Then the primes that split in $L_{\mathfrak{m}}$ also split in L. Now the Chebotarev density theorem shows that $L \subset L_{\mathfrak{m}}$ (see 3.25 below).

In Section 5 below, we shall restate Theorems 3.5 and 3.6 in terms of idèles, and in Chapter VII we prove the restated theorems.

As we discuss below, there is a rather simple analytic proof that the Artin map is surjective. Thus the difficulty in proving the Reciprocity Law is in showing that the Artin map admits a conductor and that

$$\left(I^{S(\mathfrak{m})} : i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})})\right) \leq [L : K].$$

To prove the Existence Theorem we must construct a ray class field for each modulus. Unfortunately, we don't know how to construct the ray class field directly. Rather we construct enough extensions to force the theorem to be true.

EXAMPLE 3.9 The ray class group for the modulus $\mathfrak{m} = 1$ is the ideal class group, and the corresponding ray class field is the Hilbert class field; it is the maximal abelian extension of K that is unramified at all primes including the real primes (which means that real primes stay real). For example, the Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ itself (because $\mathbb{Q}$ has class number 1). The Hilbert class field of $\mathbb{Q}[\sqrt{-5}]$ is $\mathbb{Q}[\sqrt{-1}, \sqrt{5}]$—both 2 and 5 ramify in $\mathbb{Q}[\sqrt{-5}]$, but only 2 ramifies in $\mathbb{Q}[\sqrt{-1}]$ and only 5 ramifies in $\mathbb{Q}[\sqrt{5}]$, from which it follows that the primes of $\mathbb{Q}[\sqrt{-5}]$ dividing 2 and 5 do not ramify $\mathbb{Q}[\sqrt{-1}, \sqrt{5}]$.

EXAMPLE 3.10 Let m be a positive integer which is odd or divisible by 4. The ray class field for (m) is $\mathbb{Q}[\zeta_m + \bar{\zeta}_m]$, and the ray class field for $\infty(m)$ is $\mathbb{Q}[\zeta_m]$.[4] Thus the Reciprocity Law implies the Kronecker-Weber theorem: every abelian extension of $\mathbb{Q}$ has conductor dividing $\infty(m)$ for some m, and therefore is contained in a cyclotomic field.

EXAMPLE 3.11 Let d be a square-free integer. We compute the conductor of $K = \mathbb{Q}[\sqrt{d}]$ over $\mathbb{Q}$ by finding the smallest integer m such that $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_m]$.

First, consider an odd prime p. Then $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, and so has a unique quotient group of order 2. Therefore, $\mathbb{Q}[\zeta_p]$ contains a unique quadratic field, which because it can only be ramified at p, must equal $\mathbb{Q}[\sqrt{p^*}]$, where $p^* = (-1)^{\frac{p-1}{2}} p$ (the sign is chosen so that $p^* \equiv 1 \mod 4$).

Second, note that $\zeta_8 = (1+i)/\sqrt{2}$, and so $\zeta_8 + \bar{\zeta}_8 = \sqrt{2}$. Therefore $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\zeta_8]$ (in fact, $\mathbb{Q}[\sqrt{2}]$ is the largest real subfield of $\mathbb{Q}[\zeta_8]$, and $\mathbb{Q}[\zeta_8] = \mathbb{Q}[i, \sqrt{2}]$).

Let n be the product of the odd primes dividing d (so $d = \pm n$ or $\pm 2n$). I claim that

$$\begin{aligned} \mathbb{Q}[\sqrt{d}] &\subset \mathbb{Q}[\zeta_n] \text{ if } d \equiv 1 \mod 4, \\ \mathbb{Q}[\sqrt{d}] &\subset \mathbb{Q}[\zeta_{4n}] \text{ if } d \equiv 3 \mod 4, \\ \mathbb{Q}[\sqrt{d}] &\subset \mathbb{Q}[\zeta_{8n}] \text{ if } d \equiv 2 \mod 4 \end{aligned}$$

and that, in each case, this is the smallest cyclotomic field containing $\mathbb{Q}[\sqrt{d}]$. For example, note that $d = p_1 \dots p_r$, $d \equiv 1 \mod 4$, implies that $d = p_1^* \cdots p_r^*$, and so $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_n]$. Also note that if d is even, then $\mathbb{Q}[\sqrt{d}]$ is not contained in $\mathbb{Q}[\zeta_{4n}]$ because otherwise $\mathbb{Q}[\zeta_{4n}]$ would contain i, $\sqrt{d}$, $\sqrt{d/2}$, and hence would contain i, $\sqrt{2}$, and ζ_8.

We conclude that the conductor of $\mathbb{Q}[\sqrt{d}]$ is $|\Delta_{K/\mathbb{Q}}|$ or $\infty|\Delta_{K/\mathbb{Q}}|$ depending on whether $d > 0$ or $d < 0$—here $\Delta_{K/\mathbb{Q}}$ is the discriminant of $K/\mathbb{Q}$.

[4] This follows from the description of the ray class group in 1.8(c) of the notes and the description of the Frobenius element in ANT, 8.18.

REMARK 3.12 For a finite abelian extension L/K and modulus $\mathfrak{m}$ with $S(\mathfrak{m})$ equal to the set of primes of K ramifying in L, let

$$T(L/K,\mathfrak{m}) = i(K_{\mathfrak{m},1})\cdot \mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) \subset I_K.$$

Takagi showed that for $\mathfrak{m}$ sufficiently divisible (in fact, for all $\mathfrak{m}$ divisible by the conductor $\mathfrak{f}$ of L/K), the group $T(L/K,\mathfrak{m})$ is independent of $\mathfrak{m}$ and $I_K^{S(\mathfrak{m})}/T(L/K,\mathfrak{m}) \approx \mathrm{Gal}(L/K)$. For this reason, $T(L/K,\mathfrak{m})$ is often called the ***Takagi group*** of L/K when $\mathfrak{f}|\mathfrak{m}$. Artin showed that the Takagi group is the kernel of the map $\mathfrak{a} \mapsto (\mathfrak{a}, L/K)$: $I_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$.

EXERCISE 3.13 Compute the conductor of $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ by applying the quadratic reciprocity law to find the smallest $\mathfrak{m}$ such that $i(\mathbb{Q}_{\mathfrak{m},1})$ is in the kernel of the Artin map (cf. Exercise 0.11).

The field L corresponding to a congruence subgroup H is called the ***class field*** of H, whence the name of the subject. Note that for a prime $\mathfrak{p}$ of K not dividing the conductor of L/K, the residue class degree $f(\mathfrak{P}/\mathfrak{p})$ for a prime lying over $\mathfrak{p}$ is the order of $\mathfrak{p}$ in $I^{\mathfrak{m}}/H$ (because this is the order of the Frobenius element in $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$). Thus we have obtained a classification of the abelian extensions of K in terms of the ideal structure of K, and for each abelian extension we know the decomposition laws of the primes in K.

EXERCISE 3.14 Verify the last row in the following table:

Discriminant	-15	-20	-23	-24	-31
Class number	2	2	3	2	3
Hilbert class field	X^2+3	X^2+1	X^3-X-1	X^2+3	X^3+X-1

The first row lists the discriminants of the first five imaginary quadratic fields with class number not equal to 1, the second row lists their class numbers, and the final row lists the minimal polynomial of a generator of the Hilbert class field. (Note that for a totally imaginary field, the class number and the narrow-class number coincide.)

[For example, the quadratic field with discriminant -24 is $\mathbb{Q}[\sqrt{-6}]$, and its Hilbert class field is $L = \mathbb{Q}[\sqrt{-6},\sqrt{-3}] = \mathbb{Q}[\sqrt{2},\sqrt{-3}]$. Thus $L = \mathbb{Q}[\alpha]$ with $\alpha = \sqrt{2}+\sqrt{-3}$, which has minimum polynomial X^4+2X^2+5. However, $\mathbb{Z}[\alpha]$ is not equal to the ring of integers in L; cf. mo122765.]

EXERCISE 3.15 This exercise explains what happens when we ignore a finite set S of prime ideals of K. Let $\mathfrak{m}$ be a modulus of K with $S(\mathfrak{m}) \cap S = \emptyset$, and let H be a subgroup of $I^{S\cup S(\mathfrak{m})}$ containing $i(K_{\mathfrak{m},1})$. Define an extension L of K to be an S-class field for H if

(a) L is a finite abelian extension of K, and the prime ideals in S split completely in L;

(b) $\mathfrak{m}(\mathfrak{p}) = 0 \Rightarrow \mathfrak{p}$ does not ramify in L;

(c) the prime ideals not in $S \cup S(\mathfrak{m})$ that split in L are precisely those in H.

Prove that an S-class field L exists for each group H as above, that it is unique, and that $I^{S\cup S(\mathfrak{m})}/H \simeq \mathrm{Gal}(L/K)$; moreover, every field L satisfying (a) is the S-class field for some H.

Hint: Show $I^{S\cup S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \simeq I^{S(\mathfrak{m})}/\langle S\rangle \cdot i(K_{\mathfrak{m},1})$, where $\langle S\rangle$ is the subgroup of $I^{S(\mathfrak{m})}$ generated by the primes in S.

The norm limitation theorem

In our classification of the abelian extensions of K, we attach to L the group $H = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})})$ for $\mathfrak{m}$ a modulus sufficiently large to be a defining modulus (and then $(I^{S(\mathfrak{m})} : H) = [L : K]$). One might hope that something similar works for nonabelian extensions, but the following theorem shows that it does not.

THEOREM 3.16 (NORM LIMITATION THEOREM) *Let L be a finite extension of K, and let L'/K be the maximal abelian subextension of L/K. For every defining modulus $\mathfrak{m}$ for L'/K,*

$$i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L'/K}(I_{L'}^{S(\mathfrak{m})}).$$

For example, if L is a cubic extension of K that is not Galois over K, then $L' = K$, and so

$$i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) = I_K^{S(\mathfrak{m})}.$$

The norm limitation theorem indicates that, for a nonabelian extension L/K, $\mathrm{Spl}(L/K)$ is not described by congruence conditions. For a proof of the norm limitation theorem, see, e.g., Grant and Leitzel 1969.

The principal ideal theorem

> *... à ma honte, je ne suis par arrivé à retrouver ce "corollaire" que tous les idéaux de K deviennent principaux dans la plus grande extension abélienne non ramifiée dans le fini. Si ça s'explique en deux mots, je t'en serais fort reconnaissant.*
> Grothendieck, letter to Serre, 19.9.1956.[5]

The following theorem was conjectured by Hilbert about 1900.

THEOREM 3.17 (PRINCIPAL IDEAL THEOREM) *Every ideal in K becomes principal in the Hilbert class field of K.*

I explain the idea of the proof. Recall that for a group G, the ***commutator*** (or ***derived***) subgroup G' of G is the subgroup generated by the commutators $ghg^{-1}h^{-1}$, $g, h \in G$. The quotient $G^{\mathrm{ab}} = G/G'$ is abelian, and it is the largest abelian quotient of G. If L is a Galois extension of K with Galois group G, then $L^{G'}$ is an abelian extension of K with Galois group G^{ab}, and it is the largest abelian extension of K contained in L.

[5] ... to my shame, I have been unable to find the "corollary" stating that all ideals of K become principal in the largest abelian extension unramified at the finite primes. If it can be explained in two words, I would be very grateful to you.

Serre responded:

> Enclosed is a little paper on the "Hauptidealsatz" explaining how the theorem can be reduced to an (actually very mysterious) theorem in group theory. This, in fact, is the reduction given by Artin himself in his paper on the subject (Abh. Hamburg, around volume 7–10); if you could find a beautiful cohomological proof of the theorem it would be so much better, but everyone has got stuck on it up to now.

See also the endnote to Serre's letter (Grothendieck and Serre 2001).

Suppose we have fields

$$L \supset K' \supset K$$

with L Galois over K (not necessarily abelian). For every finite set of primes S of K, $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{K'}$ is a homomorphism $I_K^S \to I_{K'}^S$. Consider:

$$\begin{array}{ccc} I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ \downarrow \text{canonical} & & \downarrow ? \\ I_{K'}^S & \xrightarrow{\psi_{L/K'}} & \mathrm{Gal}(L/K')^{\mathrm{ab}}. \end{array}$$

What is the map "?" making the diagram commute?

Before describing it, I need to explain a construction in group theory. Let H be a group of finite index in a group G, and write G as a disjoint union of cosets,

$$G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n.$$

For $g \in G$, set $\varphi(g) = g_i$ if $g \in Hg_i$, and define

$$V(g) = \prod_{i=1}^{n} g_i g \varphi(g_i g)^{-1} \mod H',$$

where H' is the commutator subgroup of H.

PROPOSITION 3.18 *The map $g \mapsto V(g)$ is a homomorphism $G \to H/H'$, and it is independent of the choice of the coset representatives g_i.*

PROOF. The verification is straightforward—see, for example, Hall 1959, 14.2.1. □

Thus, whenever we have a group G and a subgroup H of finite index, we have a well-defined homomorphism

$$V : G^{\mathrm{ab}} \to H^{\mathrm{ab}},$$

called the ***Verlagerung*** (or ***transfer***) map. Roughly speaking, we are trying to define a "norm" from G to H, which doesn't work because the groups are not abelian, but does work when we pass to the associated abelian groups.

In the situation of the above diagram, $\mathrm{Gal}(L/K')$ is a subgroup of $\mathrm{Gal}(L/K)$, and hence the Verlagerung is a homomorphism

$$V\colon \mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/K')^{\mathrm{ab}}.$$

Emil Artin showed that this is the map making the above diagram commute (cf. II, 3.2b).

Consider the fields

$$K'' \supset K' \supset K,$$

where K' is the Hilbert class field of K, and K'' is the Hilbert class field of K'. Then

(a) K'' is normal over K (because any conjugate of K'' is again an abelian unramified extension of K', and hence is contained in K'');

(b) K' is the largest abelian extension of K contained in K'' (because every abelian extension of K contained in K'' is unramified over K, and hence is contained in K').

From (b) we find that $\mathrm{Gal}(K''/K)^{\mathrm{ab}} = \mathrm{Gal}(K'/K)$. Therefore, when $L = K''$, the previous diagram becomes

$$\begin{array}{ccc} C_K & \xrightarrow{\simeq} & \mathrm{Gal}(K'/K) \\ \downarrow{\scriptstyle \text{canonical}} & & \downarrow{\scriptstyle \text{Ver}} \\ C_{K'} & \xrightarrow{\simeq} & \mathrm{Gal}(K''/K'), \end{array}$$

where C_K and $C_{K'}$ are the class groups of K and K'. Let $G = \mathrm{Gal}(K''/K)$ and let $H = \mathrm{Gal}(K''/K')$. Because of (b), H is the commutator subgroup of G. The next theorem (which was conjectured by Emil Artin) shows that V is zero in this situation, and hence that the canonical map $C_K \to C_{K'}$ is zero, i.e., that every ideal of K becomes principal in K'.

THEOREM 3.19 *Let G be a finite group, and let H be its commutator subgroup; then*

$$V\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$$

is zero.

PROOF. This is a theorem in group theory, also called the Principal Ideal Theorem. It was proved by Furtwängler in 1930. For a simple proof, see: Witt, Proc. International Congress of Mathematicians, Amsterdam, 1954, Vol 2, pp. 71–73. Also Zassehaus, Theory of Groups, V, Theorem 12, or Artin and Tate 1961, Chapter XII. □

REMARK 3.20 It is in fact easy to see that there exists an extension L of K of degree dividing the class number h of K such that every ideal in K becomes principal in L: write the class group of K as a direct sum of cyclic groups; choose a generator $\mathfrak{a}_i$ for each summand, and let h_i be the order of $\mathfrak{a}_i$ in the class group; write $\mathfrak{a}_i^{h_i} = (a_i)$, and define L to be the field obtained from K by adjoining an h_ith root of a_i for each i.

However, a field constructed in this fashion will not usually be the Hilbert class field of K—it need not even be Galois over K. There may exist fields of degree $< h$ over K in which every ideal in K becomes principal.

REMARK 3.21 Note that the principal ideal theorem says that "ideal" factorizations of elements in K become actual factorizations in the Hilbert class field L: let $a \in K$, and let $(a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$; then $\mathfrak{p}_i \mathcal{O}_L = (\pi_i)$ for some $\pi_i \in \mathcal{O}_L$, and so $a = u\pi_1^{r_1} \cdots \pi_s^{r_s}$ in $\mathcal{O}_L$.

REMARK 3.22 The principal ideal theorem does not, of course, imply that every ideal in the Hilbert class field K' of K is principal, because not every ideal of K' is in the image of the homomorphism $I_K \to I_{K'}$. One can form the Hilbert class field K'' of K', and so on, to obtain a tower

$$K \subset K' \subset K'' \subset \cdots \subset K^{(n)} \subset \cdots$$

in which $K^{(n+1)}$ is the Hilbert class field of $K^{(n)}$. For every automorphism τ of K^{al}, $\tau K^{(n+1)}$ is obviously the largest abelian unramified extension of $\tau K^{(n)}$, which implies that $\tau K' = K$, $\tau K'' = K''$, etc., and so on. In particular, $K^{(n)}$ is Galois over K. The class field tower problem (stated by Hasse in 1925) asks whether this tower is always finite, and so terminates in a field with class number one. The answer was shown to be negative by Golod and Shafarevich in 1964 (see Roquette 1967). For example, $\mathbb{Q}[\sqrt{-2.3.5.7.11.13}]$ has infinite class field. In fact, $\mathbb{Q}[\sqrt{d}]$ has an infinite class field tower whenever d has more than 8 prime factors.

The Chebotarev Density Theorem

Let L be a Galois extension of K with Galois group G. Recall that, for every prime ideal $\mathfrak{p}$ of K unramified in L,

$$(\mathfrak{p}, L/K) \stackrel{\text{def}}{=} \{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}$$

is a conjugacy class in G.

THEOREM 3.23 (CHEBOTAREV DENSITY THEOREM) *Let L/K be a finite extension of number fields with Galois group G, and let C be a conjugacy class in G. Then the set of prime ideals of K such that $(\mathfrak{p}, L/K) = C$ has density $|C|/|G|$ in the set of all prime ideals of K. In particular, if G is abelian, then, for a fixed $\tau \in G$, the set of prime ideals $\mathfrak{p}$ of K with $(\mathfrak{p}, L/K) = \tau$ has density $1/(G:1)$.*

PROOF. For an abelian extension L/K this follows from Theorem 2.5 and Theorem 3.5: the latter says that the map $\mathfrak{p} \mapsto (\mathfrak{p}, L/K)$ induces a surjective homomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ for some modulus $\mathfrak{m}$, and the former says that the primes are equidistributed among the classes in $C_{\mathfrak{m}}$. The nonabelian case is derived from the abelian case by an ingenious argument—see Chapter VIII □

COROLLARY 3.24 *If a polynomial $f(X) \in K[X]$ splits into linear factors modulo $\mathfrak{p}$ for all but finitely prime ideals $\mathfrak{p}$ in K, then it splits in $K[X]$.*

PROOF. Apply the theorem to the splitting field of $f(X)$. □

For a finite extension L/K of number fields and a finite set S of primes of K, let $\mathrm{Spl}_S(L/K)$ be the set of primes of K not in S that split in L.

THEOREM 3.25 *If L and M are Galois extensions of K, then*

$$L \subset M \iff \mathrm{Spl}_S(L/K) \supset \mathrm{Spl}_S(M/K).$$

Hence

$$L = M \iff \mathrm{Spl}_S(L/K) = \mathrm{Spl}_S(M/K).$$

PROOF. As a consequence of (1.12),

$$\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K).$$

Hence

$$\mathrm{Spl}_S(L/K) \supset \mathrm{Spl}_S(M/K) \Rightarrow \mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(M/K),$$

which, by the Chebotarev density theorem, implies

$$[LM : K] = [M : K],$$

and so $L \subset M$. The reverse implication is obvious. □

REMARK 3.26 (a) Theorem 3.25 is not true without the Galois assumption (see Cassels and Fröhlich 1967, p. 363).

(b) In the statement of Theorem 3.25, S can be replaced by any set of primes of density 0.

(c) Let $f(X)$ be an irreducible polynomial in $K[X]$. If $f(X)$ has a root modulo $\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$, then $f(X)$ has a root in K (Cassels and Fröhlich 1967, p. 363, 6.2).

(d) Chebotarev proved his theorem using Dirichlet (analytic) densities. Artin noted that it should hold for natural densities (see later), and, in fact, it does.

(e) Given a finite Galois extension K of $\mathbb{Q}$ and a conjugacy class C, Chebotarev's theorem says that there exists a prime ideal $\mathfrak{p}$ of K, unramified over $\mathbb{Q}$, such that $(\mathfrak{p}, L/K) = C$. It is interesting to know how big $\mathbb{N}\mathfrak{p}$ has to be. For a recent paper on this question, see Ahn, Jeoung-Hwan; Kwon, Soun-Hi. An explicit upper bound for the least prime ideal in the Chebotarev density theorem. Ann. Inst. Fourier (Grenoble) 69 (2019), no. 3, 1411–1458.

The conductor-discriminant formula

Two ***Dirichlet characters*** $\chi: I^S \to \mathbb{C}^\times$ and $\chi': I^{S'} \to \mathbb{C}^\times$ are said to be ***cotrained*** if they agree on $I^{S''}$ for some $S'' \supset S \bigcup S'$. This is an equivalence relation. In each equivalence class, there is a unique χ with smallest S—such a χ is said to be ***primitive.***

Let χ_1 be the primitive character equivalent to χ. The smallest modulus $\mathfrak{m}$ such that χ_1 is zero on $i(K_{\mathfrak{m},1})$ is called the ***conductor*** of $\mathfrak{f}(\chi)$ of χ. Set $\mathfrak{f}(\chi) = \mathfrak{f}_\infty(\chi)\mathfrak{f}_0(\chi)$, where $\mathfrak{f}_\infty$ and $\mathfrak{f}_0$ are respectively divisible only by infinite primes and finite primes.

THEOREM 3.27 (FÜHRERDISKRIMINANTENPRODUKTFORMEL) *For every finite abelian extension L/K of number fields with Galois group G,*

$$\operatorname{disc}(L/K) = \prod_{\chi \in G^\vee} \mathfrak{f}_0(\chi \circ \psi_{L/K}), \quad G^\vee \stackrel{\text{def}}{=} \operatorname{Hom}(G, \mathbb{C}^\times);$$
$$\mathfrak{f}(L/K) = \operatorname{lcm}_\chi \left(\mathfrak{f}(\chi \circ \psi_{L/K})\right).$$

Clearly $\bigcap \operatorname{Ker}(\chi: G \to \mathbb{C}^\times) = 0$, from which the second statement follows. We omit the proof of the first—it is really a statement about local fields.

REMARK 3.28 Let H be the kernel of the character χ. Then $\mathfrak{f}(\chi) = \mathfrak{f}(L^H/K)$. For example, if χ is injective, then $\mathfrak{f}(\chi) = \mathfrak{f}(L/K)$.

EXAMPLE 3.29 Let $L = \mathbb{Q}[\sqrt{d}]$. Then $G \simeq \mathbb{Z}/2\mathbb{Z}$, and there are only two characters $G \to \mathbb{C}^\times$, namely, the trivial character χ_0 an an injective character χ_1. Therefore, the theorem says that $\Delta_{K/\mathbb{Q}} = \mathfrak{f}_0(\chi_1) = \mathfrak{f}_0(K/\mathbb{Q})$, as we showed in Example 3.11.

EXAMPLE 3.30 Let $L = \mathbb{Q}[\zeta_p]$, p an odd prime. Then $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order $p-1$. It therefore has $p-2$ nontrivial characters. If χ is nontrivial, then $\mathfrak{f}(\chi)|\infty(p)$, but $\mathfrak{f}(\chi) = 1$ or ∞ is impossible (because it would imply χ is trivial). Therefore, $\mathfrak{f}(\chi) = (p)$ or $\infty(p)$ if χ is nontrivial, and so the conductor-discriminant formula shows (correctly) that $\Delta_{L/\mathbb{Q}} = \pm p^{p-2}$.

EXERCISE 3.31 Verify the conductor-discriminant formula for the extension $\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q}$.

REMARK 3.32 Let L/K be a finite extension of number fields with Galois group G (not necessarily abelian). To a representation $\rho: G \to \mathrm{GL}(V)$ of G on a finite-dimensional vector space V, Artin attaches a Dirichlet L-series $L(s, \rho)$ (see the introduction). The analytic properties of these ***Artin L-series*** are still not fully understood.

When G is commutative, the Artin map $I^S \to G$ identifies characters of G with Dirichlet/Weber characters, and hence Artin L-series with Dirichlet L-series. This was Artin's motivation for seeking the map (not, as seems natural today, in order to construct a *canonical* isomorphism between the groups $C_{\mathfrak{m}}$ and G, already known to be abstractly isomorphic).

A part of Langlands's philosophy is a vast generalization of this correspondence between Dirichlet L-series and abelian Artin L-series.

The reciprocity law and power reciprocity

Assume K contains a primitive nth root of 1, and let $a \in K$. If $\sqrt[n]{a}$ is one root of $X^n - a$, then the remaining roots are of the form $\zeta\sqrt[n]{a}$, where ζ is an nth root of 1. Therefore $L \stackrel{\text{def}}{=} K[\sqrt[n]{a}]$ is Galois over K, and $\sigma\sqrt[n]{a} = \zeta\sqrt[n]{a}$ for some nth root ζ of 1.

If $\mathfrak{p}$ is a prime ideal of K that is relatively prime to n and a, then $\mathfrak{p}$ is unramified in L, and we can define an nth root $(\frac{a}{\mathfrak{p}})_n$ of 1 by the formula

$$(\mathfrak{p}, L/K)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}.$$

One can show that

$$\left(\frac{a}{\mathfrak{p}}\right)_n = 1 \iff a \text{ is an } n\text{th power modulo } \mathfrak{p},$$

and so $(\frac{a}{\mathfrak{p}})_n$ generalizes the quadratic residue symbol. For this reason $\left(\frac{a}{\mathfrak{p}}\right)_n$ is called the ***power residue symbol.*** Artin's reciprocity law implies all known reciprocity laws for these symbols, and so, as Artin pointed out, it can be viewed as a generalization of them to fields without roots of unity. We shall explain this in Chapter VIII

An elementary unsolved problem

Let K be a number field, let S be a nonempty finite set of prime ideals of K, and let p be a prime number not divisible by any prime in S. Does there exist a sequence of fields $\ldots, L_n, L_{n+1}, \ldots$ such that

(a) L_n is unramified outside the primes of S;

(b) $p^n | [L_n : K]$?

A key case, for which the answer is unknown, is $K = \mathbb{Q}$ and $S = \{l\}$.

More explicitly (and slightly harder), fix primes $p \neq l$ in $\mathbb{Q}$. Does there exist a sequence of monic irreducible polynomials $f_n(X) \in \mathbb{Z}[X]$ such that

(a) $\operatorname{disc}(f_n(X))$ is not divisible by any prime other than l;

(b) $p^n | \deg f_n(X)$.

See Milne 2006, pp. 48–49, to find where this problem turned up. It is certainly very difficult.[6]

[6]Let K be a number field, let S be a set of primes of K, and let K_S be the largest extension of K unramified outside S. Let P be the set of prime numbers ℓ such that $\ell^\infty | [K_S : K]$. It is now known that P contains *all* prime numbers provided that S contains all the prime ideals of K lying over at least two primes in $\mathbb{Q}$. See Chenevier and Clozel, JAMS 22 (2009), 467–519, Cor. 5.2.

Explicit global class field theory: Kronecker's Jugentraum and Hilbert's twelfth problem

Unlike local class field theory, global class field theory does not (in general) provide an explicit construction of the abelian extensions of a number field K.

Gauss knew that the cyclotomic extensions of $\mathbb{Q}$ are abelian. Towards the end of the 1840s Kronecker had the idea that the cyclotomic fields, and their subfields, exhaust the abelian extensions of $\mathbb{Q}$, and furthermore, that every abelian extension of an imaginary quadratic number field E is contained in the extension given by adjoining to E roots of 1 and certain special values of the modular function j. Many years later he was to refer to this idea as the most cherished dream of his youth (mein liebster Jugendtraum).

More precisely, Kronecker's dream[7] is that every abelian extension of $\mathbb{Q}$ is contained in the field obtained by adjoining to $\mathbb{Q}$ all values of the function $e^{2\pi iz}$ for $z \in \mathbb{Q}^\times$, and that every abelian extension of an imaginary quadratic field K is contained in the field obtained by adjoining to K all values of the function $j(z)$ for $z \in K^\times$.

Later Hilbert took this up as the twelfth of his famous problems: for any number field K, find functions that play the same role for K that the exponential function plays for $\mathbb{Q}$ and the modular function j plays for an imaginary quadratic field[8]. The first part of Kronecker's dream, that every abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic extension, was proved by Weber (1886, 1899, 1907, 1911) and Hilbert (1896).

The statement above of "Kronecker's dream" is not quite correct. Let K be an imaginary quadratic field. We can write $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau$ with $\Im(\tau) > 0$. It is known that $K[j(\tau)]$ is the Hilbert class field of K. Now adjoin to K all roots of unity and all values $j(\tau)$ with $\tau \in K$, $\Im(\tau) > 0$. The resulting field K' is abelian over K, and $[K^{\mathrm{ab}} : K']$ is product of groups of order 2. To get the whole of K^{ab}, it is necessary to adjoin special values of other elliptic functions. These statements were partially proved Weber (1908) and Feuter (1914), and completely proved by Takagi (1920).

From the modern point of view, special values of elliptic modular functions are related to the arithmetic of elliptic curves with complex multiplication, and it is results about the latter that allow one to prove that the former generate abelian extension of an imaginary quadratic field.

Beginning with the work of Taniyama, Shimura, and Weil in the late fifties, the theory of elliptic curves and elliptic modular curves has been successfully generalized to higher dimensions. In this theory, an elliptic curve with complex multiplication by an imaginary quadratic field is replaced by an abelian variety with complex multiplication by a CM field, that is, a quadratic totally imaginary extension K of a totally real field F, and an elliptic modular function by an automorphic function.

Philosophically, one expects that, with the exception of $\mathbb{Q}$, one can not obtain abelian extensions of totally real fields by adjoining special values of automorphic functions. However, it is known that, roughly speaking, one does obtain the largest possible abelian extension of a CM-field K consistent with this restriction.

More precisely, let K be a CM-field and let F be the largest totally real subfield of K. Then $G \overset{\text{def}}{=} \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/K)$ is a subgroup of index 2 in $G' \overset{\text{def}}{=} \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/F)$, and the corresponding Verlagerung is a homomorphism $V : G'^{\mathrm{ab}} \to G^{\mathrm{ab}}$. In this case, V has a very simple description.

[7] For a careful account of Kronecker's idea and work on it, see Schappacher 1998

[8] See pp. 18-20 of Mathematical Developments arising from Hilbert's Problems, Proc. Symp. Pure Math. XXVIII, Part 1, AMS, 1976.

THEOREM 3.33 *Let K be a CM-field, and let F be the totally real subfield of K with $[K : F] = 2$. Let H be the image of the Verlagerung map*

$$\mathrm{Gal}(F^{\mathrm{al}}/F)^{\mathrm{ab}} \to \mathrm{Gal}(K^{\mathrm{al}}/K)^{\mathrm{ab}}.$$

Then the extension of K obtained by adjoining the special values of all automorphic functions defined on canonical models of Shimura varieties with rational weight is $(K^{\mathrm{ab}})^H \cdot \mathbb{Q}^{\mathrm{ab}}$.

PROOF. See Wei 1993, Wei 1994. □

Notes

The relation between congruence groups and abelian extensions of K was known before Artin defined his map. It emerged only slowly over roughly the period 1870–1920. The main contributors were Kronecker, Weber, Hilbert, and Takagi. Chebotarev proved his theorem in (1926) (a less precise result had been proved much earlier by Frobenius), and Artin defined his map and proved it gave an isomorphism in 1927. (Earlier, it had been known that $I^{\mathfrak{m}}/H \approx \mathrm{Gal}(L/K)$, but no *canonical* isomorphism was known.) The fact that analysis, in the form of Chebotarev's (or Frobenius's) theorem was required to prove the main theorems, which are purely algebraic in form, was regarded as a defect, and in 1940, after much effort, Chevalley succeeded in giving a purely algebraic proof of the main theorems. (The difficult point is proving that if L/K is an abelian extension of number fields of prime degree p, then *at least one* prime of K does not split or ramify in L.[9]) He also introduced idèles, which make it possible to state class field theory directly for infinite extensions. Group cohomology (at least 2-cocycles etc.) had been used implicitly in class field theory from the 1920s, but it was used systematically by Nakayama, Hochschild, and Tate in the 1950s. In 1951/52 in a very influential seminar, Artin and Tate gave a purely algebraic and very cohomological treatment of class field theory. Since then there have been important improvements in our understanding of local class field theory (mainly due to Lubin and Tate). Nonabelian class field theory is a part of Langlands's program, which is a vast interlocking series of conjectures, and some progress has been made, especially in the local case and the function field case. A fairly satisfactory abelian class field theory for more general fields (fields of finite transcendence degree over $\mathbb{Q}$ or $\mathbb{F}_p$) has been created by Bloch, Kato, Saito, and others. It uses algebraic K-theory (see Raskind 1995 for a survey and Wiesend 2007 for a recent result).

4 Idèles

Theorems 3.5 and 3.6 show that, for any number field K, there is a canonical isomorphism $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Rather than studying $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$ directly, it turns out to be more natural to introduce another group that has it as a quotient—this is the idèle class group.

[9] Class field theory holds also for fields that are finite extensions of $k(X)$ with k finite, and local class field theory holds for local fields whose residue fields k are only quasi-finite, i.e., perfect with $\mathrm{Gal}(k^{\mathrm{al}}/k) \simeq \hat{\mathbb{Z}}$. When one tries to do global class field theory for finite extensions of $k(X)$ with k *quasi-finite*, one finds that everything works except that, for some k, there *do* exist nontrivial abelian extensions in which every prime splits. See my book, Arithmetic Duality Theorems, Appendix to Chapter I.

Topological groups

A group G with a topology is called a ***topological group*** if the maps

$$g, g' \mapsto gg' : G \times G \to G, \quad g \mapsto g^{-1} : G \to G$$

are continuous. The translation map

$$g \mapsto ag : G \to G$$

is then a homeomorphism.

In general, to determine a topology on a set we have to give a fundamental system of neighbourhoods of each point, i.e., a set of neighbourhoods of the point such that every neighbourhood contains one in the set. Because the translation map is a homeomorphism, the topology on a topological group is determined by a fundamental system of neighbourhoods of 1.

We shall need to make use of various generalities concerning topological groups, which can be found in many books. Fortunately, we shall only need quite elementary things.

Let $(X_i)_i$ be a (possibly infinite) family of topological spaces. The product topology on $\prod X_i$ is that for which the sets of the form $\prod U_i$, U_i open in X for all i and equal to X_i for all but finitely many i, form a basis. Tychonoff's theorem says that a product of compact spaces is compact. However, an infinite product of locally compact spaces will not in general be locally compact: if V_i is a compact neighbourhood of x_i in X_i for all i, then $\prod V_i$ will be compact, but it will not be a neigbourhood of (x_i) unless $V_i = X_i$ for all but finitely many i.

Idèles

We now often write v for a prime of K. Then:

$$\begin{aligned}
|\cdot|_v &= \text{the normalized absolute value for } v \text{ (for which the product formula holds)},\\
K_v &= \text{the completion of } K \text{ at } v,\\
\mathfrak{p}_v &= \text{the corresponding prime ideal in } \mathcal{O}_K \text{ , (when } v \text{ is finite)},\\
\mathcal{O}_v &= \text{the ring of integers in } K_v,\\
U_v &= \mathcal{O}_v^\times\\
\hat{\mathfrak{p}}_v &= \text{the completion of } \mathfrak{p}_v = \text{ maximal ideal in } \mathcal{O}_v.
\end{aligned}$$

Recall that, for all v, K_v is locally compact—in fact, $\mathcal{O}_v$ is a compact neighbourhood of 0. Similarly $K_v^\times$ is locally compact; in fact

$$1 + \hat{\mathfrak{p}}_v \supset 1 + \hat{\mathfrak{p}}_v^2 \supset 1 + \hat{\mathfrak{p}}_v^3 \supset \cdots$$

is a fundamental system of neighbourhoods of 1 consisting of open compact subgroups.

We want to combine all the groups $K_v^\times$ into one big topological space, but $\prod K_v^\times$ is not locally compact. Instead we define the ***group of idèles*** to be[10]

$$\mathbb{I}_K = \{(a_v) \in \prod K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\}.$$

[10]Other notations for the idèles: $\mathbb{A}_K^\times$, $\mathrm{GL}_1(\mathbb{A}_K)$.

In the following, an unadorned $\mathbb{I}$ means $\mathbb{I}_K$.

For every finite set S of primes that includes all infinite primes, let

$$\mathbb{I}_S = \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times$$

with the product topology. The first factor is a finite product of locally compact spaces, and so is locally compact, and the second factor is a product of compact spaces, and so is compact (by Tychonoff). Hence $\mathbb{I}_S$ is locally compact. Note that

$$\mathbb{I} = \bigcup \mathbb{I}_S.$$

We want to endow $\mathbb{I}$ with a topology such that each $\mathbb{I}_S$ is open in $\mathbb{I}$ and inherits the product topology. We do this by decreeing that a basis for the open sets consists of the sets of the form $\prod_v V_v$ with V_v open in $K_v^\times$ for all v and $V_v = \mathcal{O}_v^\times$ for almost all[11] v. An intersection of two sets of this form contains a set of this form, and so they do form a basis for a topology. It is clear that the topology does have the property we want, and moreover that it endows $\mathbb{I}$ with the structure of a topological group. The following sets form a fundamental system of neighbourhoods of 1: for each finite set of primes $S \supset S_\infty$ and $\varepsilon > 0$, define

$$U(S,\varepsilon) = \{(a_v) \mid |a_v - 1|_v < \varepsilon, \quad v \in S, \quad |a_v|_v = 1, \quad \text{all } v \notin S\}.$$

4.1 There is a canonical surjective homomorphism id

$$(a_v) \mapsto \prod_{v \text{ finite}} p_v^{\operatorname{ord}_p(a_v)} : \mathbb{I}_K \to I_K$$

whose kernel is $\mathbb{I}_{S_\infty}$.

We can think of the idèles as a thickening of the ideals: it includes factors for the infinite primes, and it includes the units at the finite primes. Note that $\mathbb{I}/\mathbb{I}_{S_\infty}$ is a direct sum of countably many copies of $\mathbb{Z}$ with the discrete topology, but that $\prod K_v^\times/\mathbb{I}_{S_\infty}$ is a direct *product* of countably many copies of $\mathbb{Z}$, which is itself uncountable.

4.2 There is a canonical injective (diagonal) homomorphism

$$a \mapsto (a,a,a,\ldots): K^\times \to \mathbb{I}_K.$$

I claim that the image is discrete. Because we have groups, it suffices to prove that $1 \in K^\times$ is open in the induced topology. Let $U = U(S,\varepsilon)$ with S any finite set containing S_∞ and $1 > \varepsilon > 0$. For every $a \in K^\times \cap U$,

$$\begin{cases} |a-1|_v < \varepsilon & \text{for all } v \in S \\ |a|_v = 1 & \text{for all } v \notin S. \end{cases}$$

The second condition implies that

$$|a-1|_v \le \max(|a|_v, |-1|_v) \le 1.$$

Therefore, if $a \in K^\times \cap U$, then $\prod_v |a-1|_v < \varepsilon^{|S|} < 1$, which contradicts the product formula unless $a = 1$.

[11] Here "almost all" means "for all but possibly finitely many".

The quotient $\boldsymbol{C} = \mathbb{I}/K^\times$ is called the ***idèle class group*** of K. It maps onto the ideal class group of K. It is not compact (see (4.4) below).

4.3 There is a canonical injective homomorphism

$$a \mapsto (1, \dots, 1, a, 1, \dots 1) \colon K_v^\times \to \mathbb{I}_K$$

(a in the vth place). The topology induced on $K_v^\times$ is its natural topology, because

$$U(S,\varepsilon) \cap K_v^\times = \begin{cases} \{a \mid |a-1|_v < \varepsilon\} & v \in S \\ \{a \mid |a|_v = 1\} & v \notin S \end{cases}$$

and such sets form a fundamental system of neighbourhoods of 1 in $K_v^\times$.

4.4 There is canonical surjective homomorphism

$$\mathbf{a} = (a_v) \mapsto c(\mathbf{a}) = \prod |a_v|_v : \mathbb{I} \to \mathbb{R}_{>0}.$$

The image of $\mathbf{a}$ is called the ***content*** of $\mathbf{a}$. Define

$$\mathbb{I}^1 = \operatorname{Ker}(c) = \{\mathbf{a} \in \mathbb{I} \mid c(\mathbf{a}) = 1\}.$$

Note that, because of the product formula, $K^\times \subset \mathbb{I}^1$. The quotient $\mathbb{I}/K^\times$ can't be compact because it maps surjectively onto $\mathbb{R}_{>0}$, but one can prove that $\mathbb{I}^1/K^\times$ is compact.

ASIDE 4.5 Define $\mathbb{I}_f$ the same way as $\mathbb{I}$, except using only the finite primes. We call $\mathbb{I}_f$ the ***group of finite idèles.*** We have

$$\prod_{v \text{ finite}} \mathcal{O}_v^\times \subset \mathbb{I}_f \subset \prod_{v \text{ finite}} K_v^\times.$$

The subgroup $\prod \mathcal{O}_v^\times$ is open and compact in $\mathbb{I}_f$, and $\mathbb{I}_f / \prod \mathcal{O}_v^\times = I$ (the group of ideals of K).

Again there is a diagonal embedding of $K^\times$ into $\mathbb{I}_f$, but this time the induced topology on $K^\times$ has the following description: $U_K \overset{\text{def}}{=} \mathcal{O}_K^\times$ is open, and a fundamental system of neighbourhoods of 1 is formed by the subgroups of U_K of finite index (nontrivial theorem).[12] In particular, $K^\times$ is a discrete subgroup of $\mathbb{I}_f \iff U_K$ is finite $\iff K = \mathbb{Q}$ or an imaginary quadratic field.

NOTES The adèlic topology does not induce the idèlic topology on the idèles (because $\prod_{v|\infty} K_v^\times \times \prod_{v \text{ finite}} \mathcal{O}_v^\times$ is not open in the adèles). As an exercise, show that the idèles are not even a topological group under the induced topology. (Consider first the case of $\mathbb{Q}$, and forget about the infinite prime. (a) Make sure you understand what the standard basis for the neighbourhoods of 0 in the adèles is. (b) Translate the neighbourhoods in (a) by adding 1, and intersect with the idèles to get a base for the neighbourhoods of 1 in the idèles for the adelic topology. (c) Check that the pre-image of one of the neighbourhoods in (b) under the map $x \mapsto x^{-1}$ is not open.)

[12] Copied from sx140729. For the first claim: The subset of the finite idèles given by $\prod_v \mathcal{O}_{K_v}^\times$ is open by the definition of the topology on the restricted direct product, and an element in $K^\times$ is in this subset if and only if it is a unit in each completion, which is true if and only if it is in $\mathcal{O}_K^\times$.

The proof of the second claim is just a generalization of this first argument. A basis of open neighborhoods of 1 in the finite idèles is given by choosing any open subgroup you wish in $K_v^\times$ for finitely many primes v and choosing $\mathcal{O}_v^\times$ for the remaining v. If we just want a basis of open subsets, we may as well only look at really small ones, so we can assume that, for the finitely many primes v where we did not choose $\mathcal{O}_v^\times$, we chose some small open subset of $\mathcal{O}_v^\times$. Note that subgroups of $\mathcal{O}_v^\times$ are all finite index and generated by a power of a prime element. Note also that all these open subsets of the idèles are subsets of the one we discussed in checking the first claim.

What happens when we intersect such a neighbourhood with the diagonal image of $K^\times$? We get the subgroup of elements in $\mathcal{O}_K^\times$ which are in all the open subgroups of $\mathcal{O}_v^\times$ that we chose at the special places v. The index is just the product of the indices of those subgroups, so that's a finite index subgroup. Conversely, any finite index subgroup of $\mathcal{O}_K^\times$ is determined by its images in each completion.

NOTES Let $(V_v, U_v)_v$ be a family of topological spaces V_v, each equipped with a subspace U_v. The ***restricted product*** of the family, $\prod(V_v, U_v)$, is the subset of $\prod V_v$ consisting of the families (a_v) such that $a_v \in U_v$ for almost all v.It is equipped with the topology for which $\prod U_v$ is open and has the product topology. Sometimes the restricted product is written $\prod' V_v$. Now $\mathbb{A}_K = \prod_v (K_v, U_v)$, where $U_v = \mathcal{O}_v$ if v is finite and $U_v = K_v$ otherwise. Similarly, $\mathbb{A}_K^\times = \prod_v (K_v^\times, U_v^\times)$, where $U_v = \mathcal{O}_v^\times$ if v is finite and $U_v = K_v^\times$ otherwise.

NOTES Give more examples. Let K be a field with class number 1. Let $x = (x_v)$ be an idèle. Then the ideal of x is principal, say, equal to (a). Now $x/a \in \prod_{\text{finite}} \mathcal{O}_v^\times \times K_\infty^\times$. Hence $\mathbb{A}_K^\times = K^\times \cdot \prod_{\text{finite}} \mathcal{O}_v^\times \times K_\infty^\times$. However, $K^\times \cap (\prod_{\text{finite}} \mathcal{O}_v^\times \times K_\infty^\times) = U_K$.

NOTES Copied from sx80763. Question from Princeton's generals: What results do the major compactness theorems about adeles and ideles imply? Answer: The finiteness of the ideal class group and the units theorem (proven with classical methods) prove the compactness of the norm-one idèle class group, and the compactness of the norm-one idèle class group, proven using measure theoretic methods proves finiteness of the ideal class group and the units theorem. (See Cassels 1967.) On the other hand, the compactness result does generalize to division algebras, where there is not an obvious version of the ideal class group, etc. (See Weil's Basic Number Theory.)

Realizing ray class groups as quotients of $\mathbb{I}$

We have seen that the class group $C_K = I/i(K^\times)$ can be realized as the quotient of $\mathbb{I}$. We want to show the same for $C_\mathfrak{m}$.

Let $\mathfrak{m}$ be a modulus. For $\mathfrak{p}|\mathfrak{m}$, set

$$W_\mathfrak{m}(\mathfrak{p}) = \begin{cases} \mathbb{R}_{>0} & \mathfrak{p} \text{ real} \\ 1 + \hat{\mathfrak{p}}^{m(\mathfrak{p})} & \mathfrak{p} \text{ finite.} \end{cases}$$

Thus, in each case, $W_\mathfrak{m}(\mathfrak{p})$ is a neighbourhood of 1 in $K_\mathfrak{p}^\times$.

Define $\mathbb{I}_\mathfrak{m}$ to be the set of idèles $(a_\mathfrak{p})_\mathfrak{p}$ such that $a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p})$ for all $\mathfrak{p}|\mathfrak{m}$:

$$\mathbb{I}_\mathfrak{m} = \left(\prod_{\mathfrak{p}\nmid\mathfrak{m}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \right) \bigcap \mathbb{I}.$$

In other words, $\mathbb{I}_\mathfrak{m}$ consists of the families $(a_\mathfrak{p})_\mathfrak{p}$ indexed by the primes of K such that

$$\begin{cases} a_\mathfrak{p} \in K_\mathfrak{p}^\times & \text{for all } \mathfrak{p} \\ a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times & \text{for almost all } \mathfrak{p} \\ a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p}) & \text{for all } \mathfrak{p}|\mathfrak{m}. \end{cases}$$

Define $W_\mathfrak{m}$ to be the set of idèles $(a_\mathfrak{p})_\mathfrak{p}$ in $\mathbb{I}_\mathfrak{m}$ such that $a_\mathfrak{p}$ is a unit for all finite $\mathfrak{p}$ not dividing $\mathfrak{m}$:

$$W_\mathfrak{m} = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p} \text{ infinite}}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \times \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p} \text{ finite}}} U_\mathfrak{p}.$$

In other words, $W_\mathfrak{m}$ consists of the families $(a_\mathfrak{p})_\mathfrak{p}$ indexed by the primes of K such that

$$\begin{cases} a_\mathfrak{p} \in K_\mathfrak{p}^\times & \text{for all infinite } \mathfrak{p} \\ a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times & \text{for all finite } \mathfrak{p} \\ a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p}) & \text{for all } \mathfrak{p}|\mathfrak{m}. \end{cases}$$

Note that

$$K_{\mathfrak{m},1} = K^\times \cap \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \qquad \text{(intersection inside } \prod_{\mathfrak{p}|\mathfrak{m}} K_{\mathfrak{p}}^\times),$$

and that

$$K_{\mathfrak{m},1} = K^\times \cap \mathbb{I}_{\mathfrak{m}} \qquad \text{(intersection inside } \mathbb{I}).$$

PROPOSITION 4.6 *Let $\mathfrak{m}$ be a modulus of K.*

(a) *The map* $\mathrm{id}\colon \mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})}$ *defines an isomorphism*

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} \xrightarrow{\simeq} C_{\mathfrak{m}}.$$

(b) *The inclusion* $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}$ *defines an isomorphism:*

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathbb{I}/K^\times.$$

PROOF. (a) Consider the pair of maps

$$K_{\mathfrak{m},1} \to \mathbb{I}_{\mathfrak{m}} \xrightarrow{\mathrm{id}} I^{S(\mathfrak{m})}.$$

The first map is injective, and the second is surjective with kernel $W_{\mathfrak{m}}$, and so the kernel-cokernel sequence (II, A.2) of the pair of maps is

$$W_{\mathfrak{m}} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to 1.$$

The proves (a) of the proposition.

(b) The kernel of $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}/K^\times$ is $K^\times \cap \mathbb{I}_{\mathfrak{m}}$ (intersection in $\mathbb{I}$) which, we just saw, is $K_{\mathfrak{m},1}$. Hence the inclusion defines an injection

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \hookrightarrow \mathbb{I}/K^\times.$$

For the surjectivity, we apply the weak approximation theorem (ANT, 7.20). Let $S = S(\mathfrak{m})$ and let $\mathbf{a} = (a_v) \in \mathbb{I}$. If we choose $b \in K$ to be very close to a_v in $K_v^\times$ for all $v \in S$, then a_v/b will be close to 1 in $K_v^\times$ for all $v \in S$; in fact, we can choose b so that $a_v/b \in W_{\mathfrak{m}}(\mathfrak{p})$ for all $v \in S$. For example, for a real prime v in S, we need only choose b to have the same sign as a_v in K_v. Then $\mathbf{a}/b \in \mathbb{I}_{\mathfrak{m}}$, and it maps to $\mathbf{a}$ in $\mathbb{I}/K^\times$. □

Characters of ideals and of idèles

Let $S \supset S_\infty$ be a finite set of primes of K, and let G be a finite abelian group. A homomorphism

$$\psi\colon I^S \to G$$

is said to ***admit a modulus*** if there exists a modulus $\mathfrak{m}$ with support in S such that $\psi(i(K_{\mathfrak{m},1})) = 1$. For example, for every abelian extension L/K, Artin showed that the Artin map

$$I^S \to \mathrm{Gal}(L/K)$$

admits a modulus.

PROPOSITION 4.7 *If $\psi: I^S \to G$ admits a modulus, then there exists a unique homomorphism $\phi: \mathbb{I} \to G$ such that*

(a) *ϕ is continuous (G with the discrete topology)*

(b) *$\phi(K^\times) = 1$;*

(c) *$\phi(\mathbf{a}) = \psi(\mathrm{id}(\mathbf{a}))$, all $\mathbf{a} \in \mathbb{I}^S \overset{\text{def}}{=} \{\mathbf{a} \mid a_v = 1 \text{ all } v \in S\}$.*

Moreover, every continuous homomorphism $\phi: \mathbb{I} \to G$ satisfying (b) arises from a ψ.

PROOF. Because ψ admits a modulus $\mathfrak{m}$, it factors through $I^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) = C_{\mathfrak{m}}$. Hence we have the diagram:

$$\begin{array}{ccccc} & & I^{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} \xrightarrow{\psi} G \\ & & & & \simeq\uparrow \\ & & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} & \longrightarrow & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} \\ & & \downarrow\simeq & & \\ \mathbb{I} & \longrightarrow & \mathbb{I}/K^\times. & & \end{array} \tag{43}$$

The isomorphisms are those in Proposition 4.6, and the remaining unnamed maps are quotient maps. Define ϕ to be the composite $\mathbb{I} \to G$. It certainly has properties (a) and (b), and it also has the property that

$$\phi(\mathbf{a}) = \psi(\mathrm{id}(\mathbf{a})) \text{ for all } \mathbf{a} \in \mathbb{I}_{\mathfrak{m}},$$

and so, *a fortiori,* it has property (c).

To prove that the map is uniquely determined by (a), (b), and (c), it suffices to prove that $\mathbb{I}^S K^\times$ is dense in $\mathbb{I}$, but this follows from the weak approximation theorem (ANT, 7.20): let $\mathbf{a} \in \mathbb{I}$; choose $b \in K^\times$ to be very close to a_v for $v \in S$, and let $\mathbf{a}'$ be the element of $\mathbb{I}^S$ such that $a'_v b = a_v$ for all $v \notin S$. Then $\mathbf{a}'b \in \mathbb{I}^S \cdot K$ and is close to $\mathbf{a}$ in $\mathbb{I}$.

For the converse, let $\phi: \mathbb{I} \to G$ be a continuous map. The kernel contains an open neighbourhood of 1, and so $U(S, \varepsilon) \subset \mathrm{Ker}(\phi)$ for some S and ε. Consider an infinite prime v. The restriction of ϕ to $K_v^\times$ is a continuous map $\mathbb{R}^\times \to G$ or $\mathbb{C}^\times \to G$. Clearly, the connected component of $K_v^\times$ containing 1, namely, $\mathbb{R}_{>0}$ or $\mathbb{C}^\times$, maps to 1, and so is in the kernel. On combining these remarks, we see that the kernel of ϕ contains $W_{\mathfrak{m}}$ for some $\mathfrak{m}$.

Now we can use the diagram at the start of the proof again. We are given a homomorphism $\phi: \mathbb{I}/K^\times \to G$, which we can "restrict" to a homomorphism $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to G$. This homomorphism is trivial on $W_{\mathfrak{m}}$, and hence factors through $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}}$. The homomorphism can now be transferred to $C_{\mathfrak{m}}$, and composed with $\mathbb{I} \twoheadrightarrow C_{\mathfrak{m}}$. This is the ψ we are looking for. □

REMARK 4.8 Let G be a commutative topological group. Define a homomorphism $\psi: I^S \to G$ to be ***admissible*** if for every neighbourhood N of 1 in G, there exists a modulus $\mathfrak{m}$ such that $\psi(i(K_{\mathfrak{m},1})) \subset N$. Then every admissible homomorphism ψ defines a homomorphism $\phi: \mathbb{I} \to G$ satisfying conditions (a), (b), (c) of the proposition. Moreover, if G is complete and has "no small subgroups" i.e., there exists a neighbourhood of 1 containing no nontrivial subgroup, then every continuous homomorphism $\phi: \mathbb{I} \to G$ satisfying (b) arises from an

admissible ψ. The proof is the same as that of the proposition (see Proposition 4.1 of Tate 1967).

The circle group $G = \{z \in \mathbb{C} \mid |z| = 1\}$ is complete and has no small subgroups. The admissible $\psi: I^S \to G$, and the corresponding ϕ, are called ***Hecke characters.***

REMARK 4.9 Given ψ we chose an $\mathfrak{m}$, and then showed how to construct ϕ. In practice, it is more usually more convenient to identify ϕ directly from knowing that it satisifies the conditions (a), (b), (c). For this, the following observations are useful.

(a) Let $\mathbf{a} = (a_v)$ be an idèle such that $a_v = 1$ for all finite primes and $a_v > 0$ for all real primes; then $\phi(\mathbf{a}) = 1$. To see this, note that the topology induced on $\prod_{v|\infty} K_v^\times$ as a subgroup of $\mathbb{I}$ is its natural topology. Therefore, the restriction of ϕ to it is trivial on the connected component containing 1.

(b) Let $\mathbf{a} = (a_v)$ be an idèle such that $a_v = 1$ for all $v \in S$ and a_v is a unit for all $v \notin S$; then $\phi(\mathbf{a}) = 1$. In fact, this follows directly from condition (c).

(c) If $\mathbf{a}$ is "close to 1", $\phi(\mathbf{a}) = 1$. In fact, this follows directly from condition (a) in view of the fact that G has the discrete topology.

(d) On combining (a), (b), (c), we find that if $\mathbf{a} = (a_v)$ is such that

$$\begin{cases} a_v > 0 \text{ when } v \text{ is real;} \\ a_v \text{ is "close to 1 " when } v \in S \text{ is finite;} \\ a_v \text{ is a unit when } v \notin S \end{cases}$$

the $\phi(\mathbf{a}) = 1$. In fact, (a) and (b) say that we can multiply $\mathbf{a}$ with idèles of certain types without changing the value $\phi(\mathbf{a})$. Clearly, if a_v is close to 1 for the finite v in S, we can multiply it by such idèles to make it close to 1.

EXAMPLE 4.10 Let $L = \mathbb{Q}[\zeta_p]$, and let ψ be the Artin map

$$I^S \to (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q}), \quad S = \{p, \infty\}.$$

Recall that first map sends the ideal (uniquely) represented by (r/s), $r, s > 0$, $(p, r) = 1 = (p, s)$, to $[r][s]^{-1}$, and that the second sends $[m]$ to the automorphism $\zeta \mapsto \zeta^m$. Overall, for any prime number $l \neq p$, the map sends (l) to the Frobenius automorphism at l, $\zeta \mapsto \zeta^l$. Let $\phi: \mathbb{I} \to \mathrm{Gal}(L/\mathbb{Q})$ be the homomorphism corresponding to ψ as in the theorem. We wish to determine ϕ explicitly.

Let $\mathbf{a} = (a_\infty, a_2, \dots, a_p, \dots, a_l, \dots)$ be an idèle of $\mathbb{Q}$. If $a_\infty = 1 = a_p$, then $\phi(\mathbf{a}) = \psi(\mathrm{id}(\mathbf{a}))$. Thus $\phi(\mathbf{a}) = \zeta_p^m$, where $m = \prod l^{\mathrm{ord}_l(a_l)}$.

Consider $\mathbf{p} = (1, \dots, 1, p, 1, \dots)$ (p in the p-position). Then

$$\mathbf{p}/p = (p^{-1}, \dots, p^{-1}, 1, p^{-1}, \dots).$$

According to (d) of the above Remark, $\phi(\mathbf{p}/p) = 1$, and so

$$\phi(\mathbf{p}) = \phi(\mathbf{p}/p)\phi(p) = 1.$$

In this, p denotes both the element $p \in \mathbb{Q}_p$ and the principal idèle $(p, p, \dots)$.

Consider $\mathbf{a} = (1, \dots, 1, u, 1, \dots)$, $u \in \mathbb{Z}_p^\times$, u in the p-position. Write

$$u^{-1} = a_0 + a_1 p + \cdots + a_s p^s + \cdots, \quad 0 \le a_i < p, \quad a_i \in \mathbb{Z},$$

and let $c = a_0 + \cdots + a_s p^s \in \mathbb{Z}$. Note that $c > 0$. Then $uc \in 1 + p^{s+1}\mathbb{Z}_p$, i.e., for large s it is "close to 1". Write

$$\mathbf{a}c = (c, c, \dots, c, \overset{l|c}{1}, c, \dots, \overset{p}{uc}, c, \dots)(1, \dots, 1, \overset{l|c}{c}, 1, \dots).$$

The first factor is $\mathbf{a}c$ except that we have moved the components at the primes l dividing c to the second factor. For large s, $\phi($ first factor$) = 1$ by (d) of the above remark. The second factor lies in $\mathbb{I}^S$, and the description we have of $\phi|\mathbb{I}^S$ shows that $\phi($ second factor$)$ maps ζ to ζ^c. In conclusion,

$$\phi(\mathbf{a})(\zeta) = \zeta^c = \zeta^{u^{-1}}. \tag{44}$$

Consider $\mathbf{a} = (-1, 1, \dots, 1)$. Then

$$-\mathbf{a} = (1, -1, \dots, -1, \overset{p}{1}, -1, \dots)(1, \dots, 1, \overset{p}{-1}, 1, \dots),$$

and

$$\phi(\mathbf{a}) = \phi(-\mathbf{a}) = \phi(1, \dots, 1, -1, 1, \dots).$$

According (44), $\phi(\mathbf{a})(\zeta) = \zeta^{-1}$.

Because ϕ is a homomorphism, this completes the explicit description of it.

REMARK 4.11 From (43), we get a canonical homomorphism $\pi_{\mathfrak{m}}\colon \mathbb{I} \to C_{\mathfrak{m}}$. This is the unique continuous homomorphism $\pi_{\mathfrak{m}}\colon \mathbb{I} \to C_{\mathfrak{m}}$ such that

(a) $\pi_{\mathfrak{m}}(K^\times) = 1$;

(b) $\pi_{\mathfrak{m}}(\mathbf{a}) = \mathrm{id}(\mathbf{a})$ for all $\mathbf{a} \in \mathbb{I}^{S(\mathfrak{m})}$.

(Take ψ to be $I^S \to C_{\mathfrak{m}}$ in Proposition 4.7.).

If $\mathfrak{m}|\mathfrak{m}'$, then the composite of $\pi_{\mathfrak{m}'}$ with the canonical homomorphism $C_{\mathfrak{m}'} \to C_{\mathfrak{m}}$ satisfies the conditions characterizing $\pi_{\mathfrak{m}}$. Therefore, the $\pi_{\mathfrak{m}}$ combine to give a continuous homomorphism $\pi\colon \mathbb{I} \to \varprojlim C_{\mathfrak{m}}$. We wish to determine the kernel and image of this map.

Because each map $\pi_{\mathfrak{m}}\colon \mathbb{I} \to C_{\mathfrak{m}}$ is onto, the image is dense. In fact, $\mathbb{I}^1 \to C_{\mathfrak{m}}$ is onto, and so $\pi_{\mathfrak{m}}(\mathbb{I}^1)$ is dense. But $\pi_{\mathfrak{m}}(\mathbb{I}^1)$ is compact, because $\pi_{\mathfrak{m}}$ factors through the compact group $\mathbb{I}^1/K^\times$, and therefore is complete. This shows that π is onto.

Let $\mathbb{I}_\infty^+$ be the set of idèles $\mathbf{a}$ such that $a_v = 1$ if v is finite and $a_v > 0$ if v is real. Thus $\mathbb{I}_\infty^+$ is isomorphic to the identity component of $(K \otimes_{\mathbb{Q}} \mathbb{R})^\times = \prod_{v|\infty} K_v^\times$. The kernel of $\mathbb{I} \to \varprojlim C_{\mathfrak{m}}$ contains $\mathbb{I}_\infty^+ \cdot K^\times$, and hence its closure. In fact, it equals it. [In a future version, these things will be examined in more detail.]

Norms of idèles

Let L be a finite extension of the number field K, let v be a prime of K. Recall from (ANT, 8.2) that there is a canonical isomorphism

$$L \otimes_K K_v \to \prod_{w|v} L_w.$$

It follows (ibid. 8.3) that for any $\alpha \in L$,

$$\mathrm{Nm}_{L/K}\,\alpha = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}\,\alpha \qquad \text{(equality in } K_v\text{)}.$$

For an idèle $\mathbf{a} = (a_w) \in \mathbb{I}_L$, define $\mathrm{Nm}_{L/K}(\mathbf{a})$ to be the idèle $\mathbf{b} \in \mathbb{I}_K$ with $b_v = \prod_{w|v} \mathrm{Nm}_{L_w/K_v} a_w$. The preceding remark shows that the left hand square in the following diagram commutes, and it is easy to see that the right hand square commutes:

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{\mathrm{id}} & I_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\mathrm{id}} & I_K. \end{array}$$

Thus we get a commutative diagram:

$$\begin{array}{ccc} \boldsymbol{C}_L & \longrightarrow & C_L \\ \downarrow{\scriptstyle \mathrm{Nm}\, L/K} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ \boldsymbol{C}_K & \longrightarrow & C_K \end{array}$$

($\boldsymbol{C}_K$ = idèle class group $\mathbb{I}/K^\times$; C_K =ideal class group $I/i(K^\times)$).

PROPOSITION 4.12 *If L/K is a finite extension of local fields of characteristic zero, then*

(a) $\mathrm{Nm}_{L/K}(L^\times) = \mathbb{R}_{>0}$ *(case $K = \mathbb{R}$, $L = \mathbb{C}$);*

(b) $\mathrm{Nm}_{L/K}(L^\times) \supset 1 + \mathfrak{p}_K^m$ *for some m (case K is nonarchimedean);*

(c) $\mathrm{Nm}_{L/K}(L^\times) \supset \mathcal{O}_K^\times$ *(case K is nonarchimedean and L/K is unramified).*

PROOF. Statement (a) is obvious. For (b), see (I 1.3), and for (c), see (III, 1.2). □

COROLLARY 4.13 *Let L/K be a finite extension of number fields. Then $\mathrm{Nm}_{L/K}\mathbb{I}_L \supset W_\mathfrak{m}$ for some modulus $\mathfrak{m}$.*

5 The Main Theorems in Terms of Idèles

The statement of the main theorems of class field theory in terms of ideals is very explicit and, for many purposes, it is the most useful one. However, it has some disadvantages. One has to fix a modulus $\mathfrak{m}$, and then the theory describes only the abelian extensions whose conductor divides $\mathfrak{m}$. In particular, it provides no description of the infinite abelian extensions of K. The statement of the main theorems in terms of idèles allows one to consider infinite abelian extensions, or, what amounts to the same thing, all finite abelian extensions simultaneously. It also makes transparent the relation between the local and global Artin maps.

Let L be a finite abelian extension of K. Let v be a prime of K, and let w be a prime of L lying over v. Recall that the decomposition group $D(w)$ of w is the subgroup

$$D(w) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma w = w\}.$$

Its elements extend uniquely to automorphisms of L_w/K_v, and $D(w) \simeq \mathrm{Gal}(L_w/K_v)$. Local class field theory (I, 1.1) provides us with a homomorphism (the local Artin map)

$$\phi_v \colon K_v^\times \to D(w) \subset G.$$

LEMMA 5.1 *The subgroup $D(w)$ of G and the map ϕ_v are independent of the choice of the prime $w|v$.*

PROOF. Any other prime lying over v is of the form σw for some $\sigma \in G$, and $\sigma: L \to L$ extends by continuity to a homomorphism $\sigma: L_w \to L_{\sigma w}$ fixing K_v. We have

$$D(\sigma w) = \sigma D(w)\sigma^{-1},$$

which equals $D(w)$ because G is commutative.

Let Ω and Ω' be maximal abelian extensions of K_v containing L_w and $L_{\sigma w}$ respectively. From Chapter III, we obtain local Artin maps $\phi_v: K^\times \to \mathrm{Gal}(\Omega/K_v)$ and $\phi'_v: K^\times \to \mathrm{Gal}(\Omega'/K_v)$. The choice of an isomorphism $\tilde{\sigma}: \Omega \to \Omega'$ determines an isomorphism

$$\rho \mapsto \tilde{\sigma} \circ \rho \circ \tilde{\sigma}^{-1}: \mathrm{Gal}(\Omega/K_v) \to \mathrm{Gal}(\Omega'/K_v)$$

which is independent of $\tilde{\sigma}$. Moreover, its composite with ϕ_v is ϕ'_v (because it satisfies the conditions characterizing ϕ'_v). □

PROPOSITION 5.2 *There exists a unique continuous homomorphism $\phi_K: \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the following property: for any $L \subset K^{\mathrm{ab}}$ finite over K and any prime w of L lying over a prime v of K, the diagram*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\mathbf{a}\mapsto\phi_K(\mathbf{a})|L} & \mathrm{Gal}(L/K) \end{array}$$

commutes.

PROOF. Let $\mathbf{a} \in \mathbb{I}$, and let $L \subset K^{\mathrm{ab}}$ be finite over K. If $a_v \in U_v$ and L_w/K_v is unramified, the $\phi_v(a_v) = 1$ (see III, 1). Therefore, $\phi_v(a_v) = 1$ except for finitely many v's, and so we can define

$$\phi_{L/K}(\mathbf{a}) = \prod_v \phi_v(a_v).$$

(product inside $\mathrm{Gal}(L/K)$). Clearly, $\phi_{L/K}$ is the unique homomorphism making the above diagram commute.

If $L' \supset L$, then the properties of the local Artin maps show that $\phi_{L'/K}(\mathbf{a})|L = \phi_{L/K}(\mathbf{a})$. Therefore there exists a unique homomorphism $\phi: \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that $\phi(\mathbf{a})|L = \phi_{L/K}(\mathbf{a})$ for all $L \subset K^{\mathrm{ab}}$, L finite over K.

Again, the properties of the local Artin maps show that, for any fields $K \subset K' \subset L \subset K^{\mathrm{ab}}$ with L finite over K,

$$\begin{array}{ccc} \mathbb{I}_{K'}^S & \xrightarrow{\phi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow \mathrm{Nm} & & \downarrow \\ \mathbb{I}_K^S & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

commutes. On taking $K' = L$, we find that $\mathrm{Nm}_{L/K}(\mathbb{I}_L^S)$ is contained in the kernel of $\phi_{L/K}$. In particular, the kernel of $\phi_{L/K}$ contains an open subgroup of $\mathbb{I}_K^S$ (Corollary 4.13), and this implies that ϕ_K is continuous. □

THEOREM 5.3 (RECIPROCITY LAW) *The homomorphism $\phi_K: \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ has the following properties:*

(a) $\phi_K(K^\times) = 1$;

(b) *for every finite abelian extension L of K, ϕ_K defines an isomorphism*

$$\phi_{L/K}\colon \mathbb{I}_K/(K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K).$$

We saw in the proof of the proposition that $\phi_{L/K}(\mathrm{Nm}(\mathbb{I}_L)) = 1$, and so (assuming (a) of the theorem) we see that $\phi_{L/K}$ does factor through $\mathbb{I}_K/K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)$. Part (b) can also be stated as: ϕ defines an isomorphism

$$\phi_{L/K}\colon \boldsymbol{C}_K/\mathrm{Nm}(\boldsymbol{C}_L) \to \mathrm{Gal}(L/K).$$

EXAMPLE 5.4 Statement (a) of the theorem says that, for every $b \in K^\times$, $\prod \phi_v(b) = 1$. On applying this to the extension $K[a^{\frac{1}{n}}]/K$ under the assumption that K contains a primitive nth root of 1, one obtains the product formula for the Hilbert symbol:

$$\prod_v (a,b)_v = 1.$$

See (III, 4.8).

THEOREM 5.5 (EXISTENCE THEOREM) *Fix an algebraic closure K^{al} of K; for every open subgroup $N \subset \boldsymbol{C}_K$ of finite index, there exists a unique abelian extension L of K contained in K^{al} such that $\mathrm{Nm}_{L/K} \boldsymbol{C}_L = N$.*

A subgroup of $\boldsymbol{C}_K$ is a ***norm group*** if it is of the form $\mathrm{Nm}(\boldsymbol{C}_L)$ for some finite abelian extension L of K. The existence theorem shows that the norm groups are exactly the open subgroups of finite index in $\boldsymbol{C}_K$. If N is such a group, then the finite abelian extension L of K such that $\mathrm{Nm}(\boldsymbol{C}_L) = N$, i.e., such that $N = \mathrm{Ker}(\phi_{L/K})$, is called the ***class field of K belonging to N***.

As stated, the Existence Theorem is valid for all global fields.

COROLLARY 5.6 *The map $L \mapsto \mathrm{Nm}(\boldsymbol{C}_L)$ is a bijection from the set of finite abelian extensions of K to the set of open subgroups of finite index in $\boldsymbol{C}_K$. Moreover,*

$$\begin{aligned} L_1 \subset L_2 &\iff \mathrm{Nm}(\boldsymbol{C}_{L_1}) \supset \mathrm{Nm}(\boldsymbol{C}_{L_2});\\ \mathrm{Nm}(\boldsymbol{C}_{L_1 \cdot L_2}) &= \mathrm{Nm}(\boldsymbol{C}_{L_1}) \cap \mathrm{Nm}(\boldsymbol{C}_{L_2});\\ \mathrm{Nm}(\boldsymbol{C}_{L_1 \cap L_2}) &= \mathrm{Nm}(\boldsymbol{C}_{L_1}) \cdot \mathrm{Nm}(\boldsymbol{C}_{L_2}). \end{aligned}$$

REMARK 5.7 (a) In the number field case, the map

$$\phi_K\colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

is surjective. For an infinite prime v of K, write K_v^+ for the connected component of $K_v^\times$ containing 1; thus K_v^+ is isomorphic to $\mathbb{C}^\times$ or $\mathbb{R}_{>0}$ according as v is complex or real. Clearly $\prod_{v|\infty} K_v^+ \subset \mathrm{Ker}(\phi_K)$. By definition $K^\times \subset \mathrm{Ker}(\phi_K)$, and so $K^\times \cdot (\prod_{v|\infty} K_v^+) \subset \mathrm{Ker}(\phi_K)$. But ϕ_K is a continuous homomorphism and $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is Hausdorff, and so the kernel is a *closed* subgroup. Thus $\mathrm{Ker}(\phi_K)$ contains the closure of $K^\times \cdot (\prod_{v|\infty} K_v^+)$. It is a theorem that this is precisely the kernel. The image of the closure of $K^\times \cdot (\prod_{v|\infty} K_v^+)$ in $\boldsymbol{C}_K$ is the connected component of $\boldsymbol{C}_K$ containing 1.

For every finite abelian extension L of K, the Artin map defines an isomorphism $C_K/\mathrm{Nm}(C_L) \to \mathrm{Gal}(L/K)$. When we pass to the inverse limit over L, we get an isomorphism with $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on the right, so the problem is to compute the inverse limit

of the system $C_K/\mathrm{Nm}(C_L)$. The existence theorem shows that the groups $\mathrm{Nm}(C_L)$ are exactly the open subgroups of finite index, so this is a problem in topology.

(b) In the function field case, the Artin map $\phi_K\colon \mathbb{I}_K/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is injective, but it is not surjective (its image is dense).

REMARK 5.8 Assume that the global Artin map $\phi\colon \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ contains $K^\times$ in its kernel. Then, for every finite abelian extension L/K, $\phi_{L/K}\colon \mathbb{I} \to \mathrm{Gal}(L/K)$ arises (as in Proposition 4.7) from a homomorphism $\psi\colon I^S \to \mathrm{Gal}(L/K)$ admitting a modulus. Moreover, because ϕ is the product of the local Artin maps, ψ must be the ideal-theoretic global Artin map (which therefore admits a modulus). It is a straightforward exercise to derive Theorems 3.5 and 3.6 from their idèlic counterparts, Theorems 5.3 and 5.5. We shall prove Theorems 5.3 and 5.5 in Chapter VII

NOTES In his 1951 report Sur la théorie du corps de classes, Weil wrote:[13]

> La recherche d'une interprétation de C_k si k est un corps de nombres, analogue en quelque manière à l'interprétation par un groupe de Galois quand k est un corps de fonctions, me semble constituer l'un des problèmes fondamentaux de la théorie des nombres à l'heure actuelle; il se peut qu'une telle interprétation renferme la clef de l'hypothèse de Riemann...

For a discussion of this, see mo41296.

Example

LEMMA 5.9 *The map*

$$(r,t,(u_p)) \mapsto (rt, ru_2, ru_3, ru_5, \ldots)\colon \mathbb{Q}^\times \times \mathbb{R}_{>0} \times \prod \mathbb{Z}_p^\times \to \mathbb{I}_\mathbb{Q}$$

is an isomorphism of topological groups ($\mathbb{Q}^\times$ with the discrete topology).

PROOF. Any idèle $\mathbf{a} = (a_\infty, a_2, \ldots, a_p, \ldots)$ can be written

$$\mathbf{a} = a(t, u_2, u_3, u_5, \ldots), \quad a \in \mathbb{Q}^\times, \quad t \in \mathbb{R}_{>0}, \quad u_p \in \mathbb{Z}_p^\times;$$

—take $a = (\mathrm{sign}(a_\infty)) \prod p^{\mathrm{ord}_p(a_p)}$, $t = a_\infty/a$, $u_p = a_p/a$. Moreover, the expression is unique because the only positive rational number that is a p-adic unit for all p is 1.

The subsets

$$\{1\} \times U \times \prod_{p \text{ finite}} U_p$$

with U, U_p open neighbourhoods of 1 in $\mathbb{R}^\times, \mathbb{Q}_p^\times$, and $U_p^\times = \mathbb{Z}_p^\times$ for all but finitely many p's, form a fundamental system of neighbourhoods 1 on the left, and also on the right. □

Thus there is a canonical isomorphism of topological groups

$$\boldsymbol{C}_\mathbb{Q} \to \mathbb{R}_{>0} \times \prod_{p \text{ finite}} \mathbb{Z}_p^\times = \mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times.$$

[13] The search for an interpretation of C_k when k is a number field, in some way analogous to its interpretation as a Galois group when k is a function field, seems to me to be one of the fundamental problems of number theory at present; perhaps such an interpretation contains the key to the Riemann hypothesis...

Let

$$\mathbb{Q}^{\mathrm{cyc}} = \bigcup \mathbb{Q}[\zeta_n].$$

In this case, the global reciprocity map is the reciprocal of

$$\phi\colon \mathbb{I}_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}),$$

where $\mathbb{I}_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ is the above projection map, and $\hat{\mathbb{Z}}^{\times} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$ is the canonical isomorphism (see I A.5c).

SUMMARY 5.10 Let K be an algebraic number field. There exists a continuous surjective homomorphism (the reciprocity or Artin map)

$$\phi_K\colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that, for every finite extension L of K contained in K^{ab}, ϕ_K gives rise to a commutative diagram

$$\begin{array}{ccc} \mathbb{I}_K/K^{\times} & \xrightarrow{\ \phi_K\ } & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \big\downarrow & & \big\downarrow{\scriptstyle \tau\mapsto\tau|L} \\ \mathbb{I}_K/\left(K^{\times}\cdot \mathrm{Nm}(\mathbb{I}_L)\right) & \xrightarrow[\simeq]{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

It is determined by the following two properties:

(a) $\phi_{L/K}(u) = 1$ for every $u = (u_v) \in \mathbb{I}_K$ such that

i) if v is unramified in L, then u_v is a unit,

ii) if v is ramified in L, then u_v is sufficiently close to 1 (depending only on L/K), and

iii) if v is real but becomes complex in L, then $u_v > 0$.

(b) For every prime v of K unramified in L, the idèle

$$\alpha = (1, \dots, 1, \underset{v}{\pi}, 1, \dots), \quad \pi \text{ a prime element of } \mathcal{O}_v,$$

maps to the Frobenius element $(\mathfrak{p}_v, L/K)$ in $\mathrm{Gal}(L/K)$.

To see that there is at most one map satisfying these conditions, let $\alpha \in \mathbb{I}_K$, and use the weak approximation theorem to choose an $a \in K^{\times}$ that is close to α_v for all primes v that ramify in L or become complex. Then $\alpha = au\beta$ with u an idèle as in (a) and β a finite product of idèles as in (b). Now $\phi_{L/K}(\alpha) = \phi_{L/K}(\beta)$, which can be computed using (b).

For $K = \mathbb{Q}$, the Artin map factors through $\{\pm\} \times \mathbb{I}_f/\mathbb{Q}^{\times}$, and every element of this quotient is uniquely represented by an element of $\hat{\mathbb{Z}}^{\times} \subset \mathbb{I}_f$. In this case, we get the diagram

$$\begin{array}{ccccc} \hat{\mathbb{Z}}^{\times} & \xrightarrow[\simeq]{\ \phi_{\mathbb{Q}}\ } & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) & = & \bigcup_m \mathbb{Q}[\zeta_m] \\ \big\downarrow & & \big\downarrow{\scriptstyle \text{restrict}} & & \\ (\mathbb{Z}/m\mathbb{Z})^{\times} & \xrightarrow[\simeq]{[n]\mapsto(\zeta_m\mapsto\zeta_m^n)} & \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q}). & & \end{array}$$

which *commutes with an inverse.* This can be checked by writing an idèle α in the form $au\beta$ as above, but it is more instructive to look at an example. Let p be a prime not dividing m, and let

$$\alpha = p \cdot (1, \dots, 1, \underset{p}{p^{-1}}, 1, \dots) \in \mathbb{Z} \cdot \mathbb{I}_f = \mathbb{I}_f.$$

Then

$$\alpha = (p, \ldots, p, \underset{p}{1}, p, \ldots) \in \hat{\mathbb{Z}}^\times$$

has image $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, which acts as $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q})$ on $\mathbb{Q}[\zeta_m]$. On the other hand, $\phi_{\mathbb{Q}}(\alpha) = \phi_{\mathbb{Q}}((1, \ldots, 1, \underset{p}{p^{-1}}, 1, \ldots))$, which acts as $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q})^{-1}$.

EXERCISE 5.11 Show that, even when K is a number field, the idèle class group of K has subgroups of finite index that are not open.

Chapter VI

L-Series and the Density of Primes

Euler used the Riemann zeta function in rudimentary form to prove that there are infinitely many prime numbers. In order to prove that the primes are equally distributed among the different arithmetic progressions modulo m, Dirichlet attached L-series (regarded as functions of a real variable) to a character of $(\mathbb{Z}/m\mathbb{Z})^\times$. Riemann initiated the study of the Riemann zeta function as a function of a complex variable. In this section, we shall (following Weber) extend Dirichlet methods to the study of the distribution of the prime ideals among the classes in a ray class group. Except for the definition of the ray class group, this chapter is independent of the preceding chapters.

In this chapter, we shall need to use a little complex analysis. Recall that the power series $1 + z + \frac{z^2}{2!} + \cdots$ converges for all $z \in \mathbb{C}$ to a holomorphic function, which is denoted e^z. For every positive real number n and complex number z, n^z is defined to be $e^{(\log n)z}$, where log is the natural log (function $\mathbb{R}_{>0} \to \mathbb{R}$ inverse to e^r).

1 Dirichlet series and Euler products

A ***Dirichlet series*** is a series of the form

$$f(s) = \sum_{n \geq 1} \frac{a(n)}{n^s} \qquad a(n) \in \mathbb{C}, \quad s = \sigma + it \in \mathbb{C}.$$

An ***Euler product*** belonging to a number field K is a product of the form

$$g(s) = \prod_{\mathfrak{p}} \frac{1}{(1 - \theta_1(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}) \cdots (1 - \theta_d(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s})}, \quad \theta_i(\mathfrak{p}) \in \mathbb{C}, \quad s \in \mathbb{C},$$

in which $\mathfrak{p}$ runs over all but finitely many of the prime ideals of $\mathcal{O}_K$.

EXAMPLE 1.1 (a) The ***Riemann zeta function*** is

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}.$$

It is known that the behaviour of $\zeta(s)$, especially in the critical strip $0 \leq \Re(s) \leq 1$, is related to the distribution of the prime numbers.

(b) The ***Dedekind zeta function.*** For every number field K,

$$\zeta_K(s) = \sum_{\mathfrak{a}\geq 0} \frac{1}{\mathbb{N}\mathfrak{a}^s} = \prod_{\mathfrak{p}} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}}.$$

Here $\mathbb{N}\mathfrak{a} = (\mathcal{O}_K : \mathfrak{a})$. The sum is over the integral ideals in $\mathcal{O}_K$, and the product is over the prime ideals in $\mathcal{O}_K$.

(c) A ***Dirichlet character*** is[1] a homomorphism

$$\chi\colon I^{\mathfrak{m}} \to \mathbb{C}^\times$$

whose kernel contains $i(K_{\mathfrak{m},1})$ for some modulus $\mathfrak{m}$, i.e., χ is a character of the ray class group $C_{\mathfrak{m}}$. For such a character, the corresponding ***Dirichlet L-series*** is

$$L(s,\chi) = \sum_{\mathfrak{a}\subset\mathcal{O}_K,\,(\mathfrak{m},\mathfrak{a})=1} \frac{\chi(\mathfrak{a})}{\mathbb{N}\mathfrak{a}^s} = \prod_{(\mathfrak{m},\mathfrak{p})=1} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}}.$$

(d) A ***Hecke character*** (or ***Grössen character***) is a continuous homomorphism

$$\psi\colon \mathbb{I}_K/K^\times \to \mathbb{C}^\times$$

with image in the unit circle. If it is 1 on the identity components of $\mathbb{I}_K$ at the infinite primes, then it factors through $C_{\mathfrak{m}}$ for some $\mathfrak{m}$, and is a Dirichlet character; conversely, a Dirichlet character defines a Hecke character with discrete image. A Hecke character will take the value 1 on some set $\prod_{v\notin S} U_v$ (S a finite set of primes containing the infinite primes), and the corresponding ***Hecke L-series*** is

$$L_S(s,\psi) = \prod_{v\notin S} \frac{1}{1-\psi(\boldsymbol{\pi}_v)\mathbb{N}\mathfrak{p}_v^{-s}},$$

where $\boldsymbol{\pi}_v$ is an idèle with a prime element in the v-position and 1 elsewhere.

(e) Let L be a finite Galois extension of K with Galois group G. Let V be a finite dimensional vector space over $\mathbb{C}$ and let

$$\rho\colon G \to \mathrm{GL}(V)$$

be a homomorphism of G into the group of linear automorphisms of V. We refer to ρ as a ***(finite-dimensional) representation of*** G. The ***trace*** of ρ is the map sending σ to the trace of the automorphism $\rho(\sigma)$ of V. For $\sigma \in G$, let

$$P_\sigma(T) \overset{\text{def}}{=} \det(1-\rho(\sigma)T \mid V) = \prod_{i=1}^{\dim V} (1-a_i(\sigma)T), \qquad a_i \in \mathbb{C},$$

be the characteristic polynomial of $\rho(\sigma)$. Because $P_\sigma(T)$ depends only on the conjugacy class of σ, for every prime $\mathfrak{p}$ of K unramified in L, we can define $P_{\mathfrak{p}}(T)$ to be the characteristic polynomial of $(\mathfrak{P}, L/K)$ for any prime $\mathfrak{P}$ of L dividing $\mathfrak{p}$. The ***Artin L-series*** attached to ρ is

$$L(s,\rho) = \prod_{\mathfrak{p}} \frac{1}{P_{\mathfrak{p}}(\mathbb{N}\mathfrak{p}^{-s})} = \prod_{\mathfrak{p}} \frac{1}{(1-a_1(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s})\cdots(1-a_{\dim V}(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s})}$$

(product over all unramified primes of K; $a_i(\mathfrak{p}) = a_i((\mathfrak{P}, L/K))$).

[1] In the case $K = \mathbb{Q}$ and $\mathfrak{m} = \infty(m)$, so that $C_{\mathfrak{m}} = (\mathbb{Z}/m\mathbb{Z})^\times$, these characters and L-series were introduced by Dirichlet. For arbitary ray class groups, they were introduced by Weber. Some authors (including sometimes this one) restrict the terms "Dirichlet character" and "Dirichlet L-series" to the case $\mathbb{Q}$ and refer to the more general objects as "Weber characters" and "Weber L-series". Dirichlet used L to denote his L-functions, and the letter has been used ever since.

2 Convergence Results

We study the elementary analytic properties of Dirichlet series and Euler products.

Dirichlet series

PROPOSITION 2.1 *Let*

$$f(s) = \sum_{n\geq 1} \frac{a(n)}{n^s}.$$

Write $S(x) = \sum_{n\leq x} a(n)$, *and suppose that there exist positive constants* a *and* b *such that* $|S(x)| \leq ax^b$ *for all large* x. *Then the series* $f(s)$ *converges uniformly for* s *in*

$$D(b,\delta,\varepsilon) = \{\Re(s) \geq b+\delta, \quad |\arg(s-b)| \leq \frac{\pi}{2} - \varepsilon\}$$

for all $\delta, \varepsilon > 0$, *and it converges to an analytic function on the half plane* $\Re(s) > b$.

PROOF. Since every point s with $\Re(s) > b$ has a neighbourhood of the form $D(b,\delta,\varepsilon)$, the second part of the statement follows from the first. To prove the first, we use Cauchy's criterion for uniform convergence. For large integers $n_1 < n_2$,

$$\begin{aligned}
\left|\sum_{n=n_1}^{n_2} \frac{a(n)}{n^s}\right| &= \left|\sum_{n_1}^{n_2} \frac{s(n)-s(n-1)}{n^s}\right| \\
&= \left|\sum_{n_1}^{n_2} \frac{s(n)}{n^s} - \sum_{n_1-1}^{n_2-1} \frac{s(n)}{(n+1)^s}\right| \\
&= \left|\frac{s(n_2)}{n_2^s} - \frac{s(n_1-1)}{n_1^s} + \sum_{n_1}^{n_2-1} s(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| \\
&\leq \frac{|s(n_2)|}{n_2^\sigma} + \frac{|s(n_1-1)|}{n_1^\sigma} + \sum_{n_1}^{n_2-1} |s(n)| \left|s\int_n^{n+1} \frac{dt}{t^{s+1}}\right| \\
&\leq \frac{a}{n_2^{\sigma-b}} + \frac{a}{n_1^{\sigma-b}} + \sum_{n_1}^{n_2-1} |s| a n^b \left|\int_n^{n+1} \frac{dt}{t^{s+1}}\right| \\
&\leq \frac{2a}{n_1^{\sigma-b}} + \sum_{n_1}^{n_2-1} |s| a \left|\int_n^{n+1} \frac{t^b dt}{t^{s+1}}\right| \\
&\leq \frac{2a}{n_1^{\sigma-b}} + |s| a \int_{n_1}^{\infty} \frac{dt}{t^{\sigma+1-b}} \\
&\leq \frac{2a}{n_1^{\sigma-b}} - \frac{|s|a}{\sigma-b} \frac{1}{t^{\sigma-b}}\Big|_{n_1}^{\infty} \\
&\leq \frac{2a}{n_1^{\sigma-b}} + \frac{|s|a}{(\sigma-b)n_1^{\sigma-b}}.
\end{aligned}$$

But for $s \in D(b,\delta,\varepsilon)$,

$$\frac{|s|}{\sigma-b} = \frac{|s-b+b|}{\sigma-b} \leq \frac{|s-b|}{\sigma-b} + \frac{b}{\sigma-b} = \frac{1}{\cos\theta} + \frac{b}{\sigma-b} \leq \frac{1}{\cos\theta} + \frac{b}{\delta}$$

with $\theta = \arg(s-b)$. Now because $|\theta| \le \frac{\pi}{2} - \varepsilon$, $\frac{1}{\cos\theta}$ is bounded by some number M, and so

$$\left| \sum_{n=n_1}^{n_2} \frac{a(n)}{n^s} \right| \le \frac{2a}{n_1^{\sigma-b}} + \frac{(M + \frac{b}{\delta})a}{n_1^{\sigma-b}}.$$

The right hand side of this equation tends to zero as $n_1 \to \infty$, and so we can apply Cauchy's criterion to deduce the uniform convergence of $f(s)$. □

REMARK 2.2 (a) For the Dirichlet series $\zeta(s)$, $S(x)$ is $[x]$, and so the series of $\zeta(s)$ converges for $\Re(s) > 1$. For $\zeta_K(s)$, $S(x)$ is the number of integral ideals in K with numerical norm $\le x$. It is obvious that $S(x)$ is finite, but in fact (see 2.8 below) $S(x) \le Cx$. Therefore the series for ζ_K (and for $L(s,\chi)$) converge for $\Re(s) > 1$. (It is also possible to show directly that the Euler products converge for $\Re(s) > 1$, which implies that the Dirichlet series converge. See Fröhlich and Taylor 1991, VIII, 2.2.)

(b) Let $f(s) = \sum \frac{a(n)}{n^s}$ be a Dirichlet series with $a(n) \ge 0$. If $f(s)$ converges for all s with $\Re(s) > b$, but does not converge on the half-plane $\{s \mid \Re(s) > b - \varepsilon\}$ for any $\varepsilon > 0$, then $f(s) \to \infty$ as $s \to 1$ through real numbers > 1. i.e., the domain of convergence of $f(s)$ is limited by a singularity of f situated on the real axis. (See Serre 1970, III, 2.3.) For example, the series for $\zeta(s)$ does not converge on any half-plane $\Re(s) > 1 - \varepsilon$, $\varepsilon > 0$, and, as we shall see, $\zeta(s)$ does have a pole at $s = 1$.

LEMMA 2.3 *The zeta function $\zeta(s)$ has an analytic continuation to a meromorphic function on $\Re(s) > 0$ with its only (possible) pole at $s = 1$.*

PROOF. Define

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

For this Dirichlet series, $S(x) = 0$ or 1, and so $\zeta_2(s)$ is analytic for $s > 0$. Note that

$$\left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots\right) - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \cdots\right) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots,$$

that is,

$$\zeta(s) - \frac{2}{2^s}\zeta(s) = \zeta_2(s),$$

or

$$\zeta(s) = \frac{\zeta_2(s)}{1 - 2^{1-s}}.$$

Thus $\zeta(s)$ is analytic for $\Re(s) > 0$ except possibly for poles where $2^{s-1} = 1$. But

$$2^{s-1} = 1 \iff e^{(\log 2)(s-1)} = 1 \iff (\log 2)(s-1) = 2k\pi i,$$

and so $\zeta(s)$ is analytic except possibly at

$$s = 1 + \frac{2k\pi i}{\log 2}, \quad k \in \mathbb{Z}.$$

In fact, the only possible pole is $s = 1$. To see this, define

$$\zeta_3(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots$$

and observe (as for $\zeta_2(s)$) that $\zeta_3(s)$ is analytic for $s > 0$, and

$$\zeta(s) = \frac{\zeta_3(s)}{1 - 3^{1-s}}.$$

Hence $\zeta(s)$ is analytic for $s > 0$, except possibly for poles at

$$s = 1 + \frac{2k\pi i}{\log 3}.$$

Thus, at a pole for $\zeta(s)$, we must have

$$\frac{2k\pi i}{\log 2} = \frac{2k'\pi i}{\log 3},$$

or

$$2^{k'} = 3^k, \qquad k, k' \in \mathbb{Z}.$$

Because of unique factorization, this is possible only if $k = 0 = k'$. □

LEMMA 2.4 *For s real and $s > 1$,*

$$\frac{1}{s-1} \le \zeta(s) \le 1 + \frac{1}{s-1}.$$

Hence $\zeta(s)$ has a simple pole at $s = 1$ with residue 1, i.e.,

$$\zeta(s) = \frac{1}{s-1} + \textit{ function holomorphic near } 1.$$

PROOF. Fix an $s > 1$, s real. By examining the graph of $y = x^{-s}$, one finds that

$$\int_1^\infty x^{-s}\,dx \le \zeta(s) \le 1 + \int_1^\infty x^{-s}\,dx.$$

But

$$\int_1^\infty x^{-s}\,dx = \frac{x^{1-s}}{1-s}\bigg|_1^\infty = \frac{1}{s-1},$$

which gives the inequalities. Because $\zeta(s)$ is meromorphic near $s = 1$,

$$\zeta(s) = \frac{c}{(s-1)^m} + \frac{g(s)}{(s-1)^{m-1}}$$

near $s = 1$ for some $m \in \mathbb{N}$, $c \in \mathbb{C}$, and $g(s)$ holomorphic near $s = 1$. The inequalities imply that $m = 1$ and $c = 1$. □

PROPOSITION 2.5 *Let $f(s)$ be a Dirichlet series for which there exist real constants C and b, $b < 1$, such that*

$$|S(n) - a_0 n| \le C n^b.$$

Then $f(s)$ extends to a meromorphic function on $\Re(s) > b$ with a simple pole at $s = 1$ with residue a_0, i.e., near $s = 1$

$$f(s) = \frac{a_0}{s-1} + \textit{ holomorphic function}$$

near $s = 1$.

PROOF. For the Dirichlet series $f(s) - a_0\zeta(s)$, we have $|S(n)| \le Cn^b$, and therefore $f(s) - a_0\zeta(s)$ converges for $\Re(s) > b$. □

Euler products

Recall that an infinite product $\prod_{n=1}^{\infty}(1+b_n)$, $b_n \in \mathbb{C}$, $b_n \neq -1$, is said to ***converge*** if the sequence of partial products

$$\Pi_m = \prod_{n=1}^{m}(1+b_n)$$

converges to a nonzero value. Moreover, the product is said to ***converge absolutely*** if $\prod_{n=1}^{\infty} 1+|b_n|$ converges. A product $\prod_{n=1}^{\infty} 1+b_n$ converges if it converges absolutely, in which case, any reordering of the product converges (absolutely) to the same value.

LEMMA 2.6 *The product $\prod_1^{\infty} 1+b_n$ converges absolutely if and only if the series $\sum b_n$ converges absolutely.*

PROOF. We may suppose that $b_n \geq 0$ for all n. Then both $\Pi_m \overset{\text{def}}{=} \prod_1^m 1+b_n$ and $\Sigma_m \overset{\text{def}}{=} \sum_1^m b_n$ are monotonically increasing sequences. Since $\Pi_m \geq \Sigma_m$, it is clear that Σ_m converges if Π_m does. For the converse, note that

$$e^{\Sigma_m} = \prod_{i=1}^{m} e^{b_i} \geq \prod_{i=1}^{m}(1+b_i) = \Pi_m$$

and so, if the sequence Σ_m converges, then the sequence Π_m is bounded above, and therefore also converges. □

Recall that a product of finite sums, say,

$$\left(\sum_{i=1}^{l} a_i\right)\left(\sum_{i=1}^{m} b_i\right)\left(\sum_{i=1}^{n} c_i\right)$$

is a sum

$$\sum_{\substack{1\leq i\leq l\\ 1\leq j\leq m\\ 1\leq k\leq n}} a_i b_j c_k$$

of products, each of which contains exactly one term from each sum. Recall also that

$$\frac{1}{1-t} = 1 + t + t^2 + \cdots, \qquad |t| < 1.$$

Hence (formally at least),

$$\begin{aligned}\prod_p \frac{1}{1-p^{-s}} &= (1+2^{-s}+(2^2)^{-s}+\cdots)(1+3^{-s}+(3^2)^{-s}+\cdots)(1+5^{-s}+(5^2)^{-s}+\cdots)\cdots\\ &= \sum n^{-s}\end{aligned}$$

because each positive integer can be written as a product of powers of primes in exactly one way. This identity is sometimes referred to as the analytic form of unique factorization. We now *prove* a more general result.

PROPOSITION 2.7 *Let χ be a Dirichlet character of a number field K. For all s with $\Re(s) > 1$, the Euler product $\prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}}$ converges to $L(s,\chi)$.*

PROOF. For $\Re(s) > 1$,

$$\frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}} = 1 + \frac{\chi(\mathfrak{p})}{\mathbb{N}\mathfrak{p}^{s}} + \frac{\chi(\mathfrak{p}^2)}{(\mathbb{N}\mathfrak{p}^2)^{s}} + \cdots$$

Now

$$\prod_{\substack{(\mathfrak{p},\mathfrak{m})=1\\ \mathbb{N}\mathfrak{p}\le t_0}} \frac{1}{1-\chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}} = \sum \frac{\chi(\mathfrak{a})}{\mathbb{N}(\mathfrak{a})^{-s}},$$

where the second sum runs over all integral ideals expressible as a product of prime ideals with numerical norm $\le t_0$. As $t_0 \to \infty$, the right hand side converges (absolutely) to $L(s,\chi)$. Therefore the infinite product converges, and its value is $L(s,\chi)$. □

Partial zeta functions; the residue formula

Let K be a number field, let $\mathfrak{m}$ be a modulus. For every class $\mathfrak{k}$ in $C_\mathfrak{m} \overset{\text{def}}{=} I^\mathfrak{m}/i(K_{\mathfrak{m},1})$, we define the ***partial zeta function***

$$\zeta(s,\mathfrak{k}) = \sum_{\mathfrak{a}\ge 0\,,\ \mathfrak{a}\in\mathfrak{k}} \frac{1}{\mathbb{N}\mathfrak{a}^{s}} \qquad \text{(sum over the integral ideals in } \mathfrak{k}).$$

Note that for every character χ of $C_\mathfrak{m}$,

$$L(s,\chi) = \sum_{\mathfrak{k}\in C_\mathfrak{m}} \chi(\mathfrak{k})\zeta(s,\mathfrak{k}).$$

In particular,

$$\zeta_K(s) = \sum_{\mathfrak{k}\in C_\mathfrak{m}} \zeta(s,\mathfrak{k}).$$

Therefore, knowledge of the $\zeta(s,\mathfrak{k})$ will provide us with information about $L(s,\chi)$ and $\zeta_K(s)$.

Let

$$S(x,\mathfrak{k}) = |\{\mathfrak{a}\in\mathfrak{k} \mid \mathfrak{a} \text{ integral } \mathbb{N}\mathfrak{a}\le x\}|,$$

i.e., it is the $S(x)$ for the Dirichlet series $\zeta(s,\mathfrak{k})$. Recall from ANT, Chapter 5, p. 87 that there is a homomorphism

$$l: U \to \mathbb{R}^{r+s}, \quad u \mapsto (\log|\sigma_1(u)|,\dots,2\log|\sigma_{r+s}(u)|)$$

whose kernel is the torsion subgroup of U and whose image is an $r+s-1$ dimensional lattice. The regulator $\operatorname{reg}(K)$ is defined to be the volume of a fundamental parallelopiped for this lattice. Let $U_{\mathfrak{m},1} = U \cap K_{\mathfrak{m},1}$. Then $U_{\mathfrak{m},1}$ has finite index in U, and we define $\operatorname{reg}(\mathfrak{m})$ to be the volume of the fundamental parallelopiped for $l(U_{\mathfrak{m},1})$. Thus

$$\operatorname{reg}(\mathfrak{m}) = \operatorname{reg}(K)(U : U(\mathfrak{m})).$$

PROPOSITION 2.8 *For all* $x \ge 1$,

$$|S(x,\mathfrak{k}) - g_\mathfrak{m} x| \le C x^{1-\frac{1}{d}}, \quad g_\mathfrak{m} = \frac{2^r(2\pi)^s\ reg(\mathfrak{m})}{w_\mathfrak{m}\mathbb{N}(\mathfrak{m})|\Delta_{K/\mathbb{Q}}|^{\frac{1}{2}}}, \quad d = [K:\mathbb{Q}],$$

where

$$\begin{aligned} r &= \text{number of real primes,}\\ s &= \text{number of complex primes,}\\ w_{\mathfrak{m}} &= \text{number of roots of } 1 \text{ in } K_{\mathfrak{m},1},\\ \mathbb{N}(\mathfrak{m}) &= \mathbb{N}(\mathfrak{m}_0)2^{r_0},\\ r_0 &= \text{number of real primes in } \mathfrak{m}\text{, and}\\ \Delta_{K/\mathbb{Q}} &= \text{discriminant of } K/\mathbb{Q}. \end{aligned}$$

PROOF. First show that there is an integral ideal $\mathfrak{b}_0 \in \mathfrak{k}^{-1}$. Then for every $\mathfrak{a} \in \mathfrak{k}$, $\mathfrak{a}$ integral, $\mathfrak{a}\mathfrak{b}_0 = (\alpha)$, some $\alpha \in \mathcal{O}_K$. Now $S(x, \mathfrak{k})$ is the number of principal ideals (α) such that $\alpha \in \mathfrak{b}_0 \cap K_{\mathfrak{m},1}$ with $|\operatorname{Nm}(\alpha)| \le x\mathbb{N}(\mathfrak{b}_0)$. Now count. The techniques are similar to those in the proof of the unit theorem. For the details, see Lang 1970, VI.3, Theorem 3. (A slightly weaker result is proved in Janusz 1996, IV.2.11). □

COROLLARY 2.9 *The partial zeta function $\zeta(s, \mathfrak{k})$ is analytic for $\Re(s) > 1 - \frac{1}{d}$ except for a simple pole at $s = 1$, where it has residue $g_{\mathfrak{m}}$.*

PROOF. Apply Proposition 2.5. □

Note that $g_{\mathfrak{m}}$ does not depend on $\mathfrak{k}$.

LEMMA 2.10 *If A is a finite abelian group, and $\chi\colon A \to \mathbb{C}^\times$ is a nontrivial character (i.e., homomorphism not mapping every element to 1), then*

$$\sum_{a \in A} \chi(a) = 0.$$

PROOF. Because χ is nontrivial, there is a $b \in A$ such that $\chi(b) \ne 1$. But

$$\sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ab) = \Big(\sum_a \chi(a)\Big)\chi(b),$$

and so

$$(\chi(b) - 1)\sum_a \chi(a) = 0,$$

which implies that $\sum_a \chi(a) = 0$. □

COROLLARY 2.11 *If χ is not the trivial character, then $L(s, \chi)$ is analytic for $\Re(s) > 1 - \frac{1}{d}$.*

PROOF. Near $s = 1$,

$$L(s, \chi) = \sum_{\mathfrak{k} \in C_{\mathfrak{m}}} \chi(\mathfrak{k}) \cdot \zeta(s, \mathfrak{k}) = \frac{\sum_{\mathfrak{k} \in C_{\mathfrak{m}}} \chi(\mathfrak{k}) g_{\mathfrak{m}}}{s - 1} + \text{ holomorphic function,}$$

and the lemma shows that the first term is zero. □

Later we shall see that $L(1, \chi) \ne 0$.

COROLLARY 2.12 *The Dedekind zeta function $\zeta_K(s)$ is analytic for $\Re(s) > 1 - \frac{1}{d}$ except for a simple pole at $s = 1$, where it has residue*

$$\frac{2^r(2\pi)^s \, reg(K)}{w_K|\Delta|^{\frac{1}{2}}} h_K$$

PROOF. Recall that $\zeta_K(s) = \sum_{\mathfrak{k}\in C_K} \zeta(s,\mathfrak{k})$. □

EXAMPLE 2.13 (a) For $K = \mathbb{Q}$, the last formula becomes $1 = \frac{2}{2}$.

(b) For $K = \mathbb{Q}[\sqrt{d}]$, the formula becomes

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \begin{cases} \frac{2\log(u)}{\Delta^{\frac{1}{2}}} h_K, & u > 1 \text{ a fundamental unit}, d > 0 \\ \frac{2\pi}{w_K|\Delta|^{\frac{1}{2}}} h_K, & d < 0. \end{cases}$$

It is possible to find a closed formula for the expression on the left, and this leads to a very simple expression for the class number. Recall that the Artin map for $K/\mathbb{Q}$ can be regarded as a character $\chi\colon I^S \to \{\pm 1\}$, where S is the set of primes that ramify. Rather than a map on ideals, we regard it as a map on positive integers, and we extend it to all positive integers by setting $\chi(m) = 0$ if m is divisible by a prime that ramifies in K. Thus χ is now the multiplicative map on the set of positive integers taking the values

$$\chi(p) = \begin{cases} 1 & \text{if } p \text{ splits in } K \\ -1 & \text{if } p \text{ remains prime in } K \\ 0 & \text{if } p \text{ ramifies in } K. \end{cases}$$

For an imaginary quadratic field with discriminant < -4, the formula becomes

$$h_K = \frac{1}{2-\chi(2)} \sum_{\substack{(x,\Delta)=1 \\ 0<x<|\Delta|/2}} \chi(x).$$

For example, if $K = \mathbb{Q}[\sqrt{-5}]$, then $|\Delta| = 20$, and

$$h = \frac{1}{2-0}(\chi(1)+\chi(3)+\chi(7)+\chi(9)) = \frac{?}{2} = 2,$$

because 2 ramifies, and

$$-5 \equiv 1 \equiv 1^2 \mod 3, \qquad -5 \equiv 2 \equiv 3^2 \mod 7.$$

See Borevich and Shafarevich 1966, Chapter 5, Section 4, for more details.

3 Density of the Prime Ideals Splitting in an Extension

For a set T of prime ideals of K, we define $\zeta_{K,T}(s) = \prod_{\mathfrak{p}\in T} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}}$. If some positive integral power $\zeta_{K,T}(s)^n$ of $\zeta_{K,T}(s)$ extends to a meromorphic function on a neighbourhood of 1 having a pole of order m at 1, then we say[2] that T has ***polar density*** $\delta(T) = m/n$.

[2]Following Marcus 1977, p. 188; or p. 134 in the second edition.

PROPOSITION 3.1 (a) *The set of all prime ideals of K has polar density* 1.

(b) *The polar density of every set (having one) is* ≥ 0.

(c) *Suppose that T is the disjoint union of T_1 and T_2. If any two of T, T_1, T_2 have polar densities, then so also does the third, and $\delta(T) = \delta(T_1) + \delta(T_2)$.*

(d) *If $T \subset T'$, then $\delta(T) \leq \delta(T')$ (when both are defined).*

(e) *A finite set has density zero.*

PROOF. (a) We know that $\zeta_K(s)$ itself extends to a neighbourhood of 1, and has a simple pole at 1.

(b) To say that T has negative density means that $\zeta_{K,T}(s)$ is holomorphic in a neighbourhood of $s = 1$, and is zero there. But $\zeta_{K,T}(1) = \prod_{p\in T} \frac{1}{1-p^{-1}} > 0$.

(c) Clearly,

$$\zeta_{K,T}(s) = \zeta_{K,T_1}(s) \cdot \zeta_{K,T_2}(s).$$

Suppose, for example, that $\zeta_{K,T}(s)^m$ and $\zeta_{K,T_1}(s)^{m_1}$ extend to meromorphic functions in neighbourhoods of 1, with poles of order n and n_1 at 1. Then

$$\zeta_{K,T_2}(s)^{mm_1} = \zeta_{K,T}(s)^{mm_1}/\zeta_{K,T_1}(s)^{mm_1}$$

extends to a meromorphic function in a neighbourhood of 1, and has a pole of order $m_1 n - mn_1$ at 1. Therefore

$$\delta(T_2) = \frac{m_1 n}{mm_1} - \frac{mn_1}{mm_1} = \delta(T) - \delta(T_2).$$

(d) Combine (c) with (b).

(e) Obvious □

PROPOSITION 3.2 *If T contains no primes for which $\mathbb{N}\mathfrak{p}$ is a prime (in $\mathbb{Z}$), then $\delta(T) = 0$.*

PROOF. For $\mathfrak{p} \in T$, $\mathbb{N}\mathfrak{p} = p^f$ with $f \geq 2$. Moreover, for a given p, there are at most $[K : \mathbb{Q}]$ primes of K lying over p. Therefore $\zeta_{K,T}(s)$ can be decomposed into a product $\prod_{i=1}^{d} g_i(s)$ of d infinite products over the prime numbers each factor of a $g_i(s)$ being 1 or of the form $\frac{1}{1-p^{-f}}$ with $f \geq 2$. For each i, $g_i(1) \leq \sum_{n>0} n^{-2} = \zeta(2)$. Therefore $g_i(s)$ is holomorphic at 1. □

COROLLARY 3.3 *Let T_1 and T_2 be sets of prime ideals in K. If the sets differ only by primes for which $\mathbb{N}\mathfrak{p}$ is not prime and one has a polar density, then so does the other, and the densities are equal.*

THEOREM 3.4 *Let L be a finite extension of K, and let M be its Galois closure. Then the set of prime ideals of K that split completely in L has density $1/[M : K]$.*

PROOF. A prime ideal $\mathfrak{p}$ of K splits completely in L if and only if it splits completely in M.[3] Therefore, it suffices to prove the theorem under the assumption that L is Galois over

[3]Here's an explanation of the statement that a prime splits completely in an extension L if and only if it splits completely in its Galois closure. If a prime splits completely in L, then it splits completely in every conjugate L' of L, so it becomes a question of showing that if a prime splits completely in two fields L and L' then it splits completely in their composite. This follows easily (for example) from the criterion that a prime $\mathfrak{p}$ in K splits completely in L if and only if $L \otimes_K K_\mathfrak{p}$ is a product of copies of $K_\mathfrak{p}$ (the composite LL' is a direct factor of $L \otimes_K L'$).

K. Let S be the set of prime ideals of K that split completely in L, and let T be the set of prime ideals of L lying over a prime ideal in S. Corresponding to each $\mathfrak{p}$ in S, there are exactly $[L : K]$ prime ideals $\mathfrak{P}$ in T, and for each of them $\mathrm{Nm}_{L/K}\mathfrak{P} = \mathfrak{p}$, and so $\mathbb{N}\mathfrak{P} = \mathbb{N}\mathfrak{p}$. Therefore, $\zeta_{L,T}(s) = \zeta_{K,S}(s)^{[L:K]}$. But T contains every prime ideal of L that is unramified in L/K for which $\mathbb{N}\mathfrak{P} = p$. Therefore T differs from the set of all prime ideals in L by a set of polar density 0, and so T has density 1. This implies that $\zeta_{K,S}(s)$ has the property signifying that S has density $1/[L : K]$. □

COROLLARY 3.5 *If $f(X) \in K[X]$ splits into linear factors modulo $\mathfrak{p}$ for all but finitely many prime ideals $\mathfrak{p}$, then f splits into linear factors in K.*

PROOF. Apply the theorem to the splitting field of f. □

COROLLARY 3.6 (BAUER 1916) *For Galois extensions L and M of a number field K,*

$$L \subset M \iff Spl(L) \supset Spl(M).$$

Hence

$$L = M \iff Spl(L) = Spl(M),$$

and

$$L \mapsto Spl(L)$$

is an injection from the set of finite Galois extensions of K (contained in some fixed algebraic closure) to the set of subsets of $\{\mathfrak{p} \subset \mathcal{O}_K\}$.

PROOF. See the proof of (V 3.25). □

EXAMPLE 3.7 Let $f(X)$ be an irreducible polynomial of degree 3. The density of the set of primes $\mathfrak{p}$ for which $f(X)$ splits modulo $\mathfrak{p}$ is $1/3$ or $1/6$ depending on whether $f(X)$ has Galois group C_3 or S_3.

COROLLARY 3.8 *For every abelian extension L/K and every finite set $S \supset S_\infty$ of primes of K including those that ramify in L, the Artin map $\psi_{L/K}\colon I^S \to \mathrm{Gal}(L/K)$ is surjective.*

PROOF. Let H be the image of $\psi_{L/K}$. For all $\mathfrak{p} \notin S$, $(\mathfrak{p}, L^H/K) = (\mathfrak{p}, L/K)|L^H = 1$, which implies that $\mathfrak{p}$ splits in L^H. Hence all but finitely many prime ideals of K split in L^H, which implies that $[L^H : K] = 1$. □

4 Density of the Prime Ideals in an Arithmetic Progression

Let $f(s)$ and $g(s)$ be two functions defined (at least) for $s > 1$ and real. We write

$$f(s) \sim g(s) \qquad \text{as } s \downarrow 1$$

if $f(s) - g(s)$ is bounded for

$$1 < s < 1 + \varepsilon, \quad s \text{ real, some } \varepsilon > 0.$$

Note that

$$f(s) \sim \delta \log \frac{1}{s-1} \qquad \text{as } s \downarrow 1$$

implies

$$\lim_{s\downarrow 1} \frac{f(s)}{\log \frac{1}{s-1}} = \delta.$$

When $f(s)$ and $g(s)$ are functions holomorphic in a neighbourhood of $s = 1$ except possibly for poles at $s = 1$,

$$f(s) \sim g(s) \qquad \text{as } s \downarrow 1$$

if and only if $f(s)$ and $g(s)$ differ by a function that is holomorphic on a neighbourhood of 1.

Let T be a set of primes of K. If there exists a δ such that

$$\sum_{\mathfrak{p}\in T} \frac{1}{\mathbb{N}\mathfrak{p}^s} \sim \delta \log \frac{1}{s-1} \qquad \text{as } s \downarrow 1,$$

then we say that T has ***Dirichlet density*** δ.

If the limit

$$\lim_{x\to\infty} \frac{\text{number of } \mathfrak{p} \in T \text{ with } \mathbb{N}\mathfrak{p} \le x}{\text{number of } \mathfrak{p} \text{ with } \mathbb{N}\mathfrak{p} \le x}$$

exists, then we call it the ***natural density*** of T.

PROPOSITION 4.1 (a) *If the polar density exists, then so also does the Dirichlet density, and the two are equal.*

(b) *If the natural density exists, then so also does the Dirichlet density, and the two are equal.*

PROOF. (a) If T has polar density m/n, then

$$\zeta_{K,T}(s)^n = \frac{a}{(s-1)^m} + \frac{g(s)}{(s-1)^{m-1}},$$

where $g(s)$ is holomorphic near $s = 1$. Moreover, $a > 0$ because $\zeta_{K,T}(s) > 0$ for $s > 1$ and real. On taking logs (and applying 4.3), we find that

$$n \sum_{T} \frac{1}{\mathbb{N}\mathfrak{p}^s} \sim m \log \frac{1}{s-1} \text{ as } s \downarrow 1,$$

which shows that T has Dirichlet density m/n.

(b) See Goldstein 1971, p. 252. □

REMARK 4.2 (a) A set T may have a Dirichlet density without having a natural density. For example, let T be the set of prime numbers whose leading digit (in the decimal system) is 1. Then T does not have a natural density, but its Dirichlet density is $\log_{10}(2) = \cdot 3010300\ldots$ (statement in Serre 1970, VI, 4.5). Thus it is a *stronger* statement to say that a set of primes has natural density δ than that it has Dirichlet density δ. All of the sets whose densities we compute in these notes will also have natural densities, but we do not prove that.

(b) By definition, polar densities are rational numbers. Therefore every set having a natural density that is not rational will not have a polar density.

Recall that the ***exponential function***

$$e^z = \sum \frac{z^n}{n!} = e^x(\cos y + i \sin y), \quad z = x + iy,$$

defines an isomorphism from

$$\{z \in \mathbb{C} \mid -\pi < \Im(z) < \pi\}$$

onto the complement of the negative real axis

$$\{z \in \mathbb{R} \mid z \le 0\}$$

in $\mathbb{C}$ whose inverse is, by definition, the ***(principal branch of) the logarithm function*** $\log$. With this definition

$$\log z = \log|z| + i \arg z,$$

where the $\log$ on the right is the function defined in calculus courses and

$$-\pi < \arg z < \pi.$$

With this definition

$$\log \frac{1}{1-z} = z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots, \qquad |z| < 1.$$

LEMMA 4.3 *Let $u_1, u_2, \ldots$ be a sequence of real numbers ≥ 2 such that*

$$f(s) \stackrel{\text{def}}{=} \prod_{j=1}^{\infty} \frac{1}{1-u_j^{-s}}$$

is uniformly convergent on each region $D(1, \delta, \varepsilon)$, $\delta, \varepsilon > 0$. Then

$$\log f(s) \sim \sum \frac{1}{u_j^s} \text{ as } s \downarrow 1.$$

PROOF. We have

$$\begin{aligned}
\log f(s) &= \sum_{j=1}^{\infty} \log \frac{1}{1-u_j^{-s}} \\
&= \sum_j \sum_{m=1}^{\infty} \frac{1}{m u_j^{sm}} \\
&= \sum_j \frac{1}{u_j^s} + \sum_j \sum_{m=2}^{\infty} \frac{1}{m u_j^{sm}} \\
&= \sum_j \frac{1}{u_j^s} + g(s),
\end{aligned}$$

where

$$|g(s)| \le \sum_{j=1}^{\infty} \sum_{m=2}^{\infty} \left| \frac{1}{m u_j^{sm}} \right| = \sum_{j=1}^{\infty} \sum_{m=2}^{\infty} \frac{1}{m u_j^{m\sigma}}, \qquad \sigma = \Re(s).$$

Estimate the inner sum by using ($u \geq 2, \sigma > 1$)

$$\sum_{m=2}^{\infty} \frac{1}{mu^{m\sigma}} \leq \sum_{m=2}^{\infty} \frac{1}{2}\left(\frac{1}{u^{\sigma}}\right)^{m} = \frac{1}{2}\left(\frac{1}{1-u^{-\sigma}} - u^{-\sigma} - 1\right) = \frac{1}{2}\frac{u^{-2\sigma}}{1-u^{-\sigma}} < \frac{1}{u^{2\sigma}}.$$

Hence

$$|g(s)| \leq f(2\sigma).$$

Because $f(s)$ is holomorphic for $\Re(s) > 1$, $f(2s)$ is holomorphic for $\Re(s) > \frac{1}{2}$, and so $g(\sigma)$ is bounded as $\sigma \downarrow 1$. □

PROPOSITION 4.4 (a) *The set of all prime ideal of K has Dirichlet density* 1.

(b) *The Dirichlet density of any set (having one) is* ≥ 0.

(c) *If T is finite, then $\delta(T) = 0$.*

(d) *Suppose that T is the disjoint union of T_1 and T_2. If any two of $\delta(T_1)$, $\delta(T_2)$, $\delta(T)$ are defined, so is the third, and $\delta(T) = \delta(T_1) + \delta(T_2)$.*

(e) *If $T \subset T'$, then $\delta(T) \leq \delta(T')$ (assuming both are defined).*

PROOF. (a) The set of all primes ideals even has polar density 1.

(b) For $s > 0$ real, $\frac{1}{\mathbb{N}\mathfrak{p}^s} > 0$, and for $s = 1 + \varepsilon$, $\log \frac{1}{s-1} = -\log \varepsilon$, which is positive for $0 < \varepsilon < 1$.

(c) When T is finite, $\sum_{\mathfrak{p}\in T} \frac{1}{\mathbb{N}\mathfrak{p}^s}$ is holomorphic for all s and hence bounded near any point.

(d) Clearly

$$\sum_{\mathfrak{p}\in T} \frac{1}{\mathbb{N}\mathfrak{p}^s} = \sum_{\mathfrak{p}\in T_1} \frac{1}{\mathbb{N}\mathfrak{p}^s} + \sum_{\mathfrak{p}\in T_2} \frac{1}{\mathbb{N}\mathfrak{p}^s} \qquad \Re(s) > 1.$$

Therefore, if, for example,

$$\sum_{\mathfrak{p}\in T_1} \frac{1}{\mathbb{N}\mathfrak{p}^s} \sim \delta_1 \log \frac{1}{s-1}, \qquad \sum_{\mathfrak{p}\in T_2} \frac{1}{\mathbb{N}\mathfrak{p}^s} \sim \delta_2 \log \frac{1}{s-1},$$

then

$$\sum_{\mathfrak{p}\in T} \frac{1}{\mathbb{N}\mathfrak{p}^s} \sim (\delta_1 + \delta_2) \log \frac{1}{s-1}.$$

(e) If both $\delta(T)$ and $\delta(T')$ exist, then so also does $\delta(T' \smallsetminus T)$, and

$$\delta(T') - \delta(T) \overset{(c)}{=} \delta(T' \smallsetminus T) \overset{(a)}{\geq} 0.$$

□

PROPOSITION 4.5 *Let T be the set of prime ideals of K having degree* 1 *over $\mathbb{Q}$, i.e., such that the residue class degree $f(\mathfrak{p}/p) = 1$. Then $\delta(T) = 1$.*

PROOF. The complement of T has polar density 1 (Proposition 3.2) □

COROLLARY 4.6 *Let T be as in the Proposition. For every set S of primes of K having a Dirichlet density*

$$\delta(T \cap S) = \delta(S).$$

PROOF. The complement T' of T has density 0, and it follows easily that $\delta(S \cap T') = 0$. Because S is the disjoint union of $S \cap T$ and $S \cap T'$, this implies that $\delta(S \cap T)$ is defined and equals $\delta(S)$. □

LEMMA 4.7 *Let A be a finite abelian group, and let $a \in A$. Then*

$$\sum_{\chi \in A^\vee} \chi(a) = 0.$$

Here $A^\vee$ is the group of characters of A, i.e., $A^\vee = \mathrm{Hom}(A, \mathbb{C}^\times)$.

PROOF. If $a = 1$, then $\chi(a) = 1$ for all χ, and so the statement follows from the fact that $A^\vee$ has the same number of elements as A (it is in fact noncanonically isomorphic to A). If $a \neq 1$, there is a character χ_1 such that $\chi_1(a) \neq 1$. Then

$$\sum_{\chi \in A^\vee} \chi(a) = \sum_{\chi \in A^\vee} (\chi_1\chi)(a) = \sum_{\chi \in A^\vee} \chi_1(a)\chi(a) = \chi_1(a) \sum_{\chi \in A^\vee} \chi(a).$$

Since $\chi_1(a) \neq 1$, this implies that $\sum_{\chi \in A^\vee} \chi(a) = 0$.

Alternatively, identify A with $A^{\vee\vee}$ by means of the isomorphism

$$a \mapsto (\chi \mapsto \chi(a)) \colon A \to (A^\vee)^\vee,$$

and apply (2.10). □

THEOREM 4.8 *Let $\mathfrak{m}$ be a modulus for K, and let H be a congruence subgroup for $\mathfrak{m}$:*

$$I^{\mathfrak{m}} \supset H \supset i(K_{\mathfrak{m},1}).$$

Then

$$\delta(\{\mathfrak{p} \in H\}) = \begin{cases} 1/(I^{S(\mathfrak{m})} : H) & \text{if } L(1,\chi) \text{ is nonzero for all characters } \chi \neq \chi_0 \text{ of } I^{S(\mathfrak{m})}/H; \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. Let χ be a character of $I^{\mathfrak{m}}$ trivial on H, and let

$$L(s,\chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}}.$$

Then the argument in the proof of (4.3) shows that

$$\log L(s,\chi) - \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{\mathbb{N}\mathfrak{p}^s}$$

is holomorphic for $\Re(s) > \frac{1}{2}$. In particular,

$$\log(L(s,\chi)) \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{\mathbb{N}\mathfrak{p}^s} \qquad \text{as } s \downarrow 1.$$

But (see 4.7)

$$\sum_{\chi} \chi(\mathfrak{p}) = \begin{cases} h & \mathfrak{p} \in H \\ 0 & \mathfrak{p} \notin H, \end{cases}$$

and so, on summing over all χ, we find that

$$\sum_{\chi} \log L(s,\chi) \sim h \sum_{\mathfrak{p}\in H} \frac{1}{\mathbb{N}\mathfrak{p}^s} \qquad \text{as } s \downarrow 1.$$

If $\chi \neq \chi_0$, then $L(s,\chi)$ is holomorphic near $s=1$, say $L(s,\chi) = (s-1)^{m(\chi)}g(s)$, where $m(\chi) \geq 0$ and $g(1) \neq 0$. Thus

$$\log L(s,\chi) \sim m(\chi)\log(s-1) = -m(\chi)\log\frac{1}{s-1}.$$

If $\chi = \chi_0$, then $L(s,\chi) = \zeta_K(s)/\prod_{\mathfrak{p}|\mathfrak{m}} \frac{1}{1-\mathbb{N}\mathfrak{p}^{-s}}$, and so

$$\log L(s,\chi_0) \sim \log \zeta_K(s) \sim \log\frac{1}{s-1} \qquad \text{as } s \downarrow 1.$$

On combining these statements, we find that

$$h\sum_{\mathfrak{p}\in H} \mathbb{N}\mathfrak{p}^{-s} \sim (1 - \sum_{\chi\neq\chi_0} m(\chi))\log\frac{1}{s-1},$$

and hence

$$\delta(\{\mathfrak{p}\in H\}) = \frac{1-\sum_{\chi\neq\chi_0} m(\chi)}{h}.$$

This shows that $\delta(\{\mathfrak{p}\in H\}) = \frac{1}{h}$ if $L(1,\chi)\neq 0$ for all $\chi\neq\chi_0$, and $\delta(\{\mathfrak{p}\in H\}) = 0$ otherwise (and at most one $L(s,\chi)$ can have a zero at $s=1$, and it can only be a simple zero). □

The Second Inequality

THEOREM 4.9 *For every Galois extension L of K and modulus $\mathfrak{m}$ of K,*

$$(I^{S(\mathfrak{m})} : i(K_{\mathfrak{m},1})\cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})})) \leq [L:K].$$

PROOF. Let $H = \mathrm{Nm}_{L/K} I_L^{\mathfrak{m}} \cdot i(K_{\mathfrak{m},1})$. From Theorem 4.8, we know that $\delta(\{\mathfrak{p}\in H\}) = 1/(I^{S(\mathfrak{m})} : H)$ or 0, and that the first case holds exactly when, for all nontrivial characters χ of I^S/H, $L(1,\chi)\neq 0$.

If $\mathfrak{p}$ splits in L, i.e., $f(\mathfrak{P}/\mathfrak{p}) = 1$ for all $\mathfrak{P}|\mathfrak{p}$, then $\mathfrak{p}$ is the norm of any prime ideal of $\mathcal{O}_L$ lying over it, and so $\{\mathfrak{p}\in H\}$ contains the set of prime ideals splitting in L. Hence, Theorem 3.4 shows that

$$\delta(\{\mathfrak{p}\in H\}) \geq [L:K]^{-1} \neq 0.$$

On combining the two statements we find

(a) $\delta(\{\mathfrak{p}\in H\}) \neq 0$;

(b) that for all nontrivial characters χ of I^S/H, $L(1,\chi)\neq 0$;

(c) $(I^S : H) = \delta(\{\mathfrak{p}\in H\})^{-1} \leq [L:K]$. □

COROLLARY 4.10 *Let χ be a nontrivial character of $C_{\mathfrak{m}}$, and suppose that there is a Galois extension L of K such that $\mathrm{Nm}_{L/K} C_{\mathfrak{m},L} \subset \mathrm{Ker}(\chi)$. Then $L(1,\chi)\neq 0$.*

PROOF. This was shown in the course of the proof of the theorem. □

The Existence Theorem (Chapter V, 3.6) implies that the hypothesis of the corollary holds for all χ. It is possible to prove that $L(1, \chi) \neq 0$ without using class field theory, but, at this point we prefer to return to class field theory. We shall complete the proof of the Chebotarev Theorem in Chapter VIII

Chapter VII

Global Class Field Theory: Proofs of the Main Theorems

> *J'ai revu un peu la théorie du corps de classes, dont j'ai enfin l'impression d'avoir compris les énoncés essentiels (bien entendu, pas les démonstrations!)*
> Grothendieck, letter to Serre, 19.9.56.[1]

In this chapter we prove the main theorems of global class field theory, namely, the Reciprocity Law and the Existence Theorem (Theorems 5.3 and 5.5 of Chapter V), following the method of Tate 1967 (see also Artin and Tate 1961). Throughout, we work with idèles rather than ideals.

This chapter is independent of Chapter VI, except that Theorem 4.9 of Chapter VI can be used to replace Section 6. We shall need to refer to Chapter V only for the definitions of the idèle class group and the the definition of the global Artin map $\phi: \mathbb{I} \to \mathrm{Gal}(L/K)$ as the "product" of the local Artin maps (Section 5). On the other hand, we shall make frequent use of the results in Chapters II and III.

We use the notation from Chapter V (especially p. 169). In particular, $|\cdot|_v$ denotes the normalized absolute value for v (for which the product formula holds).

1 Outline

Let L/K be a finite Galois extension of number fields with Galois group G. The idèle class group $\boldsymbol{C}_L \overset{\text{def}}{=} \mathbb{I}_L/L^\times$ plays the same role for global class field theory that the multiplicative group $L^\times$ plays for local class field theory. In particular, when L/K is abelian, we shall prove that there is a isomorphism

$$\phi: \boldsymbol{C}_K/\,\mathrm{Nm}_{L/K}(\boldsymbol{C}_L) \to G$$

[1] I have been reviewing a little class field theory, of which I finally have the impression that I understand the main results (but not the proofs, of course!)

whose local components are the local Artin maps, i.e., such that for any prime v of K and prime w of L lying over it, the following diagram commutes,

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi} & \mathrm{Gal}(L/K), \end{array}$$

where ϕ_v is the local Artin map of Chapters I and III.

According to Tate's theorem (3.11, Chapter II), to obtain such an isomorphism, it suffices to prove that, for every finite Galois extension L/K with Galois group G,

(a) $H^1(G, \boldsymbol{C}_L) = 0$;

(b) $H^2(G, \boldsymbol{C}_L)$ is cyclic of order $[L : K]$ with a canonical generator $u_{L/K}$;

(c) if $E \supset L \supset K$ are two finite Galois extensions of K, then $\mathrm{Res}(u_{E/K}) = u_{E/L}$.

The isomorphism $\phi_{L/K}$ is then the inverse of that defined by $u_{L/K}$,

$$H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, \boldsymbol{C}_L).$$

Once the fundamental class $u_{L/K}$ has been shown to be compatible with the local fundamental classes, $\phi_{L/K}$ will be a product of the local Artin maps.

In fact, we adopt a slightly different approach. We shall *define* the global Artin map $\boldsymbol{C}_K \to \mathrm{Gal}(L/K)$ to be the "product" of the local Artin maps, and we shall use results slightly weaker than (a) and (b) to deduce that it has the correct properties.

In Section 2, we express the cohomology of the idèles in terms of the cohomology of the local fields,

$$H^0(G, \mathbb{I}_L) = \mathbb{I}_K;$$
$$H_T^r(G, \mathbb{I}_L) \simeq \bigoplus\nolimits_v H_T^r(G^v, L^{v\times})$$

(sum over the primes v of K; for some choice of a prime $w|v$, G^v is the decomposition group of w and $L^v = L_w$). After computing the Herbrand quotient of the group of S-units in Section 3, we prove the first inequality,

> for any cyclic extension L/K, $(\boldsymbol{C}_K : \mathrm{Nm}_{L/K}\boldsymbol{C}_L) \geq [L : K]$,

in Section 4. We also prove in Section 4 that, for any abelian extension, the Galois group is generated by the Frobenius elements. In Section 5 we state the theorem,

> For every Galois extension L/K of number fields, (a) $(\boldsymbol{C}_K : \mathrm{Nm}_{L/K}\boldsymbol{C}_L) \leq [L : K]$ (second inequality); (b) $H^1(G, \boldsymbol{C}_L) = 1$; (c) $H^2(G, \boldsymbol{C}_L)$ has order $\leq [L : K]$.

and we prove it using Theorem 4.9 of Chapter VI. In the following section, we give a different proof of the theorem that avoids the use complex analysis.

After some preliminaries on Brauer groups, in Section 7 we complete the proof of the reciprocity law by showing that, for every abelian extension L/K, $K^\times$ is contained in the kernel of $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$. Because we already know that $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$ is contained in the kernel of $\phi_{L/K}$ and that $\phi_{L/K}$ is surjective (because $\mathrm{Gal}(L/K)$ is generated by the Frobenius elements), the second inequality implies that $\phi_{L/K}$ is an isomorphism.

We prove the Existence Theorem in Section 9 by showing the every (open) subgroup of finite index in $\boldsymbol{C}_K$ contains the norm group of some subextension of the extension obtained by first adjoining a root of unity to K and then making a Kummer extension.

To some extent, the cyclic cyclotomic extensions of K play the same role as the unramified extensions of a local field. For example, a key point in the last step of the proof of the Reciprocity Law is that every element of $\mathrm{Br}(K)$ is split by a cyclic cyclotomic extension.

2 The Cohomology of the Idèles

Let L/K be a finite Galois extension of number fields with Galois group G. Recall that $\sigma \in G$ acts on the primes w of L lying over a fixed prime v of K according to the rule $|\sigma a|_{\sigma w} = |a|_w$. Therefore σ is an isomorphism of valued fields

$$(L, |\ |_w) \to (L, |\ |_{\sigma w}),$$

and so extends to the completions: there is a commutative diagram

$$\begin{array}{ccc} L_w & \xrightarrow{\sigma} & L_{\sigma w} \\ \uparrow{\scriptstyle i_w} & & \uparrow{\scriptstyle i_{\sigma w}} \\ L & \xrightarrow{\sigma} & L. \end{array}$$

Fix a prime v of K, and let w_0 be a prime of L lying over v. The map $\sigma \mapsto \sigma w_0$ defines a bijection

$$G/G_{w_0} \to \{w|v\},$$

where G_{w_0} is the decomposition group of w_0.

We wish to extend the action of G on L to an action of G on $\prod_{w|v} L_w$. Recall (ANT, 8.2) that the map

$$a \otimes b \mapsto (i_w(a)b)_w : L \otimes_K K_v \to \prod\nolimits_{w|v} L_w$$

is an isomorphism. The group G acts on $L \otimes_K K_v$ through its action on L, and we use the isomorphism to transfer this action to $\prod_{w|v} L_w$. Thus,

(a) the elements of G acts continuously on $\prod_{w|v} L_w$;

(b) all elements of the form $(a, \dots, a)$, $a \in K_v$, are fixed by G;

(c) for every $a \in L$, $\sigma(\dots, i_w(a), \dots) = (\dots, i_w(\sigma a), \dots)$.

These conditions determine the action uniquely (in fact, (a) and (c) determine it because K is dense in K_v).

LEMMA 2.1 *For $\sigma \in G$ and $\alpha = (\alpha(w)) \in \prod_{w|v} L_w$,*

$$(\sigma\alpha)(w) = \sigma(\alpha(\sigma^{-1}w)). \qquad (*)$$

PROOF. The rule $(*)$ does define a continuous action of G on $\prod L_w$, and so it suffices to check that it satisfies (b) and (c). Condition (b) is obvious. For (c), let $\alpha(w) = i_w(a)$, $a \in L$. Then (by $(*)$)

$$(\sigma\alpha)(w) = \sigma(i_{\sigma^{-1}w}(a)).$$

When we replace w with $\sigma^{-1}w$ in the commutative diagram above, we obtain the formula $\sigma \circ i_{\sigma^{-1}w} = i_w \circ \sigma$. Therefore

$$(\sigma\alpha)(w) = i_w(\sigma a),$$

as required. □

In more down-to-earth terms, $(\sigma\alpha)(\sigma w) = \sigma(\alpha(w))$: if α has the element a in the w-position, then $\sigma\alpha$ has the element σa in the σw-position.

Note that the action of G on $\prod_{w|v} L_w$ induces an action of G on the subsets $\prod_{w|v} L_w^\times$ and $\prod_{w|v} U_w$ of $\prod_{w|v} L_w$.

PROPOSITION 2.2 *Choose a $w_0|v$, and let G_{w_0} be its decomposition group. For $\alpha \in \prod_{w|v} L_w$ and $\sigma \in G$, define $f_\alpha(\sigma) = \sigma(\alpha(\sigma^{-1}w_0))$. Then $f_\alpha \in \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$, and the map*

$$\alpha \mapsto f_\alpha \colon \prod_{w|v} L_w \to \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$$

is an isomorphism of G-modules. Similar statements hold with L_w replaced with $L_w^\times$ and with U_w.

PROOF. Recall (II 1) that

$$\operatorname{Ind}_{G_{w_0}}^G(L_{w_0}) = \{f \colon G \to L_{w_0} \mid f(\rho\sigma) = \rho f(\sigma), \text{ all } \rho \in G_{w_0}\}$$

and that $\tau \in G$ acts on $f \in \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$ according to the rule $(\tau f)(\sigma) = f(\sigma\tau)$. For $\rho \in G_{w_0}$,

$$f_\alpha(\rho\sigma) = \rho\sigma(\alpha(\sigma^{-1}\rho^{-1}w_0)) = \rho\sigma(\alpha(\sigma^{-1}w_0)) = \rho f_\alpha(\sigma),$$

and so $f_\alpha \in \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$. Moreover,

$$(\tau f_\alpha)(\sigma) = f_\alpha(\sigma\tau) = \sigma\tau(\alpha(\tau^{-1}\sigma^{-1}w_0)) = \sigma(\tau\alpha)(\sigma^{-1}w_0) = f_{\tau\alpha}(\sigma),$$

and so $\alpha \mapsto f_\alpha$ is a homomorphism of G-modules $\prod_{w|v} L_w \to \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$. Given $f \in \operatorname{Ind}_{G_{w_0}}^G(L_{w_0})$, set

$$\alpha_f(w) = \sigma(f(\sigma^{-1})), \quad w = \sigma w_0.$$

Then $f \mapsto \alpha_f$ is an inverse to $\alpha \mapsto f_\alpha$. □

PROPOSITION 2.3 *For all r,*

$$H^r(G, \textstyle\prod_{w|v} L_w^\times) \simeq H^r(G_{w_0}, L_{w_0}^\times).$$

In particular,

$$H^0(G, \textstyle\prod_{w|v} L_w^\times) \simeq K_v^\times.$$

Similar statements hold with $L_w^\times$ replaced with U_w.

PROOF. We have

$$H^r(G, \textstyle\prod_{w|v} L_w^\times) = H^r(G, \operatorname{Ind}_{G_{w_0}}^G L_{w_0}^\times) = H^r(G_{w_0}, L_{w_0}^\times)$$

by Shapiro's lemma (II, 1.11). □

REMARK 2.4 The group $H^r(G_{w_0}, L_{w_0}^\times)$ is independent of the prime w_0 dividing v up to a *canonical* isomorphism, for let w be a second such prime. Then we can write $w = \sigma w_0$, and we have a compatible pair of isomorphisms

$$\tau \mapsto \sigma\tau\sigma^{-1}: G_{w_0} \to G_w, \qquad x \mapsto \sigma^{-1}x: L_w \to L_{w_0},$$

and hence isomorphisms

$$H^r(G_w, L_w^\times) \to H^r(G_{w_0}, L_{w_0}^\times)$$

for each r (see II, §1).

If $w = \sigma' w_0$, then $\sigma' = \sigma\tau$ with $\tau \in G_{w_0}$. The maps defined by σ and σ' differ by the automorphism of $H^r(G_{w_0}, L_{w_0}^\times)$ defined by τ, which is the identity map (II, 1.27d). Therefore $H^r(G_{w_0}, L_{w_0}^\times)$ and $H^r(G_w, L_w^\times)$ are *canonically* isomorphic. This suggests the following notation: choose a prime $w|v$ and set,

$$G^v = G_w, \quad L^v = L_w, \quad U^v = U_w.$$

These objects are defined only up to noncanonical isomorphisms, but $H^r(G^v, L^{v\times})$ and $H^r(G^v, U^v)$ are defined up to *canonical* isomorphisms.

We endow $\mathbb{I}_L$ with the action of G such that the inclusions

$$\prod_{w|v} L_w^\times \to \mathbb{I}_L$$

are G-homomorphisms. Thus if α has a_w in the w-position, then $\sigma\alpha$ has σa_w in the σw-position.

PROPOSITION 2.5 (a) *The map $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ induces an isomorphism $\mathbb{I}_K \to \mathbb{I}_L^G$.*

(b) *For all $r \geq 0$,*

$$H_T^r(G, \mathbb{I}_L) = \bigoplus\nolimits_v H_T^r(G^v, L^{v\times}).$$

PROOF. (a) Clearly $\alpha = (a_w)$ is fixed by G if and only if each subfamily $(a_w)_{w|v}$ is fixed by G. But $(a_w)_{w|v}$ is fixed by G only if a_w is independent of w and lies in $K_v^\times$.

(b) For each finite set S of primes of K, let

$$\mathbb{I}_{L,S} = \prod_{v\in S}\Big(\prod_{w|v} L_w^\times\Big) \times \prod_{v\notin S}\Big(\prod_{w|v} U_w\Big).$$

Then $\mathbb{I}_{L,S}$ is stable under the action of G, and $\mathbb{I}_L$ is the directed union of the $\mathbb{I}_{L,S}$ as S runs over the finite sets of primes of K containing all infinite primes and all primes that ramify in L. Hence (see II, 4.4),

$$H^r(G, \mathbb{I}_L) = \varinjlim H^r(G, \mathbb{I}_{L,S}).$$

On applying (II, 1.25) and (2.3), we find that

$$\begin{aligned} H^r(G, \mathbb{I}_{L,S}) &= \prod_{v\in S} H^r(G, \textstyle\prod_{w|v} L_w^\times) \times \prod_{v\notin S} H^r(G, \prod_{w|v} U_w) \\ &= \prod_{v\in S} H^r(G^v, L^{v\times}) \times \prod_{v\notin S} H^r(G^v, U^v). \end{aligned}$$

Because of (III, 1.1), the second factor is zero when $r > 0$, and so

$$\begin{aligned} H^r(G, \mathbb{I}_L) &= \varinjlim_S H^r(G, \mathbb{I}_{L,S}) \\ &= \varinjlim_S \bigoplus\nolimits_{v\in S} H^r(G^v, L^{v\times}) \\ &= \bigoplus\nolimits_{\text{all } v} H^r(G^v, L^{v\times}). \end{aligned}$$

The same argument works for $r \leq 0$ when one uses the Tate groups. □

COROLLARY 2.6 (a) $H^1(G, \mathbb{I}_L) = 0$;

(b) $H^2(G, \mathbb{I}_L) \simeq \bigoplus_v \left(\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}\right)$, *where* $n_v = [L^v : K_v]$.

PROOF. (a) Apply Hilbert's theorem 90 (II, 1.22).

(b) From Theorem 2.1 of Chapter III, we know that the invariant map gives an isomorphism

$$H^2(G^v, L^{v\times}) \to \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}.$$

□

PROPOSITION 2.7 *Let S be a finite set of primes of K, and let T be the set of primes of L lying over primes in S. If L/K is cyclic, then the Herbrand quotient*

$$h(\mathbb{I}_{L,T}) = \prod_{v\in S} n_v, \quad n_v = [L^v : K_v].$$

PROOF. We have

$$\mathbb{I}_{L,T} = \left(\prod_{v\in S}\left(\prod_{w|v} L_w^\times\right)\right) \times \left(\prod_{v\notin S}\left(\prod_{w|v} U_w\right)\right).$$

The Herbrand quotient of the second factor is 1 (apply III, 2.5), and so

$$\begin{aligned} h(G, \mathbb{I}_{L,T}) &= \prod_{v\in S} h(G, \textstyle\prod_{w|v} L_w^\times) \\ &= \prod_{v\in S} h(G^v, L^{v\times}) \\ &= \prod_{v\in S} \left|H^2(G^v, L^{v\times})\right| \\ &= \prod_{v\in S} n_v. \end{aligned}$$

□

The norm map on idéles

Let L/K be a finite Galois extension of number fields. As for any G-module, there is a norm map

$$x \mapsto \prod_{\sigma\in G} \sigma x : \mathbb{I}_L \to \mathbb{I}_L^G = \mathbb{I}_K.$$

We need to examine this map. Recall (ANT, 8.4) that there is a commutative diagram:

$$\begin{array}{ccc} L^\times & \longrightarrow & \prod_{w|v} L_w^\times \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle (a_w)\mapsto\prod \mathrm{Nm}_{L_w/K_v} a_w} \\ K^\times & \longrightarrow & K_v^\times. \end{array}$$

For every w, $\mathrm{Nm}\, L_w^\times$ is open in $K_v^\times$ (because it is of finite index; see I, 1.3), and for any unramified w, the norm map sends U_w onto U_v (see III, 1.2). The image of the right hand vertical map in the diagram is equal to $\mathrm{Nm}\, L_w^\times$ for any $w|v$ (because any two L_w's are K_v-isomorphic). We denote it by $\mathrm{Nm}\, L^{v\times}$.

Let $S \supset S_\infty$ be a finite set of primes of K containing those that ramify, and let T be the set of primes lying over a prime of S. The above remarks show that

$$\mathrm{Nm}_{L/K}\, \mathbb{I}_{L,T} = \prod_{v\in S} V_v \times \prod_{v\notin S} U_v,$$

where V_v is an open subgroup of finite index $K_v^\times$. This is an open subgroup in $\mathbb{I}_{K,S}$ and $\mathbb{I}_{K,S}$ is open in $\mathbb{I}_K$. We have proved the following result.

PROPOSITION 2.8 *For every finite Galois extension L/K of number fields, $\mathrm{Nm}_{L/K}\, \mathbb{I}_L$ contains an open subgroup of $\mathbb{I}_K$ and therefore is itself open.*

In fact, we showed earlier (V, 4.13) that every norm group contains $W_\mathfrak{m}$ for some modulus $\mathfrak{m}$, and $W_\mathfrak{m}$ is open.

We next consider the norm map on idèle classes. Consider

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \boldsymbol{C}_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \boldsymbol{C}_K & \longrightarrow & 0. \end{array}$$

The left hand square commutes, and so the norm map $\mathbb{I}_L \to \mathbb{I}_K$ induces a norm map $\mathrm{Nm}_{L/K}\colon \boldsymbol{C}_L \to \boldsymbol{C}_K$. From the snake lemma, we find that the quotient map $\mathbb{I}_K \to \boldsymbol{C}_K$ induces an isomorphism

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}(\mathbb{I}_L) \to \boldsymbol{C}_K/\mathrm{Nm}(C_L).$$

3 The Cohomology of the Units

Let L/K be a finite extension of number fields with Galois group G. Let $S \supset S_\infty$ be a finite set of primes of K, and let T be the set of primes of L lying over a prime of K in S. Because T is stable under the action of G, the group of T-units

$$U(T) \stackrel{\text{def}}{=} \{\alpha \in L \mid \mathrm{ord}_w(\alpha) = 0 \text{ all } w \notin T\}$$

is also stable under G.

PROPOSITION 3.1 *In the above situation, assume that G is cyclic. Then the Herbrand quotient $h(U(T))$ is defined, and satisfies*

$$n \cdot h(U(T)) = \prod_{v \in S} n_v,$$

where $n = [L : K]$ and $n_v = [L^v : K_v]$.

We first show that any two G-stable full lattices[2] in the same real vector space have the same Herbrand quotient. Then we construct two such lattices, one with Herbrand quotient $n \cdot h(U(T))$ and the other with Herbrand quotient $\prod n_v$.

LEMMA 3.2 *Let G be a finite group, and let k be an infinite field. Let M and N be $k[G]$-modules that are of finite dimension when regarded as k-vector spaces. If $M \otimes_k \Omega$ and $N \otimes_k \Omega$ are isomorphic as $\Omega[G]$ modules for some field $\Omega \supset k$, then they are already isomorphic as $k[G]$-modules.*

PROOF. First note that if V is the space of solutions for a system of homogeneous linear equations over k, then the solution space for the same system of equations over Ω admits a basis with coordinates in k. In fact, the standard algorithm for finding a basis for the solution space yields the same result when carried out over k or Ω.

A k-linear map $\alpha: M \to N$ is a G-homomorphism if $\alpha(\sigma m) = \sigma\alpha(m)$ all $m \in M$, $\sigma \in G$. Once bases have been chosen for M and N, giving a k-linear map $\alpha: M \to N$ is the same as giving a matrix A, and the condition that α be a G-homomorphism takes the form $A \cdot B(\sigma) = C(\sigma) \cdot A$ for certain matrices $B(\sigma)$ and $C(\sigma)$. This is a linear condition on the coefficients of A, and so the remark shows that there are $k[G]$-homomorphisms $\alpha_1, \dots, \alpha_r: M \to N$ that form an Ω-basis for the space of $\Omega[G]$-homomorphisms $M \otimes_k \Omega \to N \otimes_k \Omega$.

Because $M \otimes_k \Omega$ and $N \otimes_k \Omega$ are isomorphic as $\Omega[G]$-modules, there exist $a_1, \dots, a_r \in \Omega$ such that $\sum a_i\alpha_i$ is an isomorphism, and hence has nonzero determinant. But $\det(\sum a_i\alpha_i)$ is a polynomial in the a_i with coefficients in k, and the preceding sentence shows that not all of its coefficients are zero. As k is infinite, there exist a_i's in k such that $\sum a_i\alpha_i$ has nonzero determinant[3], and hence is a $k[G]$-isomorphism $M \to N$. □

REMARK 3.3 For those who find the above proof too simple, here is another. Assume that k has characteristic zero. The group H of automorphisms of M as a $k[G]$-module is a product of groups of the form $\mathrm{GL}_d(D)$, D a division algebra over k. The functor of isomorphisms $M \to N$ is a principal homogeneous space for H (nonempty, because there exists an isomorphism over some field containing k), and hence defines an element of $H^1(k, H)$. Now a generalization of Hilbert's theorem 90 shows that $H^1(k, H) = 1$.

LEMMA 3.4 *Let G be a finite cyclic group, and let M and N be G-modules that are finitely generated as $\mathbb{Z}$-modules, and such that $M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $N \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as G-modules. If either $h(M)$ or $h(N)$ is defined, so also is the other, and the two are equal.*

[2] Recall that a subgroup M of a real vector space V is called a ***full lattice*** if M is the $\mathbb{Z}$-submodule generated by a basis for V; equivalently, if it is finitely generated and the canonical map $\mathbb{R} \otimes_{\mathbb{Z}} M \to V$ is an isomorphism. The definition of a full lattice in a $\mathbb{Q}$-vector space is similar.

[3] We are using that a polynomial f with coefficients in an infinite field k is zero if $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots) \in k^n$ (FT, proof of 5.18).

PROOF. After (II, 3.9), we may assume that M and N are torsion free. Choose an isomorphism

$$\alpha: M \otimes \mathbb{Q} \to N \otimes \mathbb{Q}.$$

Then $\alpha(M)$ and N are lattices in the same $\mathbb{Q}$-vector space, and so $\alpha(M) \subset n^{-1}N$ for some $n \in \mathbb{N}$ (express the elements of a basis for $\alpha(M)$ in terms of a bases for N, and let n be a common denominator for the coefficients). After replacing α with $n\alpha$, we have that $\alpha(M) \subset N$. Now we have an exact sequence

$$0 \to M \xrightarrow{\alpha} N \to N/\alpha(M) \to 0$$

with $N/\alpha(M)$ finite, and we can apply (II, 3.9) again to deduce that $h(M) = h(N)$. □

LEMMA 3.5 *Let G be a finite cyclic group, and let V be a real vector space on which G acts linearly (i.e., V is an $\mathbb{R}[G]$-module). Let M and N be two G-stable full lattices in V. If either $h(M)$ or $h(N)$ is defined, then so is the other, and they are equal.*

PROOF. Because M and N are full lattices in V, the canonical maps

$$M \otimes_{\mathbb{Z}} \mathbb{R} \to V, \quad N \otimes_{\mathbb{Z}} \mathbb{R} \to V$$

are isomorphisms. These maps are G-homomorphisms, and therefore (3.2) $M \otimes_{\mathbb{Z}} \mathbb{Q} \approx N \otimes_{\mathbb{Z}} \mathbb{Q}$ as $\mathbb{Q}[G]$-modules, and we can apply Lemma 3.4. □

We now complete the proof of the Theorem. Let V be a product of copies of $\mathbb{R}$ indexed by the elements of T, i.e.,

$$V = \operatorname{Hom}(T, \mathbb{R}).$$

We let G act on V according to the rule:

$$(\sigma f)(w) = f(\sigma^{-1}w), \quad \sigma \in G, \quad w \in T.$$

The first lattice in V is $N \overset{\text{def}}{=} \operatorname{Hom}(T, \mathbb{Z})$. For each $v \in S$, choose a w lying over v, and let G^v be the decomposition group of w. The sets $G^v \cdot w$, $v \in S$, are the orbits of G acting on T. In particular, T is a disjoint union of these sets, and so

$$\operatorname{Hom}(T, \mathbb{Z}) = \bigoplus\nolimits_v \operatorname{Hom}(G/G^v, \mathbb{Z}).$$

But $\operatorname{Hom}(G/G^v, \mathbb{Z}) = \operatorname{Ind}_{G^v}^{G}(\mathbb{Z})$ ($\mathbb{Z}$ regarded as a trivial G^v-module). Therefore,

$$h(G, N) = \prod_v h(G, \operatorname{Ind}_{G^v}^{G}(\mathbb{Z})) = \prod h(G^v, \mathbb{Z}) = \prod n_v.$$

We now define the second lattice. Let $\lambda: U(T) \to V$ be the map $a \mapsto (\ldots, \log|a|_w, \ldots)$, and let M^0 to be the image of λ. Note that λ commutes with the action of G. The kernel of λ consists of the elements a of $L^\times$ such that $|a|_w = 1$ for all w (including the infinite primes). These are the roots of 1 in L, and so $h(U(T)) = h(M^0)$. The product formula shows M^0 is contained in the subspace

$$V^0: \sum x_w = 0,$$

of V, and the proof of the T-unit theorem shows that M^0 is a lattice in V^0 (cf. ANT, 5.8). The vector $e = (1, 1, \ldots, 1)$ is stable under G, and we define $M = M^0 + \mathbb{Z}e$. Then $M \otimes_{\mathbb{Z}} \mathbb{R} = V^0 + \mathbb{R}e = V$, and so M is a lattice in V. Moreover,

$$h(M) = h(M^0) \cdot h(\mathbb{Z}) = h(M^0) \cdot n.$$

This completes the proof Proposition 3.1.

4 Cohomology of the Idèle Classes I: the First Inequality

Let L/K be a finite Galois extension of number fields with Galois group G. We have a commutative diagram of G-modules with exact rows,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \boldsymbol{C}_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \boldsymbol{C}_L & \longrightarrow & 0, \end{array}$$

That the rows are exact is the definition of the idèle class groups. The vertical arrows in the left hand square are the natural inclusions. The square therefore commutes, which shows that the right hand vertical arrow exists.

LEMMA 4.1 *The canonical map $\boldsymbol{C}_K \to \boldsymbol{C}_L$ induces an isomorphism*

$$\boldsymbol{C}_K \to \boldsymbol{C}_L^G = H^0(G, \boldsymbol{C}_L).$$

PROOF. From the bottom row of the above diagram, we obtain a cohomology sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(G, L^\times) & \longrightarrow & H^0(G, \mathbb{I}_L) & \longrightarrow & H^0(G, \boldsymbol{C}_L) & \longrightarrow & H^1(G, L^\times) \\ & & \| & & \| & & \| & & \| \\ & & L^{\times G} & & \mathbb{I}_L^{\times G} & & \boldsymbol{C}_L^G & & 0 \end{array}$$

which can be identified with

$$0 \to K^\times \to \mathbb{I}_K \to \boldsymbol{C}_K \to 0.$$

□

The ideal class group of a number field is finite, and it is generated by the classes of prime ideals. Therefore, it is generated by a finite number of prime ideals.

LEMMA 4.2 *Let K be a number field, and let $S \supset S_\infty$ be a finite set of primes of K containing a set of generators for the ideal class group of K. Then*

$$\mathbb{I}_K = K^\times \cdot \mathbb{I}_S.$$

PROOF. The condition that S contains a set of generators for the ideal class group of K means that every fractional ideal $\mathfrak{a}$ can be written

$$\mathfrak{a} = \mathfrak{b} \cdot (c)$$

with $\mathfrak{b}$ in the group generated by the prime ideals in S and $c \in K^\times$. Therefore, $\mathfrak{a} = (c)$ in the quotient group $I^S = I/\langle S \rangle$, and so $I^S/i(K^\times) = 0$.

For every finite set $S \supset S_\infty$ of primes of K, the natural map $\mathbb{I} \to I^S$ defines an isomorphism $\mathbb{I}/\mathbb{I}_S \to I^S$. On dividing out by $K^\times$ on both sides, we find that $\mathbb{I}/K^\times \cdot \mathbb{I}_S \simeq I^S/i(K^\times) \simeq 0$. □

Recall that we want to prove that for every abelian extension L/K, $\boldsymbol{C}_K/\operatorname{Nm}_{L/K} \boldsymbol{C}_L \simeq \operatorname{Gal}(L/K)$ and that for every Galois extension $H^1(G, C_L) = 1$. For a cyclic extension, the two statements imply that the Herbrand quotient

$$h(\boldsymbol{C}_L) \overset{\text{def}}{=} \frac{(\boldsymbol{C}_K : \operatorname{Nm} \boldsymbol{C}_L)}{\left|H^1(G, \boldsymbol{C}_L)\right|} = [L : K].$$

As a first step, we verify this equality.

THEOREM 4.3 *For every finite cyclic extension L/K of number fields, $h(\boldsymbol{C}_L) = [L : K]$.*

PROOF. Let S any finite set of primes of K such that:

(a) $S \supset S_\infty$, the set of infinite primes of K;

(b) S contains all primes that ramify in L;

(c) S contains the prime ideals $\mathfrak{P} \cap \mathcal{O}_K$ for a set of generators $\mathfrak{P}$ of the ideal class group of L.

Let T be the set of primes of L lying over a prime in S. Condition (c) implies that $\mathbb{I}_L = \mathbb{I}_{L,T} \cdot L^\times$, and so

$$\boldsymbol{C}_L \stackrel{\text{def}}{=} \mathbb{I}_L/L^\times = L^\times \cdot \mathbb{I}_{L,T}/L^\times \simeq \mathbb{I}_{L,T}/L^\times \cap \mathbb{I}_T.$$

Note that

$$L^\times \cap \mathbb{I}_T = \{\alpha \in L \mid \operatorname{ord}_w(\alpha) = 0\,, \forall w \notin T\} = U(T),$$

and so

$$h(\boldsymbol{C}_L) = h(\mathbb{I}_{L,T})/h(U(T)).$$

The theorem now follows from Proposition 2.7 and Proposition 3.1. □

COROLLARY 4.4 (FIRST INEQUALITY) *If L/K is cyclic of degree n, then*

$$(\mathbb{I}_K : K^\times \cdot \operatorname{Nm}(\mathbb{I}_L)) \geq n.$$

PROOF. Since $h(\boldsymbol{C}_L) = n$, its numerator must be $\geq n$. □

We now give some application of the First Inequality.

LEMMA 4.5 *Let L be a finite solvable extension of K (i.e., a finite Galois extension with solvable Galois group). If there exists a subgroup D of $\mathbb{I}_K$ such that*

(a) $D \subset \operatorname{Nm}_{L/K} \mathbb{I}_L$; *and*

(b) $K^\times \cdot D$ *is dense in* $\mathbb{I}_K$

then $L = K$.

PROOF. If $L \neq K$, then the exists a subfield K' of L that is cyclic over K and $\neq K$. Then

$$D \subset \operatorname{Nm}_{L/K}(\mathbb{I}_L) = \operatorname{Nm}_{K'/K}(\operatorname{Nm}_{L/K} \mathbb{I}_L)) \subset \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'}).$$

Therefore, $K^\times \cdot \operatorname{Nm}_{K'/K} \mathbb{I}_{K'}$ is dense in $\mathbb{I}_K$. Because it is a union of translates of $\operatorname{Nm}_{K'/K} \mathbb{I}_{K'}$, it is open (2.8), and because it is a subgroup of $\mathbb{I}_K$, it is also closed. Therefore, $K^\times \cdot \operatorname{Nm}_{K'/K} \mathbb{I}_{K'} = \mathbb{I}_K$, and the first inequality implies that $K' = K$. □

PROPOSITION 4.6 *Let L be a finite solvable extension of K. If $L \neq K$, then there are infinitely many primes of K that do not split completely in L.*

PROOF. Suppose there are only finitely many, and let $S \supset S_\infty$ be a finite set of primes of K including all those that do not split completely. We shall apply the lemma with

$$D = \mathbb{I}^S \stackrel{\text{def}}{=} \{(a_v) \mid a_v = 1 \text{ for all } v \in S\}.$$

For $w|v \notin S$, $L_w = K_v$, and so clearly $D \subset \operatorname{Nm}(\mathbb{I}_L)$. Let $\mathbf{a} = (a_v) \in \mathbb{I}$. By the Weak Approximation Theorem (ANT, 7.20), there is an element $b \in K^\times$ that is very close to a_v in K_v for all $v \in S$. Choose $\mathbf{a}'$ to be the element of $\mathbb{I}^S$ such that the v component of $b\mathbf{a}'$ is equal to a_v for all $v \notin S$. Then $b\mathbf{a}'$ is close to $\mathbf{a}$ in $\mathbb{I}_K$. Hence $K^\times \cdot D$ is dense in $\mathbb{I}_K$. □

PROPOSITION 4.7 *Let L/K be a finite solvable extension with Galois group G, and let T be a finite set of prime ideals containing those that ramify in L. Then the Frobenius elements $(\mathfrak{P}, L/K)$ for $\mathfrak{P} \notin T$ generate G.*

PROOF. After possibly replacing T with a larger set, we may suppose that it is stable under G. Then the subgroup H of G generated by the Frobenius elements at the $\mathfrak{P} \notin T$ is normal. Let $E = L^H$. Recall (V, 1.11) that

$$(\mathfrak{P} \cap E, E/K) = (\mathfrak{P}, L/K)|_E,$$

which is the identity map. Therefore all primes $\mathfrak{p}$ of K not lying under a prime of T split in E, which shows that $E = K$. By the main theorem of Galois theory, this implies that $H = G$. □

COROLLARY 4.8 *For every abelian extension L/K and finite set of primes $S \supset S_\infty$ of K including the primes that ramify in L, the map*

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K)\colon I^S \to \mathrm{Gal}(L/K)$$

is surjective. (Recall that I^S is the group of fractional ideals generated by prime ideals not in S.)

PROOF. The image contains the Frobenius elements $(\mathfrak{P}, L/K)$ for all $\mathfrak{P}$ dividing a prime $\mathfrak{p}$ not in S, and these generate $\mathrm{Gal}(L/K)$. □

REMARK 4.9 Of course, Proposition 4.6 is much weaker than the result available using complex analysis—see Theorem VI.3.4—but it suffices for the proof of the Reciprocity Law.

5 Cohomology of the Idèle Classes II: The Second Inequality

THEOREM 5.1 *Let L/K be a Galois extension of number fields with Galois group G. Then*

(a) *(second inequality) the index $(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L))$ is finite, and divides $[L : K]$;*

(b) *the group $H^1(G, \boldsymbol{C}_L) = 0$;*

(c) *the group $H^2(G, \boldsymbol{C}_L)$ is finite, and its order divides $[L : K]$.*

LEMMA 5.2 *If G is cyclic, then statements (a), (b), and (c) of the theorem are equivalent (and $(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) = (H^2(G, \boldsymbol{C}_L) : 1) = [L : K]$).*

PROOF. Without restriction on G,

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L) \simeq \boldsymbol{C}_K/\mathrm{Nm}_{L/K}(\boldsymbol{C}_L) = H^0_T(G, \boldsymbol{C}_L).$$

If G is cyclic, its cohomology is periodic, and so $H^0_T(G, \boldsymbol{C}_L) \approx H^2(G, \boldsymbol{C}_L)$. This proves that (a) and (c) are equivalent. Theorem 4.3 states that the Herbrand quotient $h(\boldsymbol{C}_L) = [L : K]$, and so each of (a) and (c) is equivalent to (b). □

LEMMA 5.3 *It suffices to prove the theorem in the case that G is a p-group, p prime.*

PROOF. Recall (II, 1.33), that if H is the Sylow p-subgroup of G then, for every G-module M, the maps

$$\mathrm{Res} : H^r_T(G, M) \to H^r_T(H, M)$$

are injective on the p-primary components. Therefore, if the theorem holds for L/L^H, then p does not divide the order of $H^1_T(G, \boldsymbol{C}_L)$ and the power of p dividing the orders $H^0_T(G, \boldsymbol{C}_L)$ and $H^2_T(G, \boldsymbol{C}_L)$ is less than the power of p dividing $[L : K]$. On applying this for all p, we obtain the lemma. □

LEMMA 5.4 *It suffices to prove the theorem in the case that G is a cyclic group of prime order p.*

PROOF. After the last lemma, we may assume that G is a p-group. We shall prove the theorem for G by induction on $(G : 1)$. Because G is a p-group, it has a normal subgroup H of index p (see GT 4.17). Consider the exact sequence (II, 1.34)

$$0 \to H^1(G/H, \boldsymbol{C}_{K'}) \xrightarrow{\text{Inf}} H^1(G, \boldsymbol{C}_L) \xrightarrow{\text{Res}} H^1(H, \boldsymbol{C}_L),$$

where $K' = L^H$. By assumption $H^1(G/H, \boldsymbol{C}_{K'}) = 0$ and by induction $H^1(H, \boldsymbol{C}_L) = 0$. Therefore $H^1(G, \boldsymbol{C}_L) = 0$—statement (b) is true.

Because $H^1(H, \boldsymbol{C}_L) = 0$, the sequence

$$0 \to H^2(G/H, \boldsymbol{C}_{K'}) \to H^2(G, \boldsymbol{C}_L) \to H^2(H, \boldsymbol{C}_L)$$

is exact, from which it follows that statement (c) is true.

Finally, note that

$$(\boldsymbol{C}_K : \mathrm{Nm}_{L/K}(\boldsymbol{C}_L)) = (\boldsymbol{C}_K : \mathrm{Nm}_{K'/K}(\boldsymbol{C}_{K'}))(\mathrm{Nm}_{K'/K}(\boldsymbol{C}_{K'}) : \mathrm{Nm}_{L/K}(\boldsymbol{C}_L)),$$

which divides $p[L : K']$ because $\mathrm{Nm}_{K'/K}$ defines a surjection

$$\boldsymbol{C}_{K'}/\mathrm{Nm}_{L/K'}(\boldsymbol{C}_L) \to \mathrm{Nm}_{K'/K}(\boldsymbol{C}_{K'})/\mathrm{Nm}_{L/K}(\boldsymbol{C}_L).$$ □

To finish the proof of Theorem 5.1 using Lemma 5.2, it therefore remains to prove that the Second Inequality holds for a cyclic extension of degree p, but in VI 4.9 we proved that the Second Inequality holds for all finite Galois extensions. (For the translation between the idealic and the idèlic form of the statement, see Proposition V 4.6). In the next section, we give an algebraic proof of the Second Inequality, independent of Chapter VI.

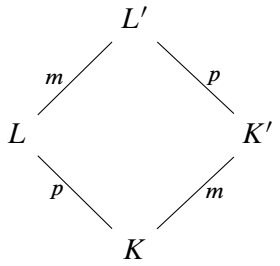
REMARK 5.5 To a finite Galois extension L/K of number fields, we have attached the group $\boldsymbol{C}_K/\mathrm{Nm}(\boldsymbol{C}_L)$ and $H^2(G, \boldsymbol{C}_L)$. When L/K is cyclic, they are canonically (up to a choice of a generator for G) isomorphic, but not otherwise. The first group is always isomorphic to G^{ab}, and the second is always cyclic of order $[L : K]$. Thus, when G is abelian but not cyclic, the two groups have the same order but are not isomorphic, and when G is nonabelian, they have different orders.

6 The Algebraic Proof of the Second Inequality

We shall prove the Second Inequality in the case that L/K is cyclic of prime degree p.

LEMMA 6.1 *It suffices to prove the Second Inequality in the case that K contains a pth root of 1.*

PROOF. Let ζ be a primitive pth root of 1 (in some fixed algebraic closure of K containing L), and let $K' = K[\zeta]$ and $L' = K' \cdot L = L[\zeta]$. Then $[K' : K] = m | p-1$, and so is relatively prime to p. Hence $K' \cap L = K$, and we have the picture:



The map

$$\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(K'/K)$$

is an isomorphism. Consider the diagram:

$$\begin{array}{ccccccc}
\boldsymbol{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \boldsymbol{C}_K & \longrightarrow & \boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} & & \downarrow & & \\
\boldsymbol{C}_{L'} & \xrightarrow{\mathrm{Nm}_{L'/K'}} & \boldsymbol{C}_{K'} & \longrightarrow & \boldsymbol{C}_{K'}/\mathrm{Nm}\,\boldsymbol{C}_{L'} & \longrightarrow & 0 \\
\downarrow{\scriptstyle \mathrm{Nm}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} & & \downarrow & & \\
\boldsymbol{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \boldsymbol{C}_K & \longrightarrow & \boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L & \longrightarrow & 0
\end{array}$$

Here i_L and i_K are the maps induced by the inclusions $\mathbb{I}_L \hookrightarrow \mathbb{I}_{L'}$ and $\mathbb{I}_K \hookrightarrow \mathbb{I}_{K'}$, $\mathrm{Nm}_{L/K}$ and $\mathrm{Nm}_{L'/K'}$ are the maps

$$x \mapsto \sum \sigma x, \quad \sigma \in \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L'/K'),$$

and $\mathrm{Nm}_{L'/L}$ and $\mathrm{Nm}_{K'/K}$ are the maps

$$x \mapsto \sum \sigma x, \quad \sigma \in \mathrm{Gal}(L'/L) \simeq \mathrm{Gal}(K'/K).$$

Clearly the squares at left commute, and this implies that the rest of the diagram exists. The composites

$$\mathrm{Nm}_{L'/L} \circ i_L \text{ and } \mathrm{Nm}_{K'/K} \circ i_K$$

are both multiplication by m. Therefore the composite

$$\boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L \to \boldsymbol{C}_{K'}/\mathrm{Nm}\,\boldsymbol{C}_{L'} \to \boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L$$

is also multiplication by m, and hence is an isomorphism (clearly, pth powers in $\boldsymbol{C}_K$ are norms, and so $\boldsymbol{C}_K/\mathrm{Nm}\,\boldsymbol{C}_L$ is killed by p). In particular, the second map is surjective, and so

$$(\boldsymbol{C}_K : \mathrm{Nm}\,\boldsymbol{C}_L) \text{ divides } (\boldsymbol{C}_{K'} : \mathrm{Nm}\,\boldsymbol{C}_{L'}),$$

which by assumption, divides p. □

We shall prove the Second Inequality in the case the K contains a primitive pth root of 1 and L is a finite abelian extension of K of exponent p with Galois group G. Let $[L : K] = p^r$, so that $G \approx (\mathbb{Z}/p\mathbb{Z})^r$. By Kummer theory (see the appendix to this chapter), there exist $a_1, \dots, a_r \in K$ such that

$$L = K[a_1^{\frac{1}{p}}, \dots, a_r^{\frac{1}{p}}].$$

Let S be a finite set of primes of K such that

(a) S contains the infinite primes;

(b) S contains all divisors of p;

(c) S is so large that all a_i are S-units.

(d) S contains a set of generators for the ideal class group of K, and so $\mathbb{I}_K = \mathbb{I}_{K,S} \cdot K^\times$ (see 4.2).

Note that, according to (A.5), conditions (b) and (c) imply that S contains all primes that ramify in L.

As usual, we write $U(S)$ for the group of S-units, i.e., the group of elements of $K^\times$ that are units for all primes outside S. Recall that the unit theorem says that

$$U(S) \approx \mathbb{Z}^{s-1} \times U(S)_{\text{tors}}, \qquad s = |S|.$$

The group $U(S)_{\text{tors}}$ is cyclic, and in our case its order is divisible by p (because it contains μ_p), and so

$$U(S)/U(S)^p \approx (\mathbb{Z}/p\mathbb{Z})^s.$$

Let $M = K[U(S)^{\frac{1}{p}}]$. This is the Kummer extension corresponding to the group

$$U(S) \cdot K^{\times p}/K^{\times p} \simeq U(S)/U(S) \cap K^{\times p} = U(S)/U(S)^p \approx (\mathbb{Z}/p\mathbb{Z})^s.$$

We therefore have extensions

$$M \overset{p^t}{\supset} L \overset{p^r}{\supset} K, \qquad r + t = s.$$

LEMMA 6.2 *There exists a finite set of primes T of K, disjoint from S, such that*

$$\{(\mathfrak{p}_v, M/K) \mid v \in T\}$$

is a basis for $\mathrm{Gal}(M/L)$ *(regarded as an $\mathbb{F}_p$-vector space).*

PROOF. Note S contains all primes of K ramified in M (by A.5). Therefore, for a prime w of M lying over a prime v not in S, the extension M_w/K_v is unramified, and hence is cyclic of exponent p. Therefore, it is either cyclic of order p or it is trivial. Thus, if $M_w \neq L_w$, then $L_w = K_v$ (here I'm using w both for the prime of M and the prime of L it divides).

According to (4.7), there exists a finite set T' of primes of M, none dividing a prime in S, such that the Frobenius elements $(\mathfrak{p}_w, M/L)$ for $w \in T'$ generate $\mathrm{Gal}(M/L)$. After replacing T' with a subset (if necessary), we may suppose that these Frobenius elements form a basis for $\mathrm{Gal}(M/L)$. Let $w \in T'$ divide the prime w_L of L and the prime w_K of K. Because $M_w \neq L_{w_L}$, we have $L_{w_L} = K_{w_K}$, and therefore $(\mathfrak{p}_w, M/L) = (\mathfrak{p}_w, M/K)$. Thus $T = \{w_K \mid w \in T'\}$ has the required property. □

Note that the order of T is t, where $p^t = [M : L]$, and that if w is a prime of M such that $w|v \in T$, then $L_w = K_v$.

LEMMA 6.3 *With the above notation, an element $a \in U(S)$ becomes a pth power in L if and only if it becomes a pth power in K_v for all $v \in T$.*

PROOF. $\Longrightarrow$: Let $a \in U(S)$. If a becomes pth power in L, then it becomes a pth power in $L_w^\times$ for all w. But if $w|v \in T$, then $L_w = K_v$, and so it becomes a pth power in K_v.

$\Longleftarrow$: Let $a \in U(S)$. Then $a^{\frac{1}{p}} \in M$. If $a^{\frac{1}{p}} \in K_v$ for all $v \in T$, then $a^{\frac{1}{p}}$ is fixed by $(\mathfrak{p}_v, M/K)$ for all $v \in T$, and hence by $\mathrm{Gal}(M/L)$. Thus, $a^{\frac{1}{p}}$ lies in L, and so $a \in L^p$. □

LEMMA 6.4 *The subgroup*

$$E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v$$

of $\mathbb{I}_K$ is contained in $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$.

PROOF. Let $\mathbf{a} = (a_v) \in E$. We have to show that each component a_v of $\mathbf{a}$ is a norm.

$v \in S$: From local class field theory, we know that

$$K_v^\times / \operatorname{Nm} L_w^\times \xrightarrow{\simeq} \mathrm{Gal}(L_w/K_v).$$

Because the second group is killed by p, so also must be the first group, which means that $K_v^{\times p} \subset \operatorname{Nm} L_w^\times$.

$v \in T$: Here $L_w = K_v$, and so every element of K_v is a norm from L_w.

$v \notin S \cup T$: Because L_w is unramified over K_v, the norm map $U_w \to U_v$ is surjective (see III, 1.2) □

Now

$$(\boldsymbol{C}_K : \operatorname{Nm} \boldsymbol{C}_L) = (\mathbb{I}_K : K^\times \cdot \operatorname{Nm} \mathbb{I}_L),$$

which divides $(\mathbb{I}_K : K^\times E)$, and so it remains to show that

$$\boxed{(\mathbb{I}_K : K^\times E) | p^r.}$$

But $\mathbb{I}_K = K^\times \cdot \mathbb{I}_S = K^\times \cdot \mathbb{I}_{S \cup T}$, and so

$$(\mathbb{I}_K : K^\times E) = (K^\times \mathbb{I}_{S \cup T} : K^\times E).$$

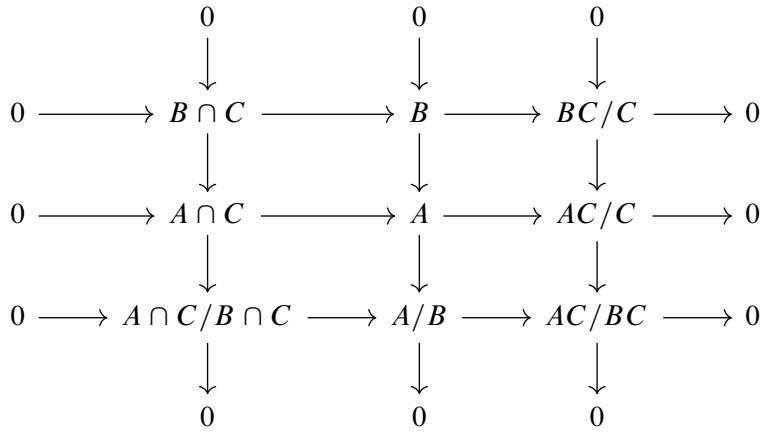
LEMMA 6.5 *Let A, B, and C be subgroups of some abelian group, and assume that $A \supset B$. Then*

$$(AC : BC)(A \cap C : B \cap C) = (A : B)$$

in the sense that, if two of the indexes are finite, so is the third, and the equality holds.

PROOF. In the following commutative diagram, the columns and the top two rows are obviously exact, and it follows (from the snake lemma for example) that the bottom row is

exact. This implies the statement.



□

On applying the lemma with $A = \mathbb{I}_{S\cup T}$, $B = E$, and $C = K^\times$ we find that

$$(\mathbb{I}_K : K^\times E) = \frac{(\mathbb{I}_{S\cup T} : E)}{(U(S \cup T) : K^\times \cap E)}.$$

LEMMA 6.6 *With the above notation:*

$$(\mathbb{I}_{S\cup T} : E) = p^{2s}.$$

LEMMA 6.7 *With the above notation:*

$$(U(S \cup T) : K^\times \cap E) = p^{s+t}.$$

Since $r + t = s$, this will prove the boxed formula.

PROOF (OF 6.6) Obviously $(\mathbb{I}_{S\cup T} : E) = \prod_{v\in S}(K_v^\times : K_v^{\times p})$. Since there are s primes in S and K contains p distinct pth roots of 1, the next proposition shows that

$$(\mathbb{I}_{S\cup T} : E) = \frac{p^{2s}}{\prod_{v\in S} |p|_v}.$$

By assumption, S contains all the primes for which $|p|_v \neq 1$, and so

$$\prod_{v\in S} |p|_v = \prod_{\text{all } v} |p|_v\,,$$

which equals 1 by the product formula. □

PROPOSITION 6.8 *Let K be a local field of characteristic zero, and let μ_n be the group of nth roots of 1 in $K^\times$. Then*

$$(K^\times : K^{\times n}) = n\frac{|\mu_n|}{|n|}.$$

If K is nonarchimedean and U is the group of units in K, then

$$(U : U^n) = \frac{|\mu_n|}{|n|}.$$

PROOF. If $K = \mathbb{C}$, the first equation becomes $1 = n\frac{n}{n^2}$, and if $K = \mathbb{R}$, it becomes $1 = n\frac{1}{n}$ when n is odd and $2 = n\frac{2}{n}$ when n is even. If K is nonarchimedean, $K^\times \approx U \times \mathbb{Z}$, and so

$$(K^\times : K^{\times n}) = (U : U^n)(\mathbb{Z} : n\mathbb{Z}) = (U : U^n)n.$$

Therefore, it remains to prove the second equation.

For an abelian group M, we write

$$h_n(M) = (M : nM)/(M_n : 1), \quad M_n = \{x \in M \mid nx = 0\}.$$

Then $h_n(M)$ is the Herbrand quotient of M regarded as a $\mathbb{Z}/n\mathbb{Z}$-module with trivial action, and so we may apply the results in II, §2.

As we saw in the proof of (III, 2.4), the exponential map defines an isomorphism from a subgroup of finite index in $\mathcal{O}_K$ onto a subgroup of finite index in U. Therefore

$$h_n(U) = h_n(\mathcal{O}_K) = (\mathcal{O}_K : n\mathcal{O}_K) \stackrel{\text{def}}{=} |n|^{-1}.$$

Hence

$$(U : U^n) = \frac{(U_n : 1)}{|n|}.$$

As $U_n = \mu_n$, this proves the second equation. □

PROOF (OF 6.7) Clearly $K^\times \cap E \supset U(S \cup T)^p$. It follows from the unit theorem (as before) that $(U(S \cup T) : U(S \cup T)^p) = p^{s+t}$, and so it remains to prove that

$$K^\times \cap E \subset U(S \cup T)^p.$$

This is accomplished by the next two lemmas (the first shows that the second may be applied to prove the inclusion). □

LEMMA 6.9 *With the above hypotheses, the obvious map*

$$U(S) \to \prod_{v \in T} U_v/U_v^p$$

is surjective.

PROOF. Let H be the kernel of the map. To prove that the map is surjective, we shall show that

$$(U(S) : H) = \prod_{v \in T} (U_v : U_v^p).$$

Because T is disjoint from S, $|p|_v = 1$ for all $v \in T$, and so (6.8) shows that the right hand side is p^t. On the other hand, by Lemma 6.3, $H = U(S) \cap L^{\times p}$, and so

$$U(S)/H = U(S)/U(S) \cap L^{\times p} \simeq U(S) \cdot L^{\times p}/L^{\times p}.$$

This last group corresponds by Kummer theory (see A.3) to the extension M/L, and hence has order $[M : L] = p^t$. □

PROPOSITION 6.10 *Let K be a number field containing a primitive nth root of 1. Let S be a set primes containing the infinite primes, the divisors of n, and a set of representatives of the ideal class group of K. Let T be a set of primes disjoint from S and such that*

$$U(S) \to \prod_{v\in T} U_v/U_v^n$$

is surjective. Suppose that $b \in K^\times$ is an nth power in K_v for all $v \in S$ and a unit outside $S \cup T$. Then $b \in K^{\times n}$.

PROOF. Let $L = K[b^{\frac{1}{n}}]$—we have to show that $L = K$. Put

$$D = \prod_{v\in S} K_v^\times \times \prod_{v\in T} U_v^n \times \prod_{v\notin S\cup T} U_v.$$

By Lemma 4.5, in order to show that $L = K$, it suffices to shows that

(a) $D \subset \mathrm{Nm}_{L/K}\, \mathbb{I}_L$, and

(b) $D \cdot K^\times = \mathbb{I}_K$.

(a) Let $\mathbf{d} = (d_v) \in D$. We have to check that d_v is a norm from $K_v[b^{\frac{1}{n}}]$ for all v.

$v \in S$: In this case $K_v[b^{\frac{1}{n}}] = K_v$, and so every element of K_v is a norm.

$v \in T$: By local class field theory, the index $(K_v^\times : \mathrm{Nm}\, K_v[b^{\frac{1}{n}}]^\times)$ is equal to the degree $[K_v[b^{\frac{1}{n}}] : K_v]$, which divides n. Hence every nth power in K_v is a norm.

$v \notin S \cup T$: Because nb is a unit at v, the field $K_v[b^{\frac{1}{n}}]$ is unramified over K_v, and hence every unit is a norm.

(b) Obviously $\mathbb{I}_S/D = \prod_{v\in T} U_v/U_v^n$, and by hypothesis $U(S) \to \prod_{v\in T} U_v/U_v^n$ is surjective. Hence $\mathbb{I}_S = D \cdot U(S)$, and therefore

$$\mathbb{I}_K = \mathbb{I}_S \cdot K^\times = D \cdot U(S) \cdot K^\times = D \cdot K^\times.$$

□

This completes the proof of Theorem 5.1 (the Second Inequality).

7 Application to the Brauer Group

We let $H^2(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$ and $H^2(/K) = H^2(\mathrm{Gal}(K^{\mathrm{al}}/K), K^{\mathrm{al}\times})$. Those who have read Chapter IV will recognize that $H^2(L/K) \simeq \mathrm{Br}(L/K)$ and $H^2(/K) = \mathrm{Br}(K)$.

THEOREM 7.1 *For every Galois extension L/K of number fields (possibly infinite), the canonical map*

$$H^2(L/K) \to \bigoplus\nolimits_v H^2(L^v/K_v)$$

is injective.

PROOF. Assume initially that L/K is a finite Galois extension with Galois group G. Because $H^1(G, \boldsymbol{C}_L) = 0$, the cohomology sequence of

$$0 \to L^\times \to \mathbb{I}_L \to \boldsymbol{C}_L \to 0$$

is

$$0 \to H^2(G, L^\times) \to H^2(G, \mathbb{I}_L) \to \cdots.$$

But

$$H^2(G, L^\times) = H^2(L/K)$$

and (see 2.5)

$$H^2(G, \mathbb{I}_L) = \bigoplus H^2(G^v, L^{v\times}) = \bigoplus H^2(L^v/K_v),$$

and so this proves the theorem in this case. To obtain the theorem for an infinite extension, pass to the limit over the finite Galois subextensions. □

An extension L/K of fields is said to be ***cyclotomic*** if $L \subset K[\zeta]$ for some root ζ of 1. The next proposition will play a role in the proof of the global reciprocity law

PROPOSITION 7.2 *For every $\beta \in H^2(/K)$, there exists a cyclic cyclotomic extension L of K such that β maps to zero in $H^2(/L)$.*

PROOF. The theorem shows that β is determined by its images in $H^2(K_v)$, and hence by the invariants $\operatorname{inv}_v(\beta_v) \in \mathbb{Q}/\mathbb{Z}$ (see Theorem 2.1, Chapter III). For every finite extension L of K and prime $w|v$ of L, $\operatorname{inv}_w(\beta|L) = [L_w : K_v] \cdot \operatorname{inv}_v(\beta)$ (ibid.), and so we have to find a cyclic cyclotomic extension L/K such that

$$[L^v : K_v] \cdot \operatorname{inv}_v(\beta_v) = 0 \bmod \mathbb{Z}$$

for all v. Note that, because $H^2(L/K)!!H^2(/K)$ maps into the direct *sum* of the local groups, $\operatorname{inv}_v(\beta_v) = 0$ for almost all v. Hence there exists an integer $m > 0$ such that $m \operatorname{inv}_v(\beta_v) = 0$ for all v. The existence of an L with the correct properties is ensured by the next lemma. □

LEMMA 7.3 *Given a number field K, a finite set S of finite primes of K, and an integer $m > 0$, there exists a totally complex cyclic cyclotomic extension L of K such that $m|[L^v : K_v]$ for all $v \in S$.*

PROOF. It suffices to prove this for $\mathbb{Q}$ and $m \cdot [K : \mathbb{Q}]$. Hence we can simply assume $K = \mathbb{Q}$.

Let l be a prime, and let ζ be a primitive l^rth root of 1 with $r > 2$. Then $\operatorname{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \simeq (\mathbb{Z}/l^r\mathbb{Z})^\times$, and

$$(\mathbb{Z}/l^r\mathbb{Z})^\times \approx \begin{cases} \Delta \times C(l^{r-1}) & l \text{ odd} \\ \Delta \times C(2^{r-2}) & l = 2 \end{cases}$$

where Δ is of order $l-1$ and 2 in the two cases and $C(t)$ denotes a cyclic group of order t (Serre 1970, II, 3.2). Therefore $L(l^r) \overset{\text{def}}{=} \mathbb{Q}[\zeta]^\Delta$ is a cyclic cyclotomic extension of $\mathbb{Q}$ of degree l^{r-2} or l^{r-3}.

Next consider $\mathbb{Q}_p[\zeta]$. If $p = l$, then $\mathbb{Q}[\zeta]$ is totally ramified over p, and so $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] = [\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(l^r)$. If $p \neq l$, then $\mathbb{Q}[\zeta]$ is totally unramified over p, and $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p]$ is the smallest integer t such that $l^r | p^t - 1$. In either case, we see that $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] \to \infty$ as $r \to \infty$. Thus, for every p, $[L(l^r)^p : \mathbb{Q}_p]$ is a power of l that tends to ∞ as r tends to ∞.

A product of cyclic groups of distinct prime power orders is again cyclic. Therefore, for distinct primes $l_1, \dots, l_s$, $L = L(l_1^{r_1}) \cdots L(l_s^{r_s})$ will be cyclic, and clearly, by choosing $l_1^{r_1} \dots l_s^{r_s}$ to be sufficiently large, we can ensure that the local degrees $m|[L^p : \mathbb{Q}_p]$ are divisible by m for all $p \in S$. □

In more concrete terms, the two results say that:

If a central simple algebra over K splits over K_v for all v, then it splits over K.

and

Every central simple algebra over K splits over a cyclic cyclotomic extension of K.

8 Completion of the Proof of the Reciprocity Law

Recall that, for a finite abelian extension L/K of number fields with Galois group G, we have defined a homomorphism $\phi_{L/K} : \mathbb{I}_K \to G$ such that $\phi_{L/K}(\mathbf{a}) = \prod_v \phi_v(a_v)$.

THEOREM 8.1 (a) *Let L/K be a finite abelian extension of number fields. Then $\phi_{L/K}$ takes the value 1 on the principal idèles $K^\times \subset \mathbb{I}_K$.*

(b) *Let L/K be a finite Galois extension of number fields. Then $\sum \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$.*

Before proving this theorem, we explain why (a) implies the Reciprocity Law for L/K. Statement (a) says that $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ contains $K^\times$ in its kernel. We know already that it contains $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$ in its kernel[4], and therefore it defines a homomorphism

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L \to \mathrm{Gal}(L/K) \qquad (*).$$

For any finite prime v of K unramified in L, $\phi_{L/K}$ maps the idèle with a prime element in v-position to the Frobenius element $(\mathfrak{p}_v, L/K)$, and so (4.7) shows that $\phi_{L/K}$ is surjective. On the other hand, the Second Inequality (5.1) states that

$$(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L) \le [L : K]$$

and so the homomorphism $(*)$ is an isomorphism.

EXAMPLE 8.2 We verify (8.1a) for the extension $\mathbb{Q}[\zeta_m]/\mathbb{Q}$, where ζ_m a primitive mth root of 1. We identify $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^\times$. Thus, for n an integer relatively prime to m, $[n]$ denotes the automorphism of $\mathbb{Q}[\zeta_m]$ sending ζ_m to ζ_m^n. It suffices to show that $\phi(a)|\mathbb{Q}[\zeta_{l^r}] = 1$ for all $l|m$. Thus, we may assume that $m = l^r$, $m \neq 2$.

The homomorphism $\phi_\infty : \mathbb{R}^\times/\mathrm{Nm}(\mathbb{C}^\times) \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ sends any negative real number to complex conjugation. Therefore $\phi_\infty(a) = [\mathrm{sign}(a)]$.

Let $a = up^s \in \mathbb{Q}_p^\times$. If $p \neq l$, then p is unramified in $\mathbb{Q}[\zeta_m]$, and $\phi_p(a)$ acts as the sth power of the Frobenius at p:

$$\phi_p(up^s) = [p^s].$$

The prime l is totally ramified in $\mathbb{Q}[\zeta_m]$ and

$$\phi_l(a) = [u^{-1}]$$

(see I, 3.13).[5]

[4] Because this is true locally.

[5] As Catherine O'Neil pointed out to me, here I'm making use of a result from I §3, contrary to my promise that §§2–4 of Chapter I can be skipped. However, it is possible to prove (a) of Theorem 8.1 in an elementary fashion for the cyclotomic extensions of $\mathbb{Q}$. For example, use the diagram in V, 5.10, to define $\phi_{\mathbb{Q}}$, and then verify that its local components are correct. This will be clarified in a future version. (See also Remark 8.3.)

It suffices to show that $\phi(a) = 1$ in the three cases: $a = -1$, $a = l$, $a =$ a prime $q \neq l$. We have:

$$\phi_p(-1) = \begin{cases} [-1] & \text{if} \quad p = \infty \\ [-1] & \text{if} \quad p = l \\ [1] & \text{if} \quad p \neq l, \infty. \end{cases}$$

$$\phi_p(l) = \begin{cases} [1] & \text{if} \quad p = l \\ [1] & \text{if} \quad p \neq l \end{cases}$$

$$\phi_p(q) = \begin{cases} [q] & \text{if} \quad p = q \\ [q^{-1}] & \text{if} \quad p = l \\ [1] & \text{if} \quad p \neq l, q. \end{cases}$$

In each case, $\prod \phi_p(a) = 1$.

REMARK 8.3 In Example V 4.10, we showed that the homomorphism $\phi : \mathbb{I}_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ attached to the Artin map $\phi : C_{\infty(m)} \to \mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ has local components equal to the local Artin maps. Since, by definition, $\phi(\mathbb{Q}^\times) = 1$, this gives an alternative proof of (8.1a) in the case $\mathbb{Q}[\zeta_m]/\mathbb{Q}$.

LEMMA 8.4 (a) *If 8.1(a) holds for L/K, then it holds for every subextension.*

(b) *If 8.1(a) holds for L/K, then it holds for $L \cdot K'/K'$ for every number field $K' \supset K$.*

PROOF. (a) Suppose $L \supset K' \supset K$. Then $\phi_{K'/K}$ is the composite of $\phi_{L/K}$ and the restriction map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K)$ (because this is true for the local Artin maps).

(b) Let $L' = L \cdot K'$. For each prime w of K', we have a commutative diagram

$$\begin{array}{ccc} K_w'^\times & \xrightarrow{\phi_w} & \mathrm{Gal}(L'^w/K'_w) \\ \downarrow \mathrm{Nm} & & \downarrow \\ K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L^v/K_v). \end{array}$$

On combining them, we get a commutative diagram:

$$\begin{array}{ccc} \mathbb{I}_{K'} & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \downarrow \mathrm{Nm} & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Because the norm map on idèles maps $K'^\times$ into $K^\times$, we see that this lemma follows from earlier results. □

From the Example 8.2 and Lemma 8.4, we find that (8.1a) holds for all cyclotomic extensions[6] of a number field K.

We next need to relate the two statements in Theorem 8.1.

LEMMA 8.5 *Let L/K be an abelian extension of number fields. If (8.1b) holds for L/K, then so also does (8.1a). Conversely, if L/K is cyclic and (8.1a) holds for L/K, then so also does (8.1b).*

[6] An extension L/K is said to be cyclotomic if $L \subset K[\zeta]$ for some root ζ of 1.

PROOF. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. We can regard χ as an element of $H^1(G, \mathbb{Q}/\mathbb{Z})$, and then its image under the boundary map arising from the sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

is an element $\delta\chi \in H^2(G, \mathbb{Z})$. Consider the diagram,

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G \\ \downarrow{\scriptstyle \cup\delta_\chi} & & \downarrow{\scriptstyle \cup\delta_\chi} & & \downarrow{\scriptstyle \chi} \\ H^2(G, L^\times) & \longrightarrow & H^2(G, \mathbb{I}_L) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The first two vertical arrows are cup-product by $\delta\chi$: if $\delta\chi$ is represented by the 2-cocycle $n_{\sigma,\tau}$ then the image of x is represented by the 2-cocycle $\sigma, \tau \mapsto x^{n_{\sigma,\tau}}$. Clearly, the left-hand square commutes. The right-hand vertical map is χ itself. That the right hand square commutes follows from (III, 3.6). Now assume 8.1b is true for L/K. Then $\chi(\phi_{L/K}(a)) = 0$ for all characters χ of G, and so $\phi_{L/K}(a)$ itself is zero. Conversely, when G is cyclic, we can choose χ to be injective, and then 8.1a implies 8.1b since $\cup\delta_\chi$ is then an isomorphism (II, 3.5). □

Since we know 8.1a for cyclotomic extensions, it follows that we know 8.1b for cyclic cyclotomic extensions. Moreover, we will have proved the whole theorem once we have proved (b) of the theorem. Thus, the next result completes the proof of the theorem

LEMMA 8.6 *If (8.1b) is true for cyclic cyclotomic extensions, then it is true for all finite Galois extensions.*

PROOF. Let $\beta \in H^2(\ /K)$. We are given that, if $\beta \in H^2(L/K)$ for some cyclic cyclotomic extension L/K, then $\sum \mathrm{inv}_v(\beta) = 0$, where β_v is the image of β in $H^2(K_v)$, but Proposition 7.2 says that ***every*** β in $H^2(K)$ lies in $H^2(L/K)$ for some cyclic cyclotomic extension L/K.

[Mention that we are using the inflation-restriction sequence

$$0 \to H^2(\mathrm{Gal}(L/K), L^\times) \to H^2(G_K, \bar{K}^\times) \to H^2(G_L, \bar{L}^\times),$$

and that β as above is in the middle group and vanishes in the right-hand group.] □

9 The Existence Theorem

In this section we prove the Existence Theorem: every open subgroup of finite index in the idèle class group is a norm group. A large part of the proof can be extracted from Section 6. However, at the cost of some repetition, I give a proof independent of Section 6 (except for some elementary statements).

LEMMA 9.1 *If U is a norm group, and $V \supset U$, then V also is a norm group.*

PROOF. Suppose $U = \mathrm{Nm}\, \boldsymbol{C}_L$. According to the Reciprocity Law, the Artin map defines an isomorphism

$$\phi : \boldsymbol{C}_K/U \to \mathrm{Gal}(L/K).$$

If M is the fixed field of $\phi(V)$, then ϕ defines an isomorphism

$$\boldsymbol{C}_K/V \to \mathrm{Gal}(M/K),$$

but, according to the Reciprocity Law, the kernel of $\phi : \boldsymbol{C}_K \to \mathrm{Gal}(M/K)$ is $\mathrm{Nm}_{M/K}\boldsymbol{C}_M$.□

It is obvious from its factorization into primes, that a rational number a is an nth power if and only if it is an nth power in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes $p|a$. The proof of the analogous statement for number fields requires the Reciprocity Law (or complex analysis).

PROPOSITION 9.2 *Let K be a number field containing a primitive nth root of 1, and let $S \supset S_\infty$ be a finite set of primes of K containing all those dividing n and enough primes to generate the class group of K. Any $a \in K^\times$ such that*

- *a is an nth power in K_v for all $v \in S$;*
- *a is a unit in K_v for all $v \notin S$.*

is an nth power in K.

PROOF. [7] Let $L = K[a^{1/n}]$—because $\zeta_n \in K$, this is an abelian extension of K. For every prime $v \in S$, $X^n - a$ splits completely in $K_v[X]$, and so $L_w = K_v$ for all $w|v$. Hence the norm map $L_w^\times \to K_v^\times$ is onto. On the other hand, L is unramified over K at any prime $v \notin S$, and so the norm map $\mathrm{Nm}_{L/K} : U_w \to U_v$ is onto. Therefore, $\mathrm{Nm}_{L/K}(\mathbb{I}_L) \supset \mathbb{I}_S$, and so

$$K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L) \supset K^\times \cdot \mathbb{I}_S = \mathbb{I}_K.$$

The Reciprocity Law now shows that $L = K$, and so a is an nth power in K. □

LEMMA 9.3 (KEY CASE OF THE EXISTENCE THEOREM) *Let K be a number field containing a primitive pth root of 1 (p prime). Then every open subgroup V of $\boldsymbol{C}_K$ such that $\boldsymbol{C}_K/V$ is a finite group killed by p is a norm group.*

PROOF. Let $S \supset S_\infty$ be a finite set of primes of K containing the infinite primes, those dividing p, and enough primes so that $\mathbb{I}_K = K^\times \cdot \mathbb{I}_S$. Let L be the extension of K corresponding by Kummer theory to the group $U(S) \cdot K^{\times p}$, i.e., $L = K[U(S)^{\frac{1}{p}}]$, and let

$$E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v.$$

We shall prove that $K^\times \cdot E = K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)$ by verifying that

(a) $E \subset \mathrm{Nm}(\mathbb{I}_L)$;

(b) $(\mathbb{I}_K : K^\times \cdot E) = p^s = (\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L))$.

For any prime v of K and prime w of L lying over it, the local Artin map is an isomorphism

$$K_v^\times / \mathrm{Nm}(L_w^\times) \to \mathrm{Gal}(L_w/K_v).$$

Because L/K is has exponent p, $\mathrm{Nm}(L_w^\times) \supset K_v^{\times p}$.

[7] From Wojtek Wawrów: Since $L = K$ in the proof is cyclic, it appears that the proof only uses the First Inequality (specifically Lemma 4.5), not the full Reciprocity Law. Regardless, it appears that this Proposition is not used anywhere.

For any prime $v \notin S$, L is unramified over K and v, and so the norm map $U_w \to U_v$ is onto.

On combining the statements in the last two paragraphs, we obtain (a).

From the Reciprocity Law,

$$(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) = [L : K],$$

and from Kummer theory,

$$[L : K] = (U(S) \cdot K^{\times p} : K^{\times p}).$$

But

$$U(S) \cdot K^{\times p}/K^{\times p} \approx U(S)/U(S) \cap K^{\times p}.$$

If $a^p \in U(S)$, then $a \in U(S)$, and so $U(S) \cap K^{\times p} = U(S)^p$. Now, by the Dirichlet Unit Theorem (ANT, 5.9),

$$U(S) \approx U(S)_{\text{ torsion}} \oplus \mathbb{Z}^{s-1},$$

and $U(S)_{\text{ torsion}}$ is the group of roots of 1 in K, which is a cyclic group whose order is divisible by p. Hence $(U(S) : U(S)^p) = p^s$.

On the other hand,

$$(\mathbb{I}_K : K^\times \cdot E) = (\mathbb{I}_S \cdot K^\times : E \cdot K^\times),$$

which, by (6.5), equals

$$(\mathbb{I}_S : E)/(\mathbb{I}_S \cap K^\times : E \cap K^\times).$$

Therefore (see 6.8),

$$(\mathbb{I}_S : E) = \prod_{v \in S} (K_v^\times : K_v^{\times p}) = \prod_{v \in S} \frac{p}{|p|_v} p = p^{2s}.$$

Here, we have used that K contains a primitive pth root of 1 and that S contains all v for which $|p|_v \neq 1$, and so $\prod_{v \in S} |p|_v = \prod_{\text{all } v} |p|_v = 1$ by the product formula. It follows that $K^\times \cdot E = K^\times \cdot \mathrm{Nm}\, \mathbb{I}_L$.

Now let V be an open subgroup of $\boldsymbol{C}_K$ such that $\boldsymbol{C}_K/V$ is killed by p, and let U be the inverse image of V in $\mathbb{I}_K$. Then U is open in $\mathbb{I}_K$ and so there is a finite set of primes S such that $U \supset \prod_{v \in S} 1 \times \prod_{v \notin S} U_v$. Moreover, $\mathbb{I}_K/U$ has exponent p, and so $U \supset \mathbb{I}_K^p$. Hence $U \supset E \cdot K^\times$, and because $E \cdot K^\times/K^\times$ is a norm group, so also must be $U/K^\times = V$. □

For simplicity, in the proof of the next lemma, we assume the Norm Limitation Theorem, which is not proved until the next chapter. For a proof avoiding that theorem, see p. 202 of Tate's article in Cassels and Fröhlich 1967, 1967.

LEMMA 9.4 *Let U be an open subgroup of finite index in $\boldsymbol{C}_K$. If there exists a finite extension K'/K such that $\mathrm{Nm}_{K'/K}^{-1}(U)$ is a norm group, then so also is U.*

PROOF. Write U' for $\mathrm{Nm}_{K'/K}^{-1}(U)$, and let L be the abelian extension of K' with $\mathrm{Nm}\, \boldsymbol{C}_L = U'$. If M is the maximum abelian subextension of L/K, then we have

$$\mathrm{Nm}_{M/K}\, \boldsymbol{C}_M = \mathrm{Nm}_{L/K}\, \boldsymbol{C}_L = \mathrm{Nm}_{K'/K}\, U' \subset U$$

and we can apply Lemma 9.1. □

THEOREM 9.5 *Every subgroup U of finite index in $\boldsymbol{C}_K$ is a norm group.*

PROOF. We prove this by induction on the index of U. If the index is 1, then there is nothing to prove. Otherwise, there exists a prime p dividing $(\boldsymbol{C}_K : U)$. After (9.4) we may assume that K contains a pth root of 1. Choose a subgroup U_1 of $\boldsymbol{C}_K$ containing U and of index p in $\boldsymbol{C}_K$. After (9.3), there exists an abelian extension K' of K such that $\mathrm{Nm}_{K'/K}\boldsymbol{C}_{K'} = U_1$; moreover K' is cyclic of degree p over K. Put $U' = \mathrm{Nm}^{-1}_{K'/K}U$. The map

$$\mathrm{Nm}_{K'/K} : \boldsymbol{C}_{K'} \to \boldsymbol{C}_K/U$$

has image U_1/U and kernel U'. Hence

$$(\boldsymbol{C}_{K'} : U') = (\boldsymbol{C}_K : U)/p$$

and so, by induction, U' is a norm group. Now we can apply (9.4) to deduce that U is a norm group. □

A Appendix: Kummer theory

Throughout this subsection, K is a field containing a primitive nth root of 1, ζ. In particular, K either has characteristic 0 or characteristic p not dividing n. Write μ_n for the group of nth roots of 1 in K. Then μ_n is a cyclic subgroup of $K^\times$ of order n with generator ζ.

PROPOSITION A.1 *Let $L = K[\alpha]$, where $\alpha^n \in K$ and no smaller power of α is in K. Then L is a Galois extension of K with cyclic Galois group of order n. Conversely, if L is cyclic extension of K of degree n, then $L = K[\alpha]$ for some α with $\alpha^n \in K$.*

PROOF. See FT 5.26. □

PROPOSITION A.2 *Two cyclic extensions $K[a^{\frac{1}{n}}]$ and $K[b^{\frac{1}{n}}]$ of K of degree n are equal if and only if $a = b^r c^n$ for some $r \in \mathbb{Z}$ relatively prime to n and some $c \in K^\times$, i.e., if and only if a and b generate the same subgroup of $K^\times/K^{\times n}$.*

PROOF. See FT 5.28. □

The last two results give us a complete classification of the cyclic extensions of K of degree n when K contains a primitive nth root of 1. It is not difficult to extend this to a classification of all abelian extensions of exponent n.

THEOREM A.3 *The map*

$$L \mapsto K^\times \cap L^{\times n}/K^{\times n}$$

defines a one-to-one correspondence between the finite abelian extensions of K of exponent n contained in some fixed algebraic closure Ω of K and the finite subgroups B of $K^\times/K^{\times n}$. The extension corresponding to B is $K[B^{\frac{1}{n}}]$, the smallest subfield of Ω containing K and an nth root of each element of B. If $L \leftrightarrow B$, then $[L : K] = (B : K^{\times n})$.

PROOF. See FT 5.29. □

EXAMPLE A.4 (a) The quadratic extensions of $\mathbb{R}$ are in one-to-one correspondence with the subgroups of $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$.

(b) The finite abelian extensions of $\mathbb{Q}$ of exponent 2 are in one-to-one correspondence with the finite subgroups of

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \approx \{\pm 1\} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$$

(copies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the prime numbers).

After this review of algebra, we return to some number theory.

PROPOSITION A.5 *Let K be a number field, and let $L = K[a_1^{\frac{1}{n}}, \cdots, a_m^{\frac{1}{n}}]$. Then L is unramified at a finite prime v of K if na_i is a unit in K_v for all i.*

PROOF. We need only consider a cyclic extension $K[a^{\frac{1}{n}}]$, which (see A.1) we can assume to have degree n. Let $\alpha = a^{\frac{1}{n}}$ and $f = X^n - a$. Then

$$\operatorname{disc} f = \pm \operatorname{Nm}_{L/K} f'(\alpha) = \pm \operatorname{Nm}_{L/K} n\alpha^{n-1} = \pm n^n a^{n-1}.$$

Thus if $\mathfrak{p}_v$ does not divide na, it does not divide $\operatorname{disc} f$, and, *a fortiori,* it does not divide $\operatorname{disc}(\mathcal{O}_L/\mathcal{O}_K)$. (See ANT, Chapter 2.) □

REMARK A.6 Determining the ramification in $K[a^{\frac{1}{n}}]/K$ at prime $\mathfrak{p}$ dividing n can be quite complicated. The following summarizes what happens when $n = p$, a prime, and K contains a primitive pth root ζ of 1. Let $\pi = \zeta - 1$, and let $a \in K^\times$ be relatively prime to p and not a pth power in K.

(a) A prime $\mathfrak{p}|p$ splits completely in the extension $K[a^{\frac{1}{p}}]/K$ if and only if $X^p \equiv a \mod p\pi\mathfrak{p}$ has a nonzero solution in $\mathcal{O}_K$ (a is then said to be ***hyperprimary*** at $\mathfrak{p}$).

(b) A prime $\mathfrak{p}|p$ is unramified in the extension $K[a^{\frac{1}{p}}]/K$ if and only if $X^p \equiv a \mod p\pi$ has a nonzero solution in $\mathcal{O}_K$ (a is then said to be ***primary*** at $\mathfrak{p}$).

(c) The extension $K[a^{\frac{1}{p}}]/K$ is unramified at all finite primes of K if and only if a is primary and $(a) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$.

For hints of proofs of these statements, see Washington 1997, Exercise 9.3, and Cassels and Fröhlich 1967, Exercise 2.12, p. 353. In the case $K = \mathbb{Q}[\zeta]$, see also Cassels 1986, pp 139–140, and Fröhlich and Taylor 1991, III, 3.11.

Chapter VIII

Complements

In this Chapter, we add some complements to the theory of class fields, and we give some applications. In particular, we extend the results proved in Serre 1970, Chapters I–IV, VI, to arbitrary number fields.

1 When are local nth powers global nth powers?

Obviously, if an element a of a number field K is an nth power in K, then it is an nth power in K_v for all primes v of K. In this section, we investigate whether there is a converse.

THEOREM 1.1 *Let K be a number field containing a primitive nth root of 1. A nonzero element of K is an nth power in K if it is an nth power in K_v for all but possibly finitely many primes v.*

PROOF. Recall that, for a field k containing a primitive nth root of 1, a polynomial $X^n - a$ splits completely in $k[X]$ if it has a root k. Let a be a nonzero element of K, and let β be an nth root of a in some extension field. If a is an nth power in K_v for almost all v, then $X^n - a$ splits completely in $K_v[X]$ for almost all v, and so v splits completely in $K[\beta]$. Since this holds for almost all v, (VII, 4.6) shows that $K[\beta] = K$. □

REMARK 1.2 If we use (VI, 3.4) rather than (VII, 4.6), we obtain the stronger result: under the hypothesis of the theorem, a nonzero element of K is an nth power in K if it becomes an nth power in K_v for a set of primes v of density $> 1/2$.

One may hope that the theorem is true even when K doesn't contain a primitive nth root of 1, but the following exercise shows that it isn't, even for $K = \mathbb{Q}$ and $n = 8$.

EXERCISE 1.3 Show that 16 is an 8th power in $\mathbb{R}$ and $\mathbb{Q}_p$ for all odd p, but (as the ancient Greeks knew) not in $\mathbb{Q}$. (Hint: Show that $\mathbb{Q}[\zeta_8] = \mathbb{Q}[i, \sqrt{2}]$ is unramified at all odd p, and deduce that, for p odd, $\mathbb{Q}_p$ contains at least one of $1 + i$, $\sqrt{2}$, or $\sqrt{-2}$.)

The field $\mathbb{Q}[\zeta_8]$ is not cyclic over $\mathbb{Q}$, and so the exercise doesn't contradict the following theorem.

THEOREM 1.4 *Let K be a number field, and let n be an integer such that $K[\zeta_{2^t}]$ is cyclic over K, where 2^t is the power of 2 dividing n. A nonzero element of K is an nth power in K if it is an nth power in K_v for all but possibly finitely many primes v.*

PROOF. STEP 1. *It suffices to prove the theorem with n a prime power.* Suppose $n = n_1n_2$ with n_1 and n_2 relatively prime, and assume that the theorem holds for n_1 and n_2. Then a nonzero element a of K that is an nth power in K_v for almost all v is both an n_1th and an n_2th power in K, say, $a = b^{n_1}$, $a = c^{n_2}$. Now, there exist integers r and s such that $rn_1 + sn_2 = 1$, and so

$$a = a^{rn_1}a^{sn_2} = c^{rn_1n_2}b^{sn_1n_2} \in K^{\times n}.$$

STEP 2. *The theorem is true if n is a power of a prime p and $K[\zeta_n]/K$ is a cyclic extension of p-power order.* Let $K' = K[\zeta_n]$, and let a be a nonzero element of K that becomes an nth power in K_v for almost all v. According to Theorem 1.1, a becomes an nth power in K', say, $a = \beta^n$, and so

$$X^n - a = \prod_{j=0}^{n-1}(X - \beta\zeta_n^j) \text{ in } K'[X].$$

Let

$$X^n - a = \prod_i f_i(X)$$

be the decomposition of $X^n - a$ into irreducible factors in $K[X]$. For each i, choose a root $\beta_i = \beta\zeta_n^{j(i)}$ of $f_i(X)$. Then $K[\beta_i] \subset K'$, and so $K[\beta_i]$ is an abelian extension of K — in particular, it is Galois over K, and so is the splitting field of $f_i(X)$. Let v be a prime of K such that a is an nth power in K_v. By hypothesis, $X^n - a$ has a root in K_v, and hence at least one of the $f_i(X)$ has a root in K_v. For that particular i, v splits completely in $K[\beta_i]$. Thus we see that every v not in S splits completely in at least one of the fields $K[\beta_i]$, but different v may split in different fields, and so we can conclude nothing from this. To see that all the v split in a single $K[\beta_i]$ we have to use the hypothesis that K' is cyclic of prime power order over K. This hypothesis implies that the intermediate fields are linearly ordered:

$$K' \supset \cdots \supset K_3 \supset K_2 \supset K_1 \supset K.$$

Choose i_0 so that $K[\beta_{i_0}]$ is the smallest of the $K[\beta_i]$. Then every $v \notin S$ splits completely in a field containing $K[\beta_{i_0}]$, and hence in $K[\beta_{i_0}]$. Thus $K[\beta_{i_0}] = K$, and $X^n - a$ has at least one root in K.

STEP 3. *The theorem is true.* After Step 1, we may assume $n = p^r$, and after Step 2, that p is odd. Suppose that a is an nth power in K_v for almost all v. Because $K[\zeta_{p^r}]$ is cyclic of p-power order over $K[\zeta_p]$, Step 3 shows that a becomes an nth power in $K[\zeta_p]$, say, $a = b^n$. On taking norms, we find that a^d is an nth power in $K^\times$, where $d = [K[\zeta_p] : K] < p$. But d is relatively prime to p, and so this implies that a is an nth power in $K^\times$ (we know that $a^d = 1$ in $K^\times/K^{\times p^r}$, and this implies that $a = 1$ in $K^\times/K^{\times p^r}$). □

REMARK 1.5 (a) For a finite set S of primes of K and an integer n, let $P(n, S)$ be the group of all $a \in K^\times$ such that $a \in K_v^{\times n}$ for all $v \notin S$. On analysing the 2^t case further, one finds that either $P(n, S) = K^{\times n}$ or there exists an $a_0 \in K^\times$ such that $P(n, S) = K^{\times n} \sqcup a_0K^{\times n}$. For example, for $K = \mathbb{Q}$, $P(8, S) = \mathbb{Q}^{\times 8} \sqcup 16\mathbb{Q}^{\times 8}$ (Artin and Tate 1961, p. 96; p. 75 in the 2009 edition). Note that $P(n, S)/K^{\times n}$ is the group making

$$0 \to P(n, S)/K^{\times n} \to K^\times/K^{\times n} \to \mathbb{I}_K/\mathbb{I}_K^n \to \mathbf{C}_K/\mathbf{C}_K^n \to 0$$

exact.

(b) The fact that the statement of the theorem doesn't hold for all K, S, n can be regarded as a pathology of small number fields. For example, if $\sqrt{-1} \in K$, then $K[\zeta_{2^\ell}]$ is cyclic over K.

(c) The key step in the proof is Step 2, and is a little subtle. This is where Whaples went astray in his proof of Grunwald's "theorem" — he let $a^{\frac{1}{n}}$ denote a root of $X^n - a$, and forgot that the different roots may have quite different properties relative to K (e.g., their minimal polynomials are the f_i which may even have different degrees). Artin and Tate explicitly warn against trying to shorten the above argument.

2 The Grunwald-Wang Theorem

Class field theory "solves" all questions about abelian extensions by translating them into questions about open subgroups of finite index in the idèle class group. Unfortunately, questions about open subgroups of finite index in the idèle class group can also be difficult. In this section, we consider the following question.

QUESTION 2.1 Let K be an algebraic number field, and suppose that, for each prime v in a finite set S, we are given a finite cyclic extension K^v of K_v of degree n_v. Does there exist a finite cyclic extension L/K of degree $n = \operatorname{lcm}(n_v)$ such that $L^v \approx K^v$? (This condition means that there exists a prime w of L dividing v and a K_v-isomorphism $L_w \to K^v$.)

The next example shows that the answer is not always yes, but, nevertheless, we shall see that it is *usually* yes.

EXAMPLE 2.2 Let $\mathbb{Q}^2$ be the unramified extension of $\mathbb{Q}_2$ of degree 8. It is easy to construct extensions L of $\mathbb{Q}$ of degree 8 such that (2) remains prime in L, and hence such that $L_w \approx K$ for the unique $w|2$ — take $L = \mathbb{Q}[X]/(g(X))$, where $g(X)$ is any monic polynomial of degree 8 in $\mathbb{Z}[X]$ that is irreducible modulo 2. However, I claim that it is impossible to construct a *cyclic* such extension . More precisely:

> Let L be a cyclic extension of $\mathbb{Q}$ of degree 8; then it is not possible for (2) to remain prime in L.

This follows from the three statements:

(i) 16 is an 8th power in $\mathbb{Q}_p$ for all $p \neq 2$ (including $p = \infty$), but not in $\mathbb{Q}_2$.

(ii) Let $L/\mathbb{Q}$ be a finite abelian extension; if $a \in \mathbb{Q}$ becomes a norm in $\mathbb{Q}_p$ for all but one p, then it is a norm for all p.

(iii) 16 is not a norm from $\mathbb{Q}^2$.

Let L be a cyclic extension of $\mathbb{Q}$ of degree 8. As the degree of L_v over $\mathbb{Q}_p$ divides 8, (i) shows that 16 becomes a norm in $\mathbb{Q}_p$ for all $p \neq 2$. According to (ii), this implies that 16 is a norm in $\mathbb{Q}_2$. Now (iii) shows that L^2 is not isomorphic to $\mathbb{Q}^2$.

For the proof of statement (i), see Exercise 1.3 (and its solution). For (ii), consider the diagram:

$$\begin{array}{ccccc} & & \mathbb{Q}_p^\times & \xrightarrow{\phi_p} & \operatorname{Gal}(L^p/\mathbb{Q}_p) \\ & & \downarrow & & \downarrow \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{I}_\mathbb{Q} & \xrightarrow{\phi} & \operatorname{Gal}(L/\mathbb{Q}). \end{array}$$

Here ϕ_p is the local Artin map into the decomposition group at a prime dividing p and ϕ is the global Artin map (we allow $p = \infty$, in which case $\mathbb{Q}_p = \mathbb{R}$). The diagram commutes (this is how we defined the global Artin map). For every $a \in \mathbb{Q}^\times$, there is the product formula

$$\prod_{p=2,3,5,\dots,\infty} \phi_p(a) = 1$$

(VII, Theorem 8.1). Now $\phi_p(a) = 1$ if and only if a becomes a norm in $\mathbb{Q}_p$, and so the product formula implies (ii). For (iii), we use that, because $\mathbb{Q}^2$ is unramified over $\mathbb{Q}_2$, the normalized ord on $\mathbb{Q}_2$ extends to the normalized ord on $\mathbb{Q}_2$. If $16 = \mathrm{Nm}(\alpha)$, then

$$4 = \mathrm{ord}_2(16) = \mathrm{ord}_2(\mathrm{Nm}(\alpha)) = 8\,\mathrm{ord}_2(\alpha),$$

which is impossible.

I now briefly explain the positive results (Artin and Tate 1961, Chapters 9 and 10). Let S be a finite set of primes of K. The composite of the maps

$$\prod_{v\in S} K_v^\times \to \mathbb{I}_K \to \mathbf{C}_K$$

is injective, and it is continuous when we endow $P \overset{\text{def}}{=} \prod_{v\in S} K_v^\times$ with the product topology. When S contains more than one prime, the product topology doesn't coincide with the topology induced by $\mathbf{C}_K$ (ibid. p. 98). Nevertheless, a subgroup of finite index in P is open for one topology if and only if it is open for the other, and an open subgroup of P of finite index is the intersection of P with an open subgroup of finite index in $\mathbf{C}_K$ (ibid. p. 99). Using the reciprocity laws, this implies the following.

THEOREM 2.3 *For each $v \in S$, let N_v be an open subgroup of finite index in $K_v^\times$. Then there exists an abelian extension L of K such that, for all $v \in S$, L^v is the extension of K_v corresponding (by local class field theory) to N_v.*

A more careful analysis, proves the following ("character" means "continuous character").

THEOREM 2.4 (GRUNWALD-WANG) *For each $v \in S$, let χ_v be a character of $K_v^\times$. There exists a character χ of $\mathbf{C}_K$ whose restriction to $K_v^\times$ is χ_v, all $v \in S$. Let n_v be the order of χ_v and $n = \mathrm{lcm}(n_v)$. Then it is possible to choose χ to have order n, except possibly when $2^t | n$ for some t with $K[\zeta_{2^t}]$ not cyclic over K.*

PROOF. See Artin and Tate 1961, Chaper X, Theorem 5. Alternatively, it is possible to prove a more precise version of the theorem by comparing the Poitou-Tate theorem for S and for the set of all primes — see a future version of the notes. □

Example 2.2 shows that the second statement may fail without the condition on n.

COROLLARY 2.5 *For each $v \in S$, let n_v be a positive integer. If v is an infinite prime, then n_v must be a possible order for an extension of K_v. Then there exists a cyclic extension L of K of degree $n = \mathrm{lcm}(n_v)$ such that the local degree is n_v for all $v \in S$.*

PROOF. For an infinite prime $v \in S$, choose a character χ_v on $K_v^\times$ of order n_v in the only way possible; for a finite prime $v \in S$ not dividing 2, choose χ_v to be the canonical character of order n_v that is 1 on U_v; for $v \in S$ dividing 2, choose χ_v of order n_v to avoid the exceptional case in the theorem. See ibid. p. 105, Theorem 5 (this shouldn't be confused with the theorem[1] of the same number on p. 103). □

Application. Let D be a central division algebra of degree d^2 over an algebraic number field K, and let i_v be the image of the class of $D \otimes_K K_v$ in $\mathrm{Br}(K_v)$ under the invariant map $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$. Let $i_v = m_v/n_v \mod \mathbb{Z}$, where m_v and n_v are relatively prime integers and $n_v > 0$.

Because $\mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ is injective (even an isomorphism if v is finite), the order of the class of $D \otimes_K K_v$ in $\mathrm{Br}(K_v)$ is n_v. Up to isomorphism, there is exactly one division algebra D_{i_v} over K_v with invariant $i_v = m_v/n_v$, and its degree is n_v^2. Thus, $D \otimes_K K_v \approx M_{\frac{d}{n_v}}(D_{n_v})$. In particular, $n_v | d$, and so $n | d$.

Because $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$ (sum over all v) is injective, the order of the class of D in $\mathrm{Br}(K)$ is $n = \mathrm{lcm}(n_v)$.

According to the corollary, there exists a cyclic extension L of K of degree n whose local degrees are n_v for each v for which $i_v \notin \mathbb{Z}$. Hence L splits D. From IV 3.6, we see that there is a central simple algebra B over K such that

(a) $B \supset L$;

(b) B is similar to D, so that $B \approx M_r(D)$ for some r; and

(c) $[B : K] = [L : K]^2$.

From the last two statements, we see that $r^2 d^2 = n^2$. Since $n | d$, it follows that in fact $r = 1$ and $n = d$. We have shown:

THEOREM 2.6 *For every division algebra over a number field K, the order of D in $\mathrm{Br}(K)$ is $\sqrt{[D : K]}$, and D contains a cyclic extension of K as a maximal subfield (and hence is split by it).*

From the theorem and the Noether-Skolem Theorem, it is possible to deduce that D is a ***cyclic algebra*** in the sense defined by Dickson on 1906, namely, that D is generated as a K-algebra by the elements of L and a single element β, with the relations

$$\beta \cdot \alpha = \sigma\alpha \cdot \beta, \quad \alpha \in L, \quad \text{and } \beta^d = \gamma,$$

where σ generates $\mathrm{Gal}(L/K)$ and $\gamma \in K^\times$.

These are very famous results[2], with many applications, for example in the theory of abelian varieties. (See my notes AV, Theorem 16.8.)

[1] Serge Lang took the notes. In the 2009 edition it is correctly numbered Theorem 6.

[2] "The high points of the structure theory of algebras of the 1930's were undoubtedly the theorem that every finite dimensional central division algebra over a number field is cyclic, and the classification of these algebras by a set of numerical invariants. The latter result amounts to the determination of the structure of the Brauer group for a number field. Besides the general theory of central simple algebras we have indicated, the proofs of these fundamental results required the structure theory of central simple algebras over p-adic fields due to Hasse, Hasse's norm theorem ("the Hasse principle"), and the Grünwald existence theorem for certain cyclic extensions.... The first proof of the cyclic structure of central division algebras over number fields was given by Brauer, Hasse, and Noether (1931)." Nathan Jacobson, Obituary for A.A. Albert, Bull. AMS, 80 (1974), p.1081.

NOTES In 1933, Grunwald proved Theorem 2.4 without the condition on n, and in 1942 Whaples gave a second proof. In 1948, Wang found the counterexample provided by (1.3, 2.2), and corrected the statement. In the fifteen years following 1933, Grunwald's "Theorem" was quite widely used, for example, to prove that every division algebra over a number field is cyclic. See Roquette 2005, 5.3.

In fact, as Brian Conrad pointed out to me, effectively, a counterexample to Grunwald's theorem was published in 1934, 14 years before Wang, but (apparently) no one, including the author, noticed. Specifically, let a and n be integers; for a prime p not dividing an, a is an nth power in $\mathbb{Q}_p$ if and only if it is an nth power mod p. Trost (1934)[3] proved by elementary means the following theorem:

> if a is an nth power for almost all primes and 8 doesn't divide n, then a is an nth power; when 8 does divide n, then a is either an nth power or it is $2^{n/2}$ times an nth power (and both occur).

For example, when $n = 8$, it is possible that $2^4 a$ is an 8th power (and hence that a is not an 8th power). This happens with $a = 16$. In other words, Trost already knew the statement (i) of Example 2.2 that leads by standard arguments to the counterexample to Grunwald's theorem.

Incidentally, Olga Taussky reviewed Grunwald's paper. Chevalley reviewed Whaples's paper for Mathematical Reviews, and even read it carefully enough to note that "some typographical errors are to be guarded against in reading the proof of the fundamental lemma", but not carefully enough to note that the main result was false.

3 The local-global principle for norms and quadratic forms

The ***local-global*** (or ***Hasse***) ***principle*** asks whether a statement is true over a number field K whenever it is true over each of the completions of K. In this section, we give two cases where class field theory allows us to prove that the principle holds.

Norms

THEOREM 3.1 (HASSE NORM THEOREM) *Let L/K be a cyclic extension of number fields, and let $a \in K^\times$. Then the image of a in K_v is a norm from L^v for all but finitely many v, and if it is a norm for all v, then it is a norm in K.*

PROOF. According to Theorem VII, 5.1, $H^1(G, \boldsymbol{C}_L) = 0$. Because of the periodicity of the cohomology of cyclic groups, this implies that $H_T^{-1}(G, \boldsymbol{C}_L) = 0$. Therefore, from the cohomology sequence of

$$1 \to L^\times \to \mathbb{I}_L \to \boldsymbol{C}_L \to 0$$

we find that

$$H_T^0(G, L^\times) \to H_T^0(G, \mathbb{I}_L)$$

is injective. But (see VII 2.5), this is the map

$$K^\times / \operatorname{Nm}(L^\times) \to \bigoplus\nolimits_v K_v^\times / \operatorname{Nm}(L^{v\times}).$$

□

REMARK 3.2 The proof fails for noncyclic extension, and, in fact, the statement is not true for noncyclic extensions. For example, 5^2 is a local norm from $\mathbb{Q}[\sqrt{13}, \sqrt{17}]$ at all primes but is not a global norm (see Cassels and Fröhlich 1967, Exercise 5.3, p. 360). Given a noncyclic abelian group G, the following paper studies the density of the extensions with

[3] E. Trost, Zur Theorie der Potenzreste, Nieuw Arch. Wisk. 18 (1934), 58–61.

group G for which the Hasse norm theorem holds: Frei, C.; Loughran, D.; Newton, R.: The Hasse norm principle for Abelian extensions. Amer. J. Math. 140 (2018), no. 6, 1639–1685.

Quadratic Forms

Recall that a ***quadratic form*** on a vector space V over a field k is a map $Q: V \to k$ such that

(a) $Q(av) = a^2 Q(v)$;

(b) $B(v, w) \stackrel{\text{def}}{=} Q(v + w) - Q(v) - Q(w)$ is a bilinear form on V.

The quadratic form Q is said to be ***nondegenerate*** if its associated bilinear form B is nondegenerate.[4] Let $c \in k$. A nondegenerate quadratic form Q is said to ***represent*** c if there exists a nonzero $v \in V$ such that $Q(v) = c$.

LEMMA 3.3 *If a nondegenerate quadratic form Q represents 0, then it represents all $c \in k$.*

PROOF. Note that, for $t \in k$,

$$Q(tv + w) = t^2 Q(v) + tB(v, w) + Q(w).$$

If v_0 is a nonzero vector such that $Q(v_0) = 0$, then, because B is nondegenerate, there exists a vector w_0 such that $B(v_0, w_0) \neq 0$. As t runs through all values of k, so also does $Q(tv_0 + w_0) = tB(v_0, w_0) + Q(w_0)$. □

When k has characteristic $\neq 2$, there exists a basis $\{e_1, \dots, e_n\}$ for V such that $B(e_i, e_j) = 0$ for $i \neq j$. Then

$$Q(\sum x_i e_j) = \sum_{i=1}^{n} a_i x_i^2, \quad n = \dim V.$$

Henceforth, we shall write the quadratic form as

$$q(X_1, \dots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2,$$

and keep in mind that an invertible change of variables will change none of our statements.

LEMMA 3.4 *A nondegenerate quadratic form $q(X_1, \dots, X_n)$ represents a if and only if $r \stackrel{\text{def}}{=} q - aY^2$ represents 0.*

PROOF. If $q(x_1, \dots, x_n) = a$, then $r(x_1, \dots, x_n, 1) = 0$. Conversely, suppose $r(x_1, \dots, x_n, y) = 0$. If $y = 0$, then q represents 0 and hence represents every element in k. If $y \neq 0$, then $q(\frac{x_1}{y}, \cdots, \frac{x_n}{y}) = q(x_1, \dots, x_n)/y^2 = a$. □

THEOREM 3.5 *Let q be a nondegenerate quadratic form in n variables with coefficients in a number field K.*

(a) *If $n \geq 3$, then q represents 0 in K_v for all but finitely many v.*

(b) *The form q represents 0 in K if it represents 0 in K_v for all v.*

Before beginning the proof, we note a consequence.

[4] When k has characteristic $\neq 2$, it is customary to set $B(v, w) = \frac{1}{2}(Q(v + w) - Q(v) - Q(w))$.

COROLLARY 3.6 *Let $c \in K$. A nondegenerate quadratic form q with coefficients in K represents c in K if and only if it represents c in K_v for all v.*

PROOF. Let $r = q - cY^2$. Then r represents 0 if and only if q represents c. □

We begin the proof with a purely algebraic result.

PROPOSITION 3.7 *Let k be a field of characteristic $\neq 2$.*

(a) *The form $q = X^2$ does not represent 0.*

(b) *The form $q = X^2 - aY^2$ represents 0 if and only if a is a square.*

(c) *The form $q = X^2 - aY^2 - bZ^2$ represents 0 if and only if b is a norm from the field $k[\sqrt{a}]$.*

(d) *The form $q = X^2 - bY^2 - cZ^2 + acT^2$ represents 0 in k if and only if c, as an element of $k[\sqrt{ab}]$, is a norm from $k[\sqrt{a}, \sqrt{b}]$.*

PROOF. (a) This is obvious.

(b) According to Lemma 3.4, $X^2 - aY^2$ represents 0 if and only if X^2 represents a.

(c) According to 3.4, $X^2 - aY^2 - bZ^2$ represents 0 if and only if $X^2 - aY^2$ represents b, i.e., if and only if b is a norm from $k[\sqrt{a}]$.

(d) Clearly,

$$q(x, y, z, t) = 0 \iff c = \frac{\mathrm{Nm}_{k[\sqrt{b}]/k}(x + \sqrt{b}y)}{\mathrm{Nm}_{k[\sqrt{a}]/k}(z + \sqrt{a}t)}.$$

Because the inverse of a norm is also a norm, this shows that q represents zero if and only if c is the product of norm from $k[\sqrt{a}]$ and a norm from $k[\sqrt{b}]$. Thus (d) follows from the next lemma. □

LEMMA 3.8 *Let k be a field of characteristic $\neq 2$. An element $c \in k^\times$ is the product of a norm from $k[\sqrt{a}]$ and a norm from $k[\sqrt{b}]$ if and only if, as an element of $k[\sqrt{ab}]$, it is a norm from $L = k[\sqrt{a}, \sqrt{b}]$.*

PROOF. We leave the degenerate cases, in which one of a, b, or ab is a square in k to the reader. Thus, we may suppose that $\mathrm{Gal}(k[\sqrt{a}, \sqrt{b}]/k) = \{1, \sigma, \tau, \sigma\tau\}$, where each of σ, τ, and $\sigma\tau$ is of order 2, and fix respectively $\sqrt{a}$, $\sqrt{b}$, and $\sqrt{ab}$. The first condition asserts,

(*) There exist $x, y \in k[\sqrt{a}, \sqrt{b}]$ such that $\sigma x = x$, $\tau y = y$, and $xy \cdot \sigma\tau(xy) = c$.

and the second asserts,

(**) There exists $z \in k[\sqrt{a}, \sqrt{b}]$ such that $z \cdot \sigma\tau(z) = c$.

Clearly, (*) $\Rightarrow$ (**). For the converse, note that

$$z \cdot \sigma z = \mathrm{Nm}_{k[\sqrt{a},\sqrt{b}]/k[\sqrt{a}]}\, z \in k[\sqrt{a}].$$

Moreover,

$$\mathrm{Nm}_{k[\sqrt{a}]/k}(z \cdot \sigma z) = z \cdot \sigma z \cdot \tau z \cdot \sigma\tau z \in k.$$

As $z \cdot \sigma\tau z = c \in k$, this implies that $\sigma z \cdot \tau z \in k$, and so

$$\sigma z \cdot \tau z = \sigma(\sigma z \cdot \tau z) = z \cdot \sigma\tau z = c.$$

Therefore,

$$\mathrm{Nm}_{k[\sqrt{a}]/k}(z \cdot \sigma z) = c^2.$$

Now Hilbert's theorem 90 (II 1.23), applied to $z \cdot \sigma z/c \in k[\sqrt{a}]$, shows that there exists an $x \in k[\sqrt{a}]^\times$ such that $\tau x/x = z \cdot \sigma z/c$. Let $y = \sigma\tau z/x$. Then

$$\tau y = \sigma z/\tau x = c/z \cdot x = z \cdot \sigma\tau z/z \cdot x = y$$

(use: definition of y; definition of x; definition of z; definition of y) and

$$xy \cdot \sigma\tau(xy) = \sigma\tau z \cdot \sigma\tau(\sigma\tau z) = \sigma\tau z \cdot z = c$$

(use: definition of y; $(\sigma\tau)^2 = 1$; definition of z) as required. □

PROOF (OF THEOREM 3.5a) If $q = q_1(X_1, \dots, X_m) + q_2(X_{m+1}, \dots, X_n)$ and q_1 represents zero, then so also does q. Therefore, it suffices to prove (3.5a) for a quadratic form in 3 variables. After multiplying q by a nonzero scalar, we may suppose $q = X^2 - aY^2 - bZ^2$, and for such a quadratic form, the statement follows from (3.7) and Theorem 3.1. □

PROOF (OF THEOREM 3.5b) We prove this by induction on the number n of variables.

When $n = 1$, there is nothing to prove, because the hypothesis is never fulfilled.

When $n = 2$, then, after multiplying q by nonzero scalar, we may suppose that $q = X^2 - aY^2$, and for such a quadratic form, the statement follows from (3.7) and Theorem 1.1.

When $n = 3, 4$ the statement follows in a similar fashion from (3.7c,d) and Theorem 1.1.

Before proving the general case, we make some elementary observations.

(a) A nondegenerate quadratic form $q_1(X_1, \dots, X_m) - q_2(X_{m+1}, \dots, X_n)$ represents 0 in a field k if and only if there is a $c \in k$ such that both q_1 and q_2 represent c.

(b) If q represents c in $k^\times$, then q represents every element in the coset $c \cdot k^{\times 2}$.

(c) The subgroup $K_v^{\times 2}$ of $K_v^\times$ is open. When v is real or complex, this is obvious. When v is nonarchimedean, Newton's Lemma (ANT, 7.32) shows that 1 can be refined to a root of $X^2 - a$ for any a with $|1 - a|_v < |2|_v^2$.

On combining (b) and (c), we see that a quadratic form q with coefficients in K_v represents the elements in a nonempty open subset of $K_v^\times$.

Assume now that $n \geq 5$ and that Theorem 3.1b has been proved for $n - 1$. Let

$$q(X_1, \dots, X_n) = aX_1^2 + bX_2^2 - r(X_3, \dots, X_n), \quad n - 2 \geq 3.$$

From (a) of the theorem, we know that, except for v in a certain finite set S, R represents 0 in K_v. Let $v \in S$. Because q represents 0 in K_v, there exists an element $c_v \in K_v^\times$ that is represented by both $aX_1^2 + bX_2^2$ and r, i.e., there exist $x_i(v) \in K_v$ such that

$$ax_1(v)^2 + bx_2(v)^2 = c_v = r(x_3(v), \dots, x_n(v)).$$

Now apply the weak approximation theorem (ANT, 7.20), to find elements $x_1, x_2 \in K$ that are close to $x_1(v), x_2(v)$ in K_v for all $v \in S$. Then

$$c \stackrel{\text{def}}{=} ax_1^2 + bx_2^2$$

will be close to c_v for each $v \in S$; in particular, we may suppose that $c/c_v \in K_v^{\times 2}$ for all $v \in S$.

Consider the quadratic form $cY^2 - r$. It represents 0 in K_v for $v \notin S$ because r represents zero in K_v, and it represents 0 in K_v for $v \in S$ because r represents c in K_v. By induction, $cY^2 - r$ represents zero in K. It follows that q represents 0 in K because each of $aX_1^2 + bX_2^2$ and r represents c in K. □

PROPOSITION 3.9 *A nondegenerate quadratic form q in 4 variables over a finite extension K of $\mathbb{Q}_p$ represents every nonzero element of $K^\times$.*

PROOF. If q represents 0, then it represents every element of K. We assume the contrary. After multiplying q by a nonzero element of K, we may suppose that

$$q = X^2 - bY^2 - cZ^2 + acT^2.$$

Because q does not represent 0 in K, neither b nor a is a square.

If $K[\sqrt{a}] \neq K[\sqrt{b}]$, then (by local class field theory, Theorem I.1.1), $\mathrm{Nm}(K[\sqrt{a}]^\times)$ and $\mathrm{Nm}(K[\sqrt{b}]^\times)$ are distinct subgroups of index 2 in $K^{\times 2}$, and therefore $K^\times = \mathrm{Nm}(K[\sqrt{a}]^\times) \cdot \mathrm{Nm}(K[\sqrt{b}]^\times)$. Since the inverse of a norm is also a norm, this means that we can write c as

$$c = \frac{x^2 - by^2}{z^2 - at^2},$$

some $x, y, z, t \in K$. On multiplying out, we find that q represents 0, contradicting our assumption. Therefore $K[\sqrt{a}] = K[\sqrt{b}]$, and $a = b \times$ (square) (see VII A.1). The square may be absorbed into the T^2, and so we may write

$$q = X^2 - bY^2 - cZ^2 + bcT^2.$$

Consider the quaternion algebra $H(b, c)$ (see IV.5.7). For

$$\alpha = x + yi + zj + tk$$

we define

$$\bar{\alpha} = x - yi - zj - tk$$

so that

$$\mathrm{Nm}(\alpha) \stackrel{\text{def}}{=} \alpha\bar{\alpha} = x^2 - by^2 - cz^2 + bct^2.$$

The map $\alpha \mapsto \mathrm{Nm}(\alpha) : H(b, c)^\times \to K^\times$ is a homomorphism, which we must show to be surjective.

For every $\alpha \in H(b, c)$,

$$P_\alpha(X) \stackrel{\text{def}}{=} (X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \mathrm{Nm}(\alpha) \in K[X].$$

Therefore, $P_\alpha(X)$ is the characteristic polynomial of α in the extension $K[\alpha]/K$. In particular,

$$\mathrm{Nm}(\alpha) = \mathrm{Nm}_{K[\alpha]/K}(\alpha).$$

Now (see IV.4.4), $H(b, c)$ contains copies of every quadratic extension of K, for example, the unramified quadratic extension of K and a totally ramified quadratic extension of K. Therefore $\mathrm{Nm}(H(b, c)^\times)$ contains the norm groups of these two distinct quadratic extensions, and so (as above) equals $K^\times$. □

COROLLARY 3.10 *Every nondegenerate quadratic form q in ≥ 5 variables over a finite extension of $\mathbb{Q}_p$ represents 0.*

PROOF. We can write $q = r(X_1, \ldots, X_4) - aX_5^2 + q'(X_6, \ldots)$, where r is a nondegenerate quadratic form in 4 variables and $a \neq 0$. Then r represents a and so q represents 0. □

COROLLARY 3.11 *A nondegenerate quadratic form q in ≥ 5 variables over a number field K represents 0 if and only if it represents 0 in every real completion of K.*

PROOF. Combine (3.10) with (3.5). □

REMARK 3.12 The proof of Proposition 3.9 works also for $K = \mathbb{R}$ down to the last step: the only quadratic extension of $\mathbb{R}$ is $\mathbb{C}$, and so

$$\mathrm{Nm}(\mathbb{H}(b,c)^\times) = \mathrm{Nm}(\mathbb{C}^\times) = \mathbb{R}_{>0}.$$

It shows therefore, that a nondegenerate form in 4 variables over $\mathbb{R}$ that does not represent zero represents all strictly positive real numbers.

4 The Fundamental Exact Sequence and the Fundamental Class

For a Galois extension L/K, we write

$$\mathrm{Br}(L/K) = H^2(\mathrm{Gal}(L/K), L^\times),$$

and for a Galois extension L/K of number fields, we write

$$H^2(L/K) = H^2(\mathrm{Gal}(L/K), \boldsymbol{C}_L).$$

Because $H^1(G, L^\times) = 0$ (see II, 1.22) and $H^1(G, \boldsymbol{C}_L) = 0$ (see VII 5.1), for every tower of Galois extensions $E \supset L \supset K$, we get exact sequences

$$0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(E/K) \to \mathrm{Br}(E/L)$$

and

$$0 \to H^2(L/K) \to H^2(E/K) \to H^2(E/L).$$

On passing to the direct limit over larger fields $E \subset K^{\mathrm{al}}$, we obtain exact sequences

$$0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(K) \to \mathrm{Br}(L)$$

and

$$0 \to H^2(L/K) \to H^2(K^{\mathrm{al}}/K) \to H^2(K^{\mathrm{al}}/L).$$

Thus, we can regard $\mathrm{Br}(L/K)$ as the subgroup of $\mathrm{Br}(K)$ of elements split by L, and similarly for $H^2(L/K)$.

Let L/K be a Galois extension of number fields of finite degree n, and consider the diagram:

$$\begin{array}{ccccc} & & & & H^2(L/K) \\ & & & \nearrow & \\ 0 \longrightarrow & \mathrm{Br}(L/K) & \longrightarrow & \bigoplus_v \mathrm{Br}(L^v/K_v) & \\ & & & \searrow & \\ & & & & \mathbb{Q}/\mathbb{Z} \end{array}$$

The top row is part of the cohomology sequence of

$$0 \to L^\times \to \mathbb{I}_L \to \boldsymbol{C}_L \to 0.$$

The zero at left comes from the fact that $H^1(G, \boldsymbol{C}_L) = 0$. The top row is exact, but the map $\bigoplus_v \mathrm{Br}(L^v/K_v) \to H^2(L/K)$ will not in general be surjective—we denote its image by $H^2(L/K)'$.

Recall (III, 2.1), that for each prime v, we have a homomorphism

$$\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}.$$

If v is nonarchimedean, it is an isomorphism of $\mathrm{Br}(K_v)$ onto $\mathbb{Q}/\mathbb{Z}$, and if v is real, it is an isomorphism of $\mathrm{Br}(K_v)$ onto $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Moreover, if L_w/K_v has degree n_v, then $\mathrm{inv}_w(\beta) = n_v \cdot \mathrm{inv}_v(\beta)$, and so inv_v defines an isomorphism

$$\mathrm{inv}_v : \mathrm{Br}(L_w/K_v) \to \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}.$$

The southeast arrow in the diagram is

$$\Sigma : \bigoplus_v \mathrm{Br}(L^v/K_v) \to \mathbb{Q}/\mathbb{Z}, \quad (\beta_v) \mapsto \sum \mathrm{inv}_v(\beta_v).$$

The image of inv_v is the cyclic subgroup of order n_v in the cyclic group $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, and therefore the image of Σ is the cyclic subgroup $\frac{1}{n_0}\mathbb{Z}/\mathbb{Z}$, where $n_0 = \mathrm{lcm}(n_v)$.

According to Theorem VII 5.1, the order of $H^2(L/K)$ divides n. According to Theorem VII 8.1, the bottom row of the diagram is a complex, and so the maps in the diagram induce a surjective homomorphism

$$H^2(L/K)' \to \frac{1}{n_0}\mathbb{Z}/\mathbb{Z}.$$

The lcm n_0 of the local degrees always divides n, but need not equal it (see Example 4.5 below). Suppose, however, that the extension L/K has the property that $n = n_0$. Then:

(a) The map $H^2(L/K)' \to \frac{1}{n_0}\mathbb{Z}/\mathbb{Z}$ is an isomorphism. (It is surjective, and $(H^2(L/K)' : 1) \le (H^2(L/K) : 1) \le n$.)

(b) $H^2(L/K)' = H^2(L/K)$, and each has order n.

(c) The bottom row is an exact sequence

$$0 \to \mathrm{Br}(L/K) \to \oplus_v \mathrm{Br}(L^v/K_v) \xrightarrow{\Sigma} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0$$

(because it is isomorphic to the top row).

LEMMA 4.1 *If L/K is cyclic, then $n = n_0$.*

PROOF. Let $S \supset S_\infty$ be a set of primes of K including all those that ramify in L. For $v \notin S$, $(\mathfrak{p}_v, L/K)$ is an element of $\mathrm{Gal}(L/K)$ of order n_v $(= f_v)$, and so the image of the Artin map $I^S \to \mathrm{Gal}(L/K)$ has order $n_0 \overset{\text{def}}{=} \mathrm{lcm}(n_v)$. According to the reciprocity law (VII, 4.8), the Artin map is onto, which implies that $n_0 = n$. [Using complex analysis, one can show more, namely, that for all v in a set of density $\varphi(n)/n$, L^v/K_v is cyclic of order n: let $\mathfrak{m}$ be the modulus of L/K, and let $\mathfrak{a}$ be an ideal in I^S such that $(\mathfrak{a}, L/K)$ generates $\mathrm{Gal}(L/K)$; then the set of prime ideals $\mathfrak{p} \equiv \mathfrak{a}$ in $C_\mathfrak{m}$ has density $1/n$.] □

Let $\mathbb{Q}^c$ be the infinite cyclic cyclotomic extension of $\mathbb{Q}$ defined in (I A.5d) (see also (VII, 7.3)), and let $\Omega = \mathbb{Q}^c \cdot K$. For every n, Ω contains a unique cyclic extension of Ω_n of degree n. The preceding lemma and remarks show that

$$0 \to \mathrm{Br}(\Omega_n/K) \to \bigoplus\nolimits_v \mathrm{Br}(\Omega_n^v/K_v) \xrightarrow{\Sigma} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact. On passing to the direct limit (actually, directed union) over all n, we obtain an exact sequence

$$0 \to \mathrm{Br}(\Omega/K) \to \bigoplus\nolimits_v \mathrm{Br}(\Omega^v/K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

THEOREM 4.2 *For every number field K, the sequence*

$$0 \to \mathrm{Br}(K) \to \bigoplus\nolimits_v \mathrm{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0$$

is exact.

PROOF. According to Proposition VII 7.2, $\mathrm{Br}(\Omega/K) = \mathrm{Br}(K)$. Moreover, $\mathrm{Br}(\Omega^v/K_v) = \mathrm{Br}(K_v)$ because, in the nonarchimedean case, $[\Omega_n^v : K_v] \to \infty$ as $n \to \infty$ (see VII 7.3). □

The sequence in the theorem is called the ***fundamental exact sequence*** of global class field theory.

COROLLARY 4.3 *For every finite extension L/K, the sequence*

$$0 \to \mathrm{Br}(L/K) \to \bigoplus\nolimits_v \mathrm{Br}(L^v/K_v) \xrightarrow{\Sigma} \tfrac{1}{n_0}\mathbb{Z}/\mathbb{Z} \to 0, \quad n_0 = lcm(n_v),$$

is exact.

PROOF. Apply the snake lemma to the diagram obtained by mapping the fundamental exact sequence for K to that for L. □

EXAMPLE 4.4 (a) For a finite cyclic extension of number fields L/K, the fundamental exact sequence becomes identified with

$$0 \to K^\times/\mathrm{Nm}(L^\times) \to \bigoplus\nolimits_v K_v^\times/\mathrm{Nm}(L^{v\times}) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0, \quad n = [L:K].$$

(b) Let D be a division algebra over a number field K, and let $i_v = \mathrm{inv}_v(D \otimes_K K_v)$. Then: $i_v = 0$ for all but finitely many v; $i_v = 0$ if v is complex; $i_v \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if v is real; and $\sum i_v \equiv 0 \bmod \mathbb{Z}$. The family (i_v) determines the isomorphism class of D, and any family (i_v) satisfying the conditions is the family of invariants of the division algebra. Clearly, the order of the class of D in $\mathrm{Br}(K)$ is the least common denominator n of the i_v. One can also prove that $[D : K] = n^2$. For example, to give a quaternion algebra over $\mathbb{Q}$ is the same as to give a set of primes of $\mathbb{Q}$ having an even finite number of elements.

EXAMPLE 4.5 Let $L = \mathbb{Q}[\sqrt{13}, \sqrt{17}]$. Clearly $n = 4$, but I claim that $n_v = 1$ or 2 for all v. Because both 13 and 17 are congruent to 1 modulo 4, 2 is unramified in L. Therefore, for $w|p$, $p \neq 13, 17$, L_w is an unramfied extension of $\mathbb{Q}_p$. In particular, its Galois group is cyclic. Since it is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, it is killed by 2, and therefore has order 1 or 2. On the other hand, $\left(\frac{17}{13}\right) = 1$ (obviously) and $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1$. Hence, 17 is a square modulo 13, and Hensel's lemma implies that it is a square in $\mathbb{Q}_{13}$. Similarly, 13 is a square in $\mathbb{Q}_{17}$.

The fundamental class

It follows from the above discussion that there is an isomorphism

$$\mathrm{inv}_K : H^2(\Omega/K) \to \mathbb{Q}/\mathbb{Z}$$

uniquely characterized by having the property that the composite

$$\bigoplus\nolimits_v \mathrm{Br}(K_v) \to H^2(\Omega/K) \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z}$$

is $(\beta_v) \mapsto \sum \mathrm{inv}_v(\beta_v)$.

LEMMA 4.6 *For every finite extension L/K of number fields and $\gamma \in H^2(\Omega/K)$, $\mathrm{inv}_L(\gamma) = n\,\mathrm{inv}_K(\gamma)$, $n = [L : K]$.*

PROOF. Use that the sum of the local degrees is the global degree. □

Therefore, for every L/K finite and Galois, we obtain an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

On passing to the direct limit over all $L \subset K^{\mathrm{al}}$, we obtain an isomorphism

$$\mathrm{inv}_K : H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}.$$

THEOREM 4.7 *For every finite Galois extension L/K of number fields, $H^2(L/K)$ is cyclic of order $n = [L : K]$ having a canonical generator $u_{L/K}$.*

PROOF. Take $u_{L/K}$ to be the element such that $\mathrm{inv}_{L/K}(u_{L/K}) = \frac{1}{n} \mod \mathbb{Z}$. □

The generator $u_{L/K}$ of $H^2(L/K)$ is called the ***fundamental class.*** One shows as in the local case (see III, 2.7) that for every tower $E \supset L \supset K$ of finite Galois extensions,

$$\mathrm{Res}(u_{E/K}) = u_{E/L}$$
$$\mathrm{Inf}(u_{L/K}) = [E : L]u_{E/K}.$$

Therefore, one may apply Tate's theorem (II, 3.11) to obtain an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \to \boldsymbol{C}_K/\mathrm{Nm}(\boldsymbol{C}_L).$$

That this is inverse to the global Artin map $\phi_{L/K}$ defined in the last chapter follows from the fact that the global fundamental classes are compatible with the local fundamental classes.

The norm limitation theorem

THEOREM 4.8 *Let E be a finite extension of K (not necessarily Galois), and let M be the maximal subextension of E such that M/K is an abelian Galois extension. Then*

$$\mathrm{Nm}_{E/K}\boldsymbol{C}_E = \mathrm{Nm}_{M/K}\boldsymbol{C}_M.$$

PROOF. Let L be a Galois extension of K containing E, and let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/E)$. Consider the commutative diagram

$$\begin{array}{ccc} H_T^{-2}(H,\mathbb{Z}) & \xrightarrow{\simeq} & H_T^0(H,\boldsymbol{C}_L) \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ H_T^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & H_T^0(G,\boldsymbol{C}_L) \end{array}$$

in which the horizontal arrows are cup-product with the fundamental classes. This can be identified with the commutative diagram:

$$\begin{array}{ccc} H^{\mathrm{ab}} & \xrightarrow{\simeq} & \boldsymbol{C}_E/\operatorname{Nm}_{L/E}\boldsymbol{C}_L \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Nm}_{E/K}} \\ G^{\mathrm{ab}} & \xrightarrow{\simeq} & \boldsymbol{C}_K/\operatorname{Nm}_{L/K}\boldsymbol{C}_L. \end{array}$$

Hence the cokernel of $H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ is isomorphic to $\boldsymbol{C}_K/\operatorname{Nm}_{E/K}(\boldsymbol{C}_E)$. But the cokernel is equal to $\mathrm{Gal}(M/K)$, which is isomorphic to $\boldsymbol{C}_K/\operatorname{Nm}_{M/K}(\boldsymbol{C}_M)$. Since $\operatorname{Nm}(\boldsymbol{C}_M) \supset \operatorname{Nm}(\boldsymbol{C}_E)$, the two groups must be equal. □

5 Higher Reciprocity Laws

Recall that, an odd prime p and integer a not divisible by p, the ***Legendre symbol*** (or ***quadratic residue symbol)***

$$\left(\frac{a}{p}\right) \overset{\text{def}}{=} \begin{cases} 1 & \text{if } a \text{ is a square modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$ with -1 as its unique element of order 2. Therefore, for $u \in \mathbb{F}_p^\times$, $u^{\frac{p-1}{2}}$ is 1 or -1 according as u is a square or not, and so $\left(\frac{a}{p}\right)$ is the unique square root of 1 such that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

The quadratic reciprocity law says that, for odd primes p and q,

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

The supplement to the quadratic reciprocity law says that

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

For α a Gaussian integer (i.e., element of $\mathbb{Z}[i]$) and π an odd Gaussian prime (i.e., prime element of $\mathbb{Z}[i]$ not dividing 2), Gauss defined $\left(\frac{\alpha}{\pi}\right)$ ***(quartic residue symbol)*** to be the unique 4th root of 1 such that

$$\left(\frac{\alpha}{\pi}\right) \equiv \alpha^{\frac{\mathbb{N}\pi-1}{4}} \mod \pi$$

and proved a ***quartic reciprocity law*** for these symbols. Later Eisenstein proved a ***cubic reciprocity law.*** Emil Artin remarked that his theorem (V 3.5) implied all possible such reciprocity laws, and therefore can be considered as a "reciprocity law for fields not containing an nth root of 1". In the remainder of this section, we explain this remark.

The power residue symbol

Let K be a number field containing a primitive nth root of 1. For every finite set $a, b, \ldots$ of elements of K, we define $S(a, b, \ldots)$ to be the set of prime ideals of K such that $\operatorname{ord}_{\mathfrak{p}}(n) \neq 0$, or $\operatorname{ord}_{\mathfrak{p}}(a) \neq 0$, or $\operatorname{ord}_{\mathfrak{p}}(b) \neq 0$,... . In particular, S itself consists only of the divisors of n.

Recall that the discriminant of $X^n - 1$ is divisible only by the primes dividing n. Therefore $X^n - 1$ has n distinct roots in $\mathbb{F}_p^{\mathrm{al}}$ for any $p \nmid n$, and the map

$$\zeta \mapsto \zeta \mod \mathfrak{p} : \mu_n(K) \to \mu_n(\mathcal{O}_K/\mathfrak{p})$$

is bijective for any prime ideal $\mathfrak{p} \nmid n$. For such a prime $\mathfrak{p}$, let $q = \mathbb{N}\mathfrak{p} \stackrel{\text{def}}{=} (\mathcal{O}_K : \mathfrak{p})$. Then $\mathbb{F}_q^\times$ is cyclic of order $q-1$, and so $n | q-1$ and $\zeta^{\frac{q-1}{n}} \in \mu_n \subset \mathbb{F}_q^\times$.

For $a \in K^\times$ and $\mathfrak{p} \notin S(a)$, define $\left(\frac{a}{\mathfrak{p}}\right)$ to be the unique nth root of 1 such that

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{\mathbb{N}\mathfrak{p}-1}{n}} \mod \mathfrak{p}.$$

5.1 *For every $a, b \in K^\times$ and $\mathfrak{p} \notin S(a, b)$,*

$$\left(\frac{ab}{\mathfrak{p}}\right) = \left(\frac{a}{\mathfrak{p}}\right)\left(\frac{b}{\mathfrak{p}}\right).$$

This is obvious from the definition.

5.2 *For $a \in K^\times$ and $\mathfrak{p} \notin S(a)$, the following are equivalent:*

(a) $\left(\frac{a}{\mathfrak{p}}\right) = 1$;

(b) *a becomes an nth power in $\mathcal{O}_K/\mathfrak{p}$;*

(c) *a becomes an nth power in $K_{\mathfrak{p}}$.*

The equivalence of (a) and (b) follows from the exactness of

$$1 \to \mathbb{F}_q^{\times n} \to \mathbb{F}_q^\times \xrightarrow{x \mapsto x^{\frac{q-1}{n}}} \mu_n \to 1, \qquad q = \mathbb{N}\mathfrak{p}.$$

If $X^n - a$ has a solution modulo $\mathfrak{p}$, then Hensel's lemma (ANT, 7.33) shows that it has a solution in $K_{\mathfrak{p}}$. Conversely, if $a = \alpha^n$, $\alpha \in K_{\mathfrak{p}}$, then $\operatorname{ord}_{\mathfrak{p}}(\alpha) = \frac{1}{n}\operatorname{ord}_{\mathfrak{p}}(a) = 0$, and so $\alpha \in \mathcal{O}_{K_{\mathfrak{p}}}$. The map $\mathcal{O}_K \to \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}$ is surjective, and so there is an $\alpha_0 \in \mathcal{O}_K$ mapping to α modulo $\mathfrak{p}$.

We extend the mapping $\mathfrak{p} \mapsto \left(\frac{a}{\mathfrak{p}}\right)$ to $I^{S(a)}$ by linearity: thus, for $\mathfrak{b} = \prod \mathfrak{p}_i^{r_i} \in I^{S(a)}$,

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod \left(\frac{a}{\mathfrak{p}_i}\right)^{r_i}.$$

We abbreviate $\left(\frac{a}{(b)}\right)$ to $\left(\frac{a}{b}\right)$.

For an abelian extension L/K in which the primes in S' do not ramify, $\psi_{L/K} : I^S \to \operatorname{Gal}(L/K)$ denotes the Artin map (see Chapter V).

5.3 *For every $a \in K^\times$ and $\mathfrak{b} \in I^{S(a)}$,*

$$\psi_{K[a^{\frac{1}{n}}]/K}(\mathfrak{b})(a^{\frac{1}{n}}) = \left(\frac{a}{\mathfrak{b}}\right) a^{\frac{1}{n}}.$$

From Galois theory, we know that there is an nth root $\zeta(\mathfrak{b})$ of 1 such that $\psi(\mathfrak{b})(a^{\frac{1}{n}}) = \zeta(\mathfrak{b}) \cdot a^{\frac{1}{n}}$ and that the map $\mathfrak{b} \mapsto \zeta(\mathfrak{b})$ is a homomorphism. Therefore, it suffices to prove the equality with $\mathfrak{b} = \mathfrak{p}$, a prime ideal. By definition,

$$\psi(\mathfrak{p})(x) \equiv x^{\mathbb{N}\mathfrak{p}} \mod \mathfrak{p}.$$

From

$$\psi(\mathfrak{p})(a^{\frac{1}{n}}) = \zeta(\mathfrak{p}) \cdot a^{\frac{1}{n}}$$

we find that

$$\zeta(\mathfrak{p}) \cdot a^{\frac{1}{n}} \equiv a^{\frac{\mathbb{N}\mathfrak{p}}{n}} \mod \mathfrak{p},$$

from which it follows that $\zeta(\mathfrak{p}) = \left(\frac{a}{\mathfrak{p}}\right)$.

5.4 *Let $a \in \mathcal{O}_K$, and let $\mathfrak{b}$ be an integral ideal in $I^{S(a)}$. If $a' \in \mathcal{O}_K$, $a' \equiv a \mod \mathfrak{b}$, then $\mathfrak{b} \in I^{S(a')}$ and*

$$\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a'}{\mathfrak{b}}\right).$$

For every prime ideal $\mathfrak{p}$ dividing $\mathfrak{b}$, $a' \equiv a \mod \mathfrak{p}$, and so $\left(\frac{a}{\mathfrak{p}}\right) = \left(\frac{a'}{\mathfrak{p}}\right)$.

The Artin Reciprocity Law allows us to prove a similar, but weaker, result for $\left(\frac{a}{\mathfrak{b}}\right)$ regarded as a function of $\mathfrak{b}$.

5.5 *Let $a \in K^\times$. There exists a modulus $\mathfrak{m}$ with support in $S(a)$ such that $\left(\frac{a}{\mathfrak{b}}\right)$ depends only on the class of $\mathfrak{b}$ in the ray class group $C_\mathfrak{m}$.*

According to Proposition VII A.5, $S(a)$ contains all primes ramifying in $K[a^{\frac{1}{n}}]$. Therefore, Artin's Reciprocity Law (V 3.5) shows that there exists a modulus $\mathfrak{m}$ with support in $S(a)$ such that $\psi(\mathfrak{b})$ depends only on the class of $\mathfrak{b}$ in the ray class group $C_\mathfrak{m}$.

NOTES Copied from mo299588. The power residue symbol is a unitary Hecke character of K, with trivial infinity type, with finite order, and with conductor dividing a power of $\mathfrak{m}$. This fact follows from class field theory, from example, from VIII, 5.5, of these notes. (Explanation to be added.)

The Hilbert symbol

Let K_v be a local field containing a primitive nth root of 1. The ***Hilbert symbol*** is a pairing

$$a, b \mapsto (a, b)_v : K_v^\times / K_v^{\times n} \times K_v^\times / K_v^{\times n} \to \mu_n,$$

where μ_n is the group of nth roots of 1 in K_v. Probably the most natural way of defining this is as the cup-product map

$$H^1(G, \mu_n) \times H^1(G, \mu_n) \to H^2(G, \mu_n \otimes \mu_n), \quad G = \mathrm{Gal}(K^{\mathrm{al}}/K),$$

followed by the isomorphism

$$H^2(G, \mu_n \otimes \mu_n) = H^2(G, \mu_n) \otimes \mu_n \to \mu_n$$

defined by the invariant map inv_v. However, in the spirit of the 1920s and 1930s, I'll define it in terms of central simple algebras.

Recall (IV.5) that for any $a, b \in K_v^\times$, we define $A(a,b;\zeta)$ to be the K_v-algebra with generators elements i, j and relations

$$i^n = a, \quad j^n = b, \quad ij = \zeta ji.$$

It is a central simple algebra of degree n over K_v. In the case that $n = 2$, $A(a,b;-1)$ is the quaternion algebra $H(a,b)$. We define

$$(a,b)_v = \zeta^{-n\cdot \mathrm{inv}_v([A(a,b;\zeta)])},$$

where $[A(a,b;\zeta)]$ is the class of $A(a,b;\zeta)$ in $\mathrm{Br}(K_v)$. Because $A(a,b;\zeta)$ is split by a field of degree n (in fact, by any maximal subfield, for example, $\mathbb{Q}[i]$), its invariant is an element of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, and hence $n\cdot \mathrm{inv}_v([A(a,b;\zeta)])$ is an element of $\mathbb{Z}/n\mathbb{Z}$. Clearly the isomorphism class of $A(a,b;\zeta)$ depends only on a and b as elements of $K_v^\times/K_v^{\times n}$, and so we do have a pairing

$$K_v^\times/K_v^{\times n} \times K_v^\times/K_v^{\times n} \to \mu_n.$$

However, it is not obvious from this perspective that the pairing is bilinear.

EXAMPLE 5.6 Consider the case $K_v = \mathbb{Q}_p$, p an odd prime, and $n = 2$. Then $(a,b)_p = \pm 1$, and

$$\begin{aligned}(a,b)_p = 1 &\iff H(a,b) \approx M_2(K_v);\\ &\iff X^2 - aY^2 - bZ^2 + abT^2 \text{ represents 0 in } K_v;\\ &\iff b \text{ is a norm from } K[\sqrt{a}];\\ &\iff X^2 - aY^2 - bZ^2 \text{ represents 0 in } K_v.\end{aligned}$$

To prove the equivalences use (respectively) that: a quaternion algebra has invariant $\frac{1}{2}$ if and only if it is a division algebra; Exercise IV.5.7; Proposition 3.7d; Proposition 3.7c. The last condition shows that our definition of the Hilbert symbol agrees with that, for example, in Serre 1970, III

5.7 *For any a, b,*

$$A(b,a;\zeta) \approx A(a,b;\zeta^{-1}) \approx A(a,b;\zeta)^{\mathrm{opp}}.$$

Therefore

$$(b,a)_v = (a,b)_v^{-1}.$$

By definition $A(b,a;\zeta)$ is the K_v-algebra with generators i', j' and relations $i'^n = b$, $j'^n = a$, and $i'j' = \zeta i'j'$. The map $i' \mapsto j$, $j' \mapsto i$ is an isomorphism $A(b,a;\zeta) \to A(a,b;\zeta^{-1})$. The map $i \mapsto i$, $j \mapsto j$ is an isomorphism $A(a,b;\zeta)^{\mathrm{opp}} \to A(a,b;\zeta^{-1})$.

5.8 *Let $a, b \in K^\times$. For any $v \notin S(a)$, $(a,b)_v = \left(\frac{a}{\mathfrak{p}_v}\right)^{\mathrm{ord}_v(b)}$.*

For simplicity, we assume that $A(a,b;\zeta)$ is a division algebra. Recall (IV.4) that, to compute the invariant of a central division algebra D over a local field K_v, we

(a) choose a maximal unramified field $L \subset D$;

(b) find an element $\beta \in D$ such that $\alpha \mapsto \beta\alpha\beta^{-1}$ is the Frobenius automorphism of L (such an α exists by the Noether-Skolem Theorem);

(c) set $\operatorname{inv}_v([D]) = \operatorname{ord}_v(\beta)$.

We apply this with $L = K_v[i] = K_v[a^{\frac{1}{n}}]$. Note that, because $v \notin S(a)$, this extension is unramified. Let $\left(\frac{a}{\mathfrak{p}_v}\right) = \zeta^r$, so that $(\mathfrak{p}, L/K_v)(i) = \zeta^r i$. Since $jij^{-1} = \zeta^{-1}i$, we see that we can take $\beta = j^{-r}$. Then $\beta^n = b^{-r}$, and so $\operatorname{ord}_v(\beta) = -\frac{r}{n}\operatorname{ord}_v(b)$. Hence

$$(a,b)_v \stackrel{\text{def}}{=} \zeta^{-n\operatorname{inv}_v(A(a,b;\zeta))} = \zeta^{r\cdot\operatorname{ord}_v(b)} = \left(\frac{a}{\mathfrak{p}_v}\right)^{\operatorname{ord}_v(b)}.$$

REMARK 5.9 In fact,

$$(a,b)_v = \frac{\phi_v(b)(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}$$

for all a, b, v. See III, 4.5.

5.10 *For $a, b \in K^\times$,*

$$\prod_v (a,b)_v = 1.$$

In the course of proving the Reciprocity Law, we showed that, for every $\beta \in \operatorname{Br}(K)$, $\sum \operatorname{inv}_v(\beta) = 0$. In particular, $\sum \operatorname{inv}_v(A(a,b;\zeta)) = 0$, and this implies the formula.

For $a, b \in K^\times$, define

$$\left(\frac{a}{b}\right) = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{\operatorname{ord}_v(b)} = \left(\frac{a}{(b)^{S(a)}}\right),$$

where $(b)^{S(a)}$ is the ideal in $I^{S(a)}$ generated by b. The symbol $\left(\frac{a}{b}\right)$ is multiplicative in b, but $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$ will not always hold unless $S(b) \cap S(a,a') = S$.

THEOREM 5.11 (POWER RECIPROCITY LAW) *Let a and b be elements of $K^\times$ such that $S(a) \cap S(b) = S$ (for example, a and b could be relatively prime). Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S} (b,a)_v.$$

Moreover, if $S(c) = S$, then

$$\left(\frac{c}{b}\right) = \prod_{v \in S} (b,c)_v .!!(c,b)!!$$

PROOF. Let $S'(a) = S(a) \smallsetminus S$ and $S'(b) = S(b) \smallsetminus S$. Our assumption is that $S'(a)$ and $S'(b)$ are disjoint. Then

$$\left(\frac{a}{b}\right) = \prod_{v \in S'(b)} \left(\frac{a}{\mathfrak{p}_v}\right)^{\operatorname{ord}_v(b)} = \prod_{v \in S'(b)} (a,b)_v$$

and

$$\left(\frac{b}{a}\right) = \prod_{v \in S'(a)} \left(\frac{b}{\mathfrak{p}_v}\right)^{\operatorname{ord}_v(a)} = \prod_{v \in S'(a)} (b,a)_v.$$

Therefore

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v\in S'(a)\cup S'(b)} (a,b)_v.$$

For $v \notin S \cup S'(a) \cup S'(b)$, $(a,b)_v = 0$ (by 5.8 for example), and so the product formula shows that

$$\prod_{v\in S'(a)\cup S'(b)} (a,b)_v \times \prod_{v\in S}(a,b)_v = 1.$$

This completes the proof of the first equality, and the second is obvious. □

To obtain a completely explicit formula, it remains to compute the Hilbert symbol for the $v \in S$. For the infinite primes, this is easy: if v is complex, then $(a,b)_v = 1$ always, and if v is real, then

$$(a,b)_v = 1 \iff X^2 - aY^2 - bZ^2 \text{ represents } 0 \iff a > 0 \text{ or } b > 0.$$

For $K = \mathbb{Q}$ and $n = 2$,

$$(u2^r, v2^s)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2} + r\frac{v^2-1}{8} + s\frac{u^2-1}{8}},$$

where u and v are 2-adic units, and the exponent is to be interpreted modulo 2. For an elementary proof of this, see Serre 1970, III, 1.2. On applying this formula successively to the pairs (p,q) with p and q odd primes, $(2,p)$ with p an odd prime, and to $(-1,p)$ with p an odd prime, one obtains the classical quadratic reciprocity law (including the supplements).

For p an odd prime and $K = \mathbb{Q}[\zeta]$ with ζ a primitive pth root of 1, one can make the Hilbert symbol $(a,b)_p$ completely explicit. Recall that p is totally ramified in K and $(p) = (\pi)^{p-1}$, where $\pi = 1-\zeta$. Let K_π denote the completion of K at (π), and let U_i denote the group of units in K_π congruent to 1 mod π^i. We have a filtration

$$\mathcal{O}_{K_\pi}^\times \supset U_1 \supset U_2 \supset \cdots \supset U_{p+1} \supset \cdots.$$

If $u \in U_{p+1}$, then u is a pth power in K_π (see VII A.6a). From this, one can deduce that $K_\pi^\times / K_\pi^{\times p}$ is freely generated (as an $\mathbb{F}_p$-vector space) by the elements

$$\pi, \zeta, 1-\pi^2, \ldots, 1-\pi^p.$$

Let $\eta_i = 1-\pi^i$, $i \geq 1$ (e.g., $\eta_1 = \zeta$).

PROPOSITION 5.12 *The Hilbert pairing*

$$a, b \mapsto (a,b)_\pi : K_\pi^\times \times K_\pi^\times \to \mu_p$$

is the unique skew-symmetric pairing satisfying

(a) $(\eta_i, \eta_j)_\pi = (\eta_i, \eta_{i+j})_\pi (\eta_{i+j}, \eta_j)_\pi (\eta_{i+j}, \pi)_\pi^{-j}$ *for all* $i, j \geq 1$;

(b) $(\eta_i, \pi)_\pi = \begin{cases} 1 & \text{if} \quad 1 \leq i \leq p-1 \\ \zeta & \text{if} \quad i = p. \end{cases}$

(c) $(\cdot,\cdot)_\pi = 1$ *on* $U_i \times U_j$ *if* $i + j \geq p+1$.

For hints, see Cassels and Fröhlich 1967, p. 354.

EXAMPLE 5.13 (Cubic reciprocity law; Eisenstein). Let $p = 3$, so that $K = \mathbb{Q}[\zeta]$, $\zeta = \frac{-1+\sqrt{3}}{2}$, and $\pi = -\zeta\sqrt{3}$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta]$, and every nonzero element of $\mathcal{O}_K$ can be written in the form $\zeta^i \pi^j a$ with $a \equiv \pm 1 \mod 3\mathcal{O}_K$. In this case, the reciprocity law becomes:

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$$

if a and b are relatively prime and congruent to $\pm 1 \mod 3\mathcal{O}_K$, and

$$\begin{cases} \left(\frac{\zeta}{a}\right) &= \zeta^{-m-n} \\ \left(\frac{\pi}{a}\right) &= \zeta^m \end{cases}$$

if $a = \pm(1 + 3(m + n\zeta))$.

Note that, if $a \in \mathbb{Z}$, then $a \equiv \pm 1 \mod 3\mathcal{O}_K$ is automatic.

Application

Fix an odd prime p and a primitive pth root ζ of 1. If x, y, z are integers such that $x^p + y^p = z^p$, then

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = z^p.$$

We may suppose that x, y, z have no common factor. If $p \nmid xyz$, then the elements $x + \zeta^i y$ of $\mathbb{Z}[\zeta]$ are relatively prime (ANT, 6.9). Therefore, each generates an ideal that is a pth power, and the same is true of

$$\alpha = \frac{x + \zeta y}{x + y} = 1 - \frac{y\pi}{x + y}, \quad \pi = 1 - \zeta.$$

Hence[5] $\left(\frac{\beta}{\alpha}\right) = 1$ for all $\beta \in \mathbb{Z}[\zeta]$ relatively prime to α.

THEOREM 5.14 *Let x, y, z be relative prime positive integers such that $p \nmid xyz$ and $x^p + y^p = z^p$. For every prime q dividing xyz, $q^{p-1} \equiv 1 \mod p^2$.*

PROOF. In this case, the Power Reciprocity Law becomes

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)^{-1} = \zeta^{\mathrm{Tr}_{\mathbb{Q}[\zeta]/\mathbb{Q}}(\eta)},$$

where $\eta = \frac{\beta-1}{p}\frac{\alpha-1}{\pi}$. We apply this equation with $\beta = q^{p-1}$. Without loss of generality, we may assume that $q|y$, so that $\alpha \equiv 1 \mod q$ and $\left(\frac{\alpha}{q}\right) = 1$. Moreover,

$$\mathrm{Tr}(\eta) = \frac{q^{p-1} - 1}{p} \mathrm{Tr}(\frac{\alpha - 1}{\pi}),$$

but

$$\mathrm{Tr}\,\frac{\alpha - 1}{\pi} = \mathrm{Tr} - \frac{y}{x + y} = -\frac{y}{x + y}(p - 1),$$

which is not divisible by p. Therefore $\frac{q^{p-1}-1}{p}$ is divisible by p. □

[5] This fixes a confusing misprint in the last version; see sx667386.

COROLLARY 5.15 (WIEFERICH'S CONDITION) *If $X^p + Y^p = Z^p$ admits a solution x, y, z with x, y, z positive integers none of which is divisible by p, then $2^{p-1} \equiv 1 \bmod p^2$.*

PROOF. If $x^p + y^p = z^p$, then at least one of x, y, or z must be even. □

A similar argument (with a different β) proves Mirimanoff's condition: $3^{p-1} \not\equiv 1 \bmod p^2$.

The only primes $< 3 \times 10^9$ satisfying Wieferich's condition are 1093 and 3511, and they fail Mirimanoff's condition. Thus this proves the first case of Fermat's last theorem for $p < 3 \times 10^9$.

EXERCISE 5.16 Let $p \in \mathbb{Z}$ be a prime congruent to 1 modulo 3 (so that $\mathbb{F}_p$ contains the cube roots of 1). Show that 2 is a cube modulo p if and only if p is of the form $x^2 + 27y^2$, $x, y \in \mathbb{Z}$.

NOTES Theorem 5.14 was proved by Furtwängler (see Hasse 1970, II, 22); see also Koch 1992, II, 6.3, and Herbrand 1936, p. 47. Class field theory also allows one to simplify the proof of Kummer's second criterion when the second case of Fermat's theorem holds (J. Herbrand, Sur les classes des corps circulaires, J. Math. Pures Appl., IX. Sér. 11, 417–441.

6 The Classification of Quadratic Forms over a Number Field

Earlier we showed that a nondegenerate quadratic form over a number field represents 0 in the field if and only if it represents zero in every completion of the field. In this section, we completely classify the quadratic forms over a number field. Specifically, we shall:

(a) Show that two quadratic forms over a number field K are equivalent if and only if they are equivalent over every completion of K.

(b) Give a complete list of invariants for the quadratic forms over a local field.

(c) Determine which families of local invariants arise from a global quadratic form.

Generalities on quadratic forms

In this subsection, k is an arbitrary field of characteristic $\neq 2$. Let (V, Q) be a quadratic space over k with corresponding bilinear form B,

$$B(v, w) = \frac{1}{2}(Q(v + w) - Q(v) - Q(w)),$$

and let U_1 and U_2 be subspaces of V. If every element of V can be written uniquely in the form $v = u_1 + u_2$ with $u_1 \in U_1$ and $u_2 \in U_2$, then we write $V = U_1 \oplus U_2$. If, addition, $B(u_1, u_2) = 0$ for all $u_1 \in U_1$ and $u_2 \in U_2$, then we write $V = U_1 \perp U_2$. For every subspace U of V,

$$U^\perp = \{v \in V \mid B(u, v) = 0 \text{ for all } u \in U\}.$$

If $Q|U$ is nondegenerate, then $V = U \perp U^\perp$.

Let (V, Q) and (V', Q') be quadratic spaces over k. A ***morphism*** $s : (V, Q) \to (V', Q')$ is a linear map $s : V \to V'$ of k-vector spaces such that $Q'(s(v)) = Q(v)$ for all $v \in V$. A morphism is an ***isomorphism*** if it admits an inverse that is also morphism. An isomorphism $(V, Q) \to (V', Q')$ will also be called an ***isometry.***

PROPOSITION 6.1 *Let (V, Q) be a quadratic space. If Q represents $a \in k^\times$, then there exists an $e \in V$ with $Q(e) = a$ and a subspace U of V such that $V = U \perp k \cdot e$.*

PROOF. Because Q represents a, there does exist an $e \in V$ such that $Q(e) = a$, and we can take U to be the orthogonal complement of $k \cdot e$. □

Let (V, Q) be a quadratic space. For every $y \in V$ with $Q(y) \neq 0$, we define the ***symmetry with respect to y (or with respect to the line $k \cdot y$)*** to be the map

$$\tau_y(x) = x - \frac{2B(x, y)}{Q(y)} y.$$

Note that τ_y is a morphism $(V, Q) \to (V, Q)$ and that $\tau_y \circ \tau_y = \mathrm{id}$, and so τ_y is an isometry. It reverses every vector in the line $k \cdot y$, and leaves every vector in the hyperplane $(k \cdot y)^\perp$ fixed. It is therefore reflection in the hyperplane $(k \cdot y)^\perp$.

PROPOSITION 6.2 *Let U and W be isometric subspaces of a quadratic space (V, Q) and assume that $Q|U$ is nondegenerate. Then $U^\perp$ and $W^\perp$ are isometric.*

PROOF. We prove this by induction on the dimension of U. Suppose first that U and W are lines, say $U = ku$ and $W = kw$. Then $Q(u) \neq 0$, $Q(w) \neq 0$, and we may suppose that $Q(u) = Q(w)$. From

$$Q(u + w) + Q(u - w) = 2Q(u) + 2Q(w) = 4Q(u)$$

we see that at least one of $Q(u+w)$ or $Q(u-w)$ is nonzero, and, after replacing w with $-w$ if necessary, we may suppose that it is the latter. Therefore the symmetry τ_{u-w} is defined:

$$\tau_{u-w} x = x - \frac{2B(x, u - w)}{Q(u - w)}(u - w).$$

Then $\tau_{u-w}(u) = w$, because

$$Q(u - w) = Q(u) + Q(w) - 2B(u, w) = 2Q(u) - 2B(u, w) = 2B(u, u - w),$$

and so τ_{u-w} maps $U^\perp$ isometrically onto $W^\perp$.

Thus, we may suppose that $\dim U \geq 2$, and so admits a nontrivial decomposition $U = U_1 \perp U_2$. Because $W \approx U$, there is a decomposition $W = W_1 \perp W_2$ with $U_1 \approx W_1$ and $U_2 \approx W_2$. Note that $Q|U_1$ will be nondegenerate, and that $U_1^\perp = U_2 \perp U^\perp$. The induction hypothesis implies that $U_2 \perp U^\perp$ is isometric to $W_2 \perp W^\perp$, and the choice of an isometry defines a decomposition $U_2 \perp U^\perp = X \perp Y$ with $X \approx W_2$ and $Y \approx W^\perp$. But then $X \approx U_2$, and the induction hypothesis shows that $Y \approx U^\perp$. Hence $W^\perp \approx U^\perp$. □

On choosing a basis e_i for a quadratic space (V, Q), we obtain a quadratic form

$$q(X_1, \ldots, X_n) = \sum a_{ij} X_i X_j, \qquad a_{ij} = B(e_i, e_j).$$

Conversely, a quadratic form q defines a quadratic space (k^n, q).

Two quadratic forms q and q' are said to be ***equivalent***, $q \sim q'$, if they define isomorphic quadratic spaces, i.e., if one can be obtained from the other by an invertible change of variables. If q and q' are quadratic forms in distinct sets of variables, then we denote $q + q'$ by $q \perp q'$; then $(k^{m+n}, q \perp q') = (k^m, q) \perp (k^n, q')$.

From Proposition 6.2 we find that:

Let $q = r \perp s$ and $q' = r' \perp s'$ be two quadratic forms, and assume that r is nondegenerate. If $q \sim q'$ and $r \sim r'$, then $s \sim s'$.

From Proposition 6.1 we find that

A nondegenerate quadratic form q in n variables represents a if and only if $q \sim r \perp aZ^2$, where r is a quadratic form in $n-1$ variables.

The ***rank*** of a quadratic space (V, Q) is defined to be the rank of the matrix $(B(e_i, e_j))$ for some basis e_i of V. The ***rank*** of a quadratic form q is the rank of the corresponding quadratic space. When q is written in diagonal form, $q = a_1X_1^2 + \cdots + a_rX_r^2$, then the rank of q is the number of nonzero coefficients a_i, i.e., the number of variables actually occurring in q.

The local-global principle

THEOREM 6.3 (HASSE-MINKOWSKI) *Let q and q' be quadratic forms over a number field K. If q and q' become equivalent over K_v for all primes v, then q and q' are equivalent over K.*

PROOF. We may suppose that q and q' are nondegenerate. We use induction on the common rank n of q and q'. If $n = 0$, both forms are zero, and there is nothing to prove. Otherwise, there exists an $a \in K^\times$ represented by q. Then $q(X_1, \dots, X_n) - aZ^2$ represents 0 in K, and hence in K_v for all v. On applying Theorem 3.5, to $q' - aZ^2$, we find that q' represents a in K. Therefore, $q \sim q_1 \perp aZ^2$ and $q' \sim q_1' \perp aZ^2$ for some quadratic forms q_1 and q_2 of rank $n-1$. Now (6.2) shows that $q_1 \sim q_2$ over K_v for all v, and so (by induction) they are equivalent over K. This implies that q and q' are equivalent over K. □

REMARK 6.4 Let (V, Q) be a quadratic space over a field k, and let O be its group of isometries. Theorem 6.3 says that

$$H^1(K, O) \to \prod_v H^1(K_v, O)$$

is injective.

The classification of quadratic forms over a local field

The archimedean case. Any quadratic form over $\mathbb{C}$ (as for any algebraically closed field of characteristic $\neq 2$) is equivalent to a unique quadratic form

$$X_1^2 + \cdots + X_n^2.$$

Thus two quadratic forms over $\mathbb{C}$ are equivalent if and only if they have the same rank n.

According to Sylvester's theorem, a quadratic form q over $\mathbb{R}$ is equivalent to a unique quadratic form

$$X_1^2 + \cdots + X_r^2 - X_{r+1}^2 - \cdots - X_{r+t}^2.$$

The number t of -1's is the ***index of negativity.*** Thus, two quadratic forms over $\mathbb{R}$ are equivalent if and only if they have the same rank n and the same index of negativity t.

The nonarchimedean case. Let K be a local field. Recall that the Hilbert symbol $(\cdot, \cdot)$ can defined for $a, b \in K^\times$ by

$$(a,b) = \begin{cases} 1 & \iff X^2 - aY^2 - bZ^2 \text{ represents } 0 \iff aY^2 + bZ^2 \text{ represents } 1 \\ -1 & \text{otherwise.} \end{cases}$$

LEMMA 6.5 *The Hilbert symbol has the following properties:*

(a) *it is bi-multiplicative and* $(ac^2, bd^2) = (a,b)$ *for all* $a,b,c,d \in K^\times$;

(b) *for any nonsquare* $a \in K^\times$, *there exists a* $b \in K^\times$ *such that* $(a,b) = -1$;

(c) $(b,a) = (a,b)^{-1} = (a,b)$;

(d) $(a,-a) = (1,a) = 1$.

PROOF. Obviously, (a,b) does not change when a or b is multiplied by a square. Also, (c) is obvious.

Note that $(a,b) = 1$ if and only if b is a norm from $K[\sqrt{a}]$. From local class field theory, we know that if a is not a square in K, then $\mathrm{Nm}(K[\sqrt{a}]^\times)$ is a subgroup of index 2 in $K^\times$, and therefore $b \mapsto (a,b)$ is an isomorphism $K^\times/\mathrm{Nm}(K[\sqrt{a}]^\times) \to \{\pm 1\}$. This completes the proof of (a) and (b). Finally, $aX^2 - aY^2 = a(X^2 - Y^2)$, and $X^2 - Y^2$ represents a^{-1} because it represents 0. □

If $q \sim a_1X_1^2 + \cdots + a_nX_n^2$ with $a_1, \ldots, a_n \in K^\times$, then we set

$$\begin{aligned} n(q) &= n \\ d(q) &= a_1 \cdots a_n \qquad (\text{in } K_v^\times/K_v^{\times 2}) \\ S(q) &= \prod_{1\le i\le j\le n} (a_i, a_j) = \prod_{1\le i\le n} (a_i, d_i) \quad (\text{in } \{\pm 1\}), \end{aligned}$$

where $d_i = a_1 \ldots a_i$. Thus $n(q)$ is the rank of q and $d(q)$ is the discriminant of q. Both depend only on the equivalence class of q. We shall prove that the same is true of $S(q)$. It is called the ***Hasse invariant*** of q.

REMARK 6.6 Serre 1970, defines

$$\varepsilon(q) = \prod_{1\le i<j\le n} (a_i, a_j) = \prod (a_i, d_{i-1}).$$

Note that

$$S(q) = \varepsilon(q) \prod_{i=1}^{n} (a_i, a_i) = \varepsilon(q) \prod_{i=1}^{n} (-1, a_i)(-a_i, a_i) = \varepsilon(q)(-1, d(q)).$$

Thus the knowledge of $(d(q), S(q))$ is equivalent to the knowledge of $(d(q), \varepsilon(q))$.

PROPOSITION 6.7 *The element* $S(q)$ *depends only on the equivalence class of* q.

PROOF. It suffices to prove that $\varepsilon(q)$ depends only on the equivalence class of q. When q has rank 1, there is nothing to prove: $\varepsilon(q) = 1$ (empty product) for all q.

Next suppose that $q \sim aX^2 + bY^2 \sim a'X^2 + b'Y^2$. Because they are equivalent, either both $aX^2 + bY^2$ and $a'X^2 + b'Y^2$ represent 1 or neither represents 1, and so $(a,b) = (a',b')$.

Next suppose that $n > 2$ and that

$$q \sim a_1X_1^2 + \cdots + a_iX_i^2 + a_{i+1}X_{i+1}^2 + \cdots \sim a_1'X_1^2 + \cdots + a_i'X_i^2 + a_{i+1}'X_{i+1}^2 + \cdots$$

with $a_j = a_j'$ except possibly for $j = i, i+1$. We then have to prove that

$$(a_i, d_{i-1})(a_{i+1}, d_i) = (a_i', d_{i-1}')(a_{i+1}', d_i').$$

But

$$(a_i, d_{i-1})(a_{i+1}, d_i) = (a_i, d_{i-1})(a_{i+1}, d_{i-1})(a_{i+1}, a_i) = (a_i a_{i+1}, d_{i-1})(a_i, a_{i+1})$$

and $a_i a_{i+1}$ differs from $a'_i a'_{i+1}$ by a square, and so it remains to show that $(a_i, a_{i+1}) = (a'_i, a'_{i+1})$. According to Proposition 6.2, $a_i X_i^2 + a_{i+1} X_{i+1}^2 \sim a'_i X_i^2 + a'_{i+1} X_{i+1}^2$, and we already shown that this implies $(a_i, a_{i+1}) = (a'_i, a'_{i+1})$.

The following elementary lemma now completes the proof. □

LEMMA 6.8 *Let B and B' be orthogonal bases for a nondegenerate quadratic space (V, Q). Then there exists a chain of orthogonal bases $B_1, B_2, \dots, B_m$ such that $B_1 = B$ and $B_m = B'$, and each B_i is obtained from B_{i-1} by altering at most two adjacent elements.*

PROOF. See O'Meara 1963, Lemma 58.1. □

PROPOSITION 6.9 *Let q be a nondegenerate quadratic form in n variables over a nonarchimedean local field K, and let $a \in K^\times$. Then q represents a if and only if*

(a) *$n = 1$ and $a = d(q)$ (in $K^\times/K^{\times 2}$);*

(b) *$n = 2$ and $(a, -d)(-1, d) = S(q)$ (equivalently, $(a, -d) = \varepsilon(q)$);*

(c) *$n = 3$ and either $a \neq -d(q)$ (modulo squares) or $a = -d(q)$ (modulo squares) and $(-1, -1) = S(q)$;*

(d) *$n \geq 4$.*

PROOF. (a) Clearly dX^2 represents a if and only if $a = d$ (in $K^\times/K^{\times 2}$).

(b) Let $q = bX^2 + cY^2$. Clearly $bX^2 + cY^2$ represents a if and only if $abX^2 + acY^2$ represents 1, i.e., if and only if $(ab, ac) = 1$. But

$$(ab, ac) = (a, a)(a, b)(a, c)(b, c) = (a, -1)(a, d(q))(b, c) = (a, -d(q)) \cdot \varepsilon(q)$$

and so the condition is that

$$\varepsilon(q) = (a, -d(q)).$$

(c) Let $q = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2$. Then q represents a if and only if there exists an $e \in K^\times$ for which the equations

$$a_1 X_1^2 + a_2 X_2^2 = e = a_3 X_3^2 - a X_4^2$$

have solutions. According to (b), this will be so if and only if

$$(e, -a_1 a_2) = (a_1, a_2), \quad (e, a_3 a) = (a_3, -a). \qquad (*)$$

Consider two linear forms $f, g : V \to \mathbb{F}_2$ on an $\mathbb{F}_2$-vector space V of dimension ≥ 2. The simultaneous linear equations $f(x) = \varepsilon_1$, $g(x) = \varepsilon_2$ will have a solution unless they are inconsistent, i.e., unless $f = 0$ and $\varepsilon_1 = -1$; or $g = 0$ and $\varepsilon_2 = -1$; or $f = g$ and $\varepsilon_1 = -\varepsilon_2$.

When we apply this observation to the linear forms $(\cdot, -a_1 a_2)$, $(\cdot, a_3 a) : K^\times/K^{\times 2} \to \{\pm 1\}$, we find that there will exist an e satisfying $(*)$ unless $-a_1 a_2 = a_3 a$ (in $K^\times/K^{\times 2}$) and $(a_1, a_2) = -(a_3, a)$. The first equality says that $a = -d(q)$ (mod squares), and (when $a = -d(q)$) the second says that $(-1, -1) = S(q)$.

(d) In this case, $q(X_1, \dots, X_n) - aZ^2$ has rank ≥ 5, and therefore represents 0 (see 3.10). □

THEOREM 6.10 *Two quadratic forms over a nonarchimedean local field are equivalent if and only if they have the same rank, the same discriminant, and the same Hasse invariant.*

PROOF. We showed in Proposition 6.7 that equivalent forms have the same invariants. For the converse, we use induction on the common rank n of the two forms q and q'. Two quadratic forms of rank 1 are obviously equivalent if they have the same discriminant, and so we may suppose $n > 1$. From Proposition 6.9, we see that q and q' represent the same elements in $K^\times$. In particular, there is an $a \in K_v^\times$ that is represented by both q and q'. Thus,

$$q \sim q_1 + aZ^2, \quad q' \sim q_1' + aZ^2$$

with q_1 and q_1' quadratic forms of rank $n-1$. Now

$$d(q) = a \cdot d(q_1), \quad S(q) = (a, d(q_1)) \cdot S(q_1)$$

and similarly for q' and q_1'. Therefore, q_1 and q_1' have the same invariants, and the induction hypothesis shows that $q_1 \sim q_1'$. □

PROPOSITION 6.11 *Let q be a quadratic form of rank n over a nonarchimedean local field K.*

(a) *If $n = 1$, then $S(q) = (-1, d)$.*

(b) *If $n = 2$, then $d(q) = -1$ (mod squares) implies $S(q) = (-1, -1)$.*

Apart from these constraints, every triple $n \geq 1$, $d \in K^\times/K^{\times 2}$, $s = \pm 1$, occurs as the set of invariants of a quadratic form over K.

PROOF. CASE $n = 1$. Then $q = dX^2$, and $S(q) = (d, d) = (-1, d)$.

CASE $n = 2$. For $q = aX^2 + bY^2$, $S(q) = (a, a)(b, d)$, and so

$$d = -1 \Rightarrow S(q) = (-1, a)(-1, b) = (-1, d) = (-1, -1).$$

Conversely, the form $X^2 - Y^2$ has $d = -1$ and $S = (-1, -1)$.

Now suppose $d \neq -1$ and s are given. We seek an $a \in K^\times$ such that $q \stackrel{\text{def}}{=} aX^2 + adY^2$ has $S(q) = s$. But

$$S(q) = (a, a)(ad, d) = (a, -1)(a, d)(d, d) = (a, -d)(d, d).$$

Because $-d \neq 1$ (in $K^\times/K^{\times 2}$), we can choose a so that $(a, -d) = s \cdot (d, d)$.

CASE $n = 3$. Choose an $a \in K^\times$ such that $a \neq -d$ in $K^\times/K^{\times 2}$. Because of the condition on a, there exists a quadratic form q_1 of rank 2 such that

$$d = d(q_1)a, \quad s = S(q_1)(a, d).$$

Take $q = q_1 + aZ^2$.

CASE $n \geq 4$. There exists a quadratic form with the shape

$$q_1(X_1, X_2, X_3) + X_4^2 + \cdots + X_n^2$$

having the required invariants. □

GENERALITIES. We define the Hasse invariant for a quadratic form q over $\mathbb{R}$ or $\mathbb{C}$ by the same formula as in the nonarchimedean case. For $\mathbb{C}$, $S(q) = 1$ always, and for $\mathbb{R}$, $S(q) = (-1)^{t(t+1)/2}$, where t is the index of negativity (because $(-1,-1) = -1$). Note that in the second case, $d(q) = (-1)^t$ (in $\mathbb{R}^\times/\mathbb{R}^{\times 2}$), and that $d(q)$ and $S(q)$ determine t when $r \leq 3$ but not for $r > 3$.

We say that a system $(n, d, s, \dots)$, $n \in \mathbb{N}$, $d \in K^\times/K^{\times 2}$, $s \in \{\pm 1\}$,... is ***realizable*** there exists a quadratic form q having $n(q) = n$, $d(q) = d$, $S(q) = s, \dots$.

(a) For a nonarchimedean local field K, (n, d, s) is realizable provided $s = 1$ when $n = 1$ and $s = (-1,-1)$ when $n = 2$ and $d = -1$.

(b) For $\mathbb{R}$, (n, d, s, t) is realizable provided $0 \leq t \leq r$, $d = (-1)^t$, $s = (-1)^{t(t+1)/2}$.

Classification of quadratic forms over global fields

THEOREM 6.12 *Let $n \in \mathbb{N}$, and suppose that for each prime v of the number field K there is given a nondegenerate quadratic form $q(v)$ of rank n over K_v. Then there exists a quadratic form q_0 over K such that $(q_0)_v \sim q_v$ for every v if and only if*

(a) *there exists a $d_0 \in K^\times$ such that $d_0 \equiv d(q_v) \mod K_v^{\times 2}$ for all v;*

(b) *$S(q(v)) = 1$ for almost all v and $\prod_v S(q(v)) = 1$.*

The conditions are obviously necessary. In view of Proposition 6.11 and the following remarks, we can restate the theorem as follows. Suppose given:

- ◇ an $n \geq 1$ and a $d_0 \in K^\times/K^{\times 2}$;
- ◇ for each prime v, finite or real, an $s_v \in \{\pm 1\}$;
- ◇ for each real prime v, an integer t_v.

Then, there exists a quadratic form q over K of rank n, discriminant d_0, Hasse invariant $S_v(q) = s_v$ for all v, and index of negativity $t_v(q) = t_v$ for all real v if and only if

(a) $s_v = 1$ for all but finitely many v and $\prod_v s_v = 1$;

(b) if $n = 1$, then $s_v = (-1, d)_v$; if $n = 2$, then either $d \neq -1$ in $K_v^\times/K_v^{\times 2}$ or $s_v = (-1,-1)_v$;

(c) for all real v, $0 \leq t_v \leq n$, $d_v = (-1)^{t_v}$ (modulo squares), and $s_v = (-1)^{t_v(t_v+1)/2}$.

In the case $n = 1$, $q_v = d(q_v)X^2$, and we can take $q_0 = d_0X^2$, where d_0 is the element of $K^\times$ whose existence is guaranteed (a).

The key case is $n = 2$, and for that we need the following lemma, whose proof requires class field theory.

LEMMA 6.13 *Let T be finite set of real or finite primes of K, and let $b \in K^\times$. If T has an even number of elements and b does not become a square in $K_v^\times$ for any $v \in T$, then there exists an $a \in K^\times$ such that*

$$(a, b)_v = \begin{cases} -1 & \text{for } v \in T \\ 1 & \text{otherwise.} \end{cases}$$

PROOF. (Following Tate, 1976, 5.2). Let L be the composite of all abelian extensions of K of exponent 2, and let $G = \mathrm{Gal}(L/K)$. By class field theory,

$$G \simeq \boldsymbol{C}_K/2\boldsymbol{C}_K \simeq \mathbb{I}/K^\times \cdot \mathbb{I}^2.$$

The cohomology sequence of

$$0 \to \mu_2 \to L^\times \xrightarrow{x \mapsto x^2} L^{\times 2} \to 0$$

is an exact sequence

$$K^\times \xrightarrow{x \mapsto x^2} K^\times \cap L^{\times 2} \to \mathrm{Hom}_{\,\mathrm{conts}}(G, \mu_2) \to 0.$$

Every element of $K^\times$ becomes a square in L, and so we have an isomorphism

$$K^\times / K^{\times 2} \to \mathrm{Hom}_{\,\mathrm{conts}}(\mathbb{I}/K^\times \cdot \mathbb{I}^2, \mu_2).$$

This map sends $a \in K^\times$ to the continuous homomorphism

$$(c_v) \mapsto \prod (a, c_v)_v$$

(because of the relation between the Hilbert symbol and the local Artin map). Thus, finding a is equivalent to finding a homomorphism $f : \mathbb{I}/\mathbb{I}^2 \to \mu_2$ such that

(a) $f = 1$ on principal idèles;

(b) $f(1, \dots, 1, i_v(b), 1, \dots, 1) = \begin{cases} -1 & \text{for } v \in T \\ 1 & \text{otherwise.} \end{cases}$

where i_v is the inclusion $K \hookrightarrow K_v$. For each v, let B_v be the $\mathbb{F}_2$-subspace of $K_v^\times / K_v^{\times 2}$ generated by $i_v(b)$, and let $B = \prod B_v \subset \mathbb{I}/\mathbb{I}^2$. Because $i_v(b)$ is not a square for $v \in T$, there exists a linear form (automatically continuous) $f_1 : B \to \mu_2$ satisfying condition (b), and f_1 will extend to a continuous linear form on $\mathbb{I}/\mathbb{I}^2$ satisfying (a) if and only if f_1 takes the value 1 on every principal idéle in B. The value of f_1 on the principal idéle of b is $\prod_{v \in T} -1$, which is 1 because of our assumption that T contains an even number of elements. Let $c \in K^\times$ be such that its idéle lies in B. Then, for every v, $i_v(c) = 1$ or $i_v(b)$ in $K_v^\times / K_v^{\times 2}$. Therefore, $i_v(c)$ becomes a square in $K_v[\sqrt{b}]$ for all v, which (by 1.1) implies that c is a square in $K[\sqrt{b}]$. Hence $c = 1$ or b in $K^\times / K^{\times 2}$, and so f_1 takes the value 1 on its idèle. □

We now prove the case $n = 2$ of the theorem. We are given quadratic forms $q(v) = a(v)X^2 + a(v)d(v)Y^2$ for all v, and we seek $q = aX^2 + ad_0Y^2$ such that $q \sim q(v)$ over K_v for all v. Thus, we seek an $a \in K^\times$ such that

$$S_v(q) \overset{\text{def}}{=} (a, a)_v (ad_0, d_0)_v = S(q(v))$$

for all v. Now

$$(a, a)_v (ad_0, d_0)_v = (a, -1)_v (a, d_0)_v (-1, d_0)_v = (a, -d_0)_v (-1, d_0)_v.$$

We apply the lemma with T equal to the set of primes for which $S(q(v))(-1, d_0)_v = -1$ and with $b = -d_0$. The set T is finite because of condition (b) of the theorem, and it has an even number of elements because

$$\prod_v S(q(v))(-1, d_0)_v = \prod_v S(q(v)) \cdot \prod_v (-1, d_0)_v = 1 \times 1 = 1.$$

Moreover,

$$S(q(v)) \cdot (-1, d_0)_v = (a(v), -d(v))_v$$

and so $-i_v(d_0) = -d(v) \neq 1$ in $K_v^\times/K_v^{\times 2}$ when $v \in T$. Thus the lemma gives us the required element a.

We next prove the case $n = 3$. For a form $q = q_1 + aZ^2$, $a \in K^\times$,

$$n(q_1) = n(q) - 1, \quad d(q_1) = a \cdot d(q), \quad S_v(q_1) = (a, d(q))_v \cdot S_v(q).$$

We seek an a for which the invariants $(2, a\cdot d_v, (a, d_v)_v \cdot s_v)$ are realizable for all v, i.e., such that $i_v(a)d_v = -1 \Rightarrow (a, d_v)_v \cdot s_v = 1$. Let $T = \{v \mid s_v \neq 1\}$—by hypothesis, it is a finite set. By the weak approximation theorem (ANT, 7.20), there exists an $a \in K^\times$ such that, for all $v \in T$, $i_v(a)d_v \neq -1$. Now, for $v \in T$, $d(q_1) \neq -1$, and so $(2, d_v, s_v)$ is realizable. For $v \notin T$, $(a, d_v) \cdot s_v = (a, d_v)$, and $i_v(a)d_v = -1$ implies $(a, d_v)_v = (-d_v, d_v)_v = 1$. Hence, for such an a, there exists a quadratic form q_1 of rank 2 such that $q_1 + aZ^2$ has the required invariants.

We prove the case $n \geq 4$ by induction. If $t_v < n$ for all n, we can find a quadratic form with shape $q_1(X) + Z^2$ with the correct local invariants. If no $t_v = 0$, then we can find a quadratic form with shape $q_1(X) - Z^2$ with the correct invariants. In the general case, we use the weak approximation theorem (ANT, 7.20) to find an element a that is positive at the real primes, where $t_v < n$ and negative at the real primes, where $t_v = 0$. Then the induction hypothesis allows us to find a $q_1(X)$ such that $q_1(X) + aZ^2$ has the correct invariants.

Applications

PROPOSITION 6.14 (GAUSS) *A positive integer n is a sum of three squares if and only if it is not of the form $4^a(8b - 1)$ with $a, b \in \mathbb{Z}$.*

PROOF. Apply the above theory to the quadratic form $X_1^2 + X_2^2 + X_3^2 - aZ^2$—see Serre 1970, Chap. IV. □

7 Density Theorems

Throughout this section, K is a number field.

THEOREM 7.1 *For any modulus $\mathfrak{m}$ of K and any nontrivial Dirichlet character $\chi : C_\mathfrak{m} \to \mathbb{C}^\times$, $L(1, \chi) \neq 0$.*

PROOF. As we noted at the end of Chapter VI, this follows from the proof of Theorem VI 4.9 once one has the Reciprocity Law. □

THEOREM 7.2 *Let $\mathfrak{m}$ be a modulus for K, and let H be a congruence subgroup for $\mathfrak{m}$: $I^\mathfrak{m} \supset H \supset i(K_{\mathfrak{m},1})$. For any class $\mathfrak{k} \in I^\mathfrak{m}/H$, the set of prime ideals in $\mathfrak{k}$ has Dirichlet density $1/(I^\mathfrak{m} : H)$.*

PROOF. Combine Theorem 7.1 with Theorem VI 4.8. □

COROLLARY 7.3 *Let L/K be a finite abelian extension with Galois group G, and let $\sigma \in G$. Then the set of prime ideals $\mathfrak{p}$ in K that are unramified in L and for which $(\mathfrak{p}, L/K) = \sigma$ has Dirichlet density $\frac{1}{[L:K]}$.*

PROOF. The Reciprocity Law V.3.5 says that the Artin map defines an isomorphism $I^\mathfrak{m}/H \to \mathrm{Gal}(L/K)$ for some modulus $\mathfrak{m}$ and some $H \supset i(K_{\mathfrak{m},1})$, and we can apply the theorem to the inverse image of σ in $I^\mathfrak{m}/H$. □

THEOREM 7.4 (CHEBOTAREV) *Let L be a finite Galois extension of the number field K with Galois group G, and let C be a subset of G stable under conjugation, i.e., such that*

$$x \in C, \quad \tau \in G \Rightarrow \tau x \tau^{-1} \in C.$$

Let

$$T = \{\mathfrak{p} \mid \mathfrak{p} \text{ unramified in } L,\ (\mathfrak{p}, L/K) \subset C\}.$$

Then T has Dirichlet density

$$\delta(T) = \frac{\text{number of elements in } C}{\text{number of elements in } G}.$$

PROOF. It suffices to prove this in the case that C is the conjugacy class of a single element σ,

$$C = \{\tau\sigma\tau^{-1} \mid \tau \in G\}.$$

Let σ have order f, and let $M = L^{<\sigma>}$. Then L is a cyclic extension of M of degree f, and therefore the Artin map gives an isomorphism

$$C_{\mathfrak{m}}/H \to <\sigma>.$$

for some modulus $\mathfrak{m}$ of M and for $H = M^{\times} \cdot \mathrm{Nm}_{L/M} C_{L,\mathfrak{m}}$. We use the notation

$$\mathfrak{P}|\mathfrak{q}|\mathfrak{p}$$

for primes $\mathfrak{P}$ of $\mathcal{O}_L$, $\mathfrak{q}$ of $\mathcal{O}_M$, and $\mathfrak{p}$ of $\mathcal{O}_K$. Let $d = [L\colon K] = (G\colon 1)$, and let c be the order of C. We have to show that

$$\delta(T) = \frac{c}{d}.$$

In the proof, we ignore the (finitely many) prime ideals that are not prime to $\mathfrak{m}$.

Let

$$T_{M,\sigma} = \{\mathfrak{q} \subset \mathcal{O}_M \mid (\mathfrak{q}, L/M) = \sigma, \quad f(\mathfrak{q}/\mathfrak{p}) = 1\}.$$

The Chebotarev density theorem for abelian extensions (7.3 shows that the set of primes satisfying the first condition in the definition of $T_{M,\sigma}$ has density $\frac{1}{f}$, and it follows (see 4.5) that $T_{M,\sigma}$ itself has density $\frac{1}{f}$.

Let

$$T_{L,\sigma} = \{\mathfrak{P} \subset \mathcal{O}_L \mid (\mathfrak{P}, L/K) = \sigma\}.$$

We shall show:

(a) the map $\mathfrak{P} \mapsto \mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$ defines a bijection $T_{L,\sigma} \to T_{M,\sigma}$;

(b) the map $\mathfrak{P} \mapsto \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K : T_{L,\sigma} \to T$ sends exactly $\frac{d}{cf}$ primes of $T_{L,\sigma}$ to each prime of T.

On combining these statements, we find that the map $\mathfrak{q} \mapsto \mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ defines a $\frac{d}{cf} : 1$ map $T_{M,\sigma} \to T$. For such a $\mathfrak{q}$, $\mathrm{Nm}_{M/K}\,\mathfrak{q} = \mathfrak{p}$ and so $\mathbb{N}\mathfrak{q} = \mathbb{N}\mathfrak{p}$; hence

$$\sum_{\mathfrak{p} \in T} \frac{1}{\mathbb{N}\mathfrak{p}^s} = \frac{cf}{d} \sum_{\mathfrak{q} \in T_{M,\sigma}} \frac{1}{\mathbb{N}\mathfrak{q}^s} \sim \frac{cf}{d} \frac{1}{f} \log \frac{1}{s-1} = \frac{c}{d} \log \frac{1}{s-1}$$

as required. It remains to prove (a) and (b).

Let $\mathfrak{P} \in T_{L,\sigma}$, and let $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Then the Galois group of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is generated by σ, but σ fixes $M_{\mathfrak{q}}$, and so $M_{\mathfrak{q}} = K_{\mathfrak{p}}$. Therefore $f(\mathfrak{q}/\mathfrak{p}) = 1$, which shows that $\mathfrak{q} \in T_{M,\sigma}$, and so we have a map

$$\mathfrak{P} \mapsto \mathfrak{q} =_{df} \mathfrak{P} \cap \mathcal{O}_M : T_{L,\sigma} \to T_{M,\sigma}.$$

This is injective because $f(\mathfrak{P}/\mathfrak{q}) = f(\mathfrak{q}/\mathfrak{p})^{-1} f(\mathfrak{P}/\mathfrak{p}) = 1 \times f$, and so $\mathfrak{P}$ is the only prime of L lying over $\mathfrak{q}$. It is surjective because, for any prime $\mathfrak{P}$ lying over $\mathfrak{q} \in T_{M,\sigma}$,

$$(\mathfrak{P}, L/K) = (\mathfrak{P}, L/K)^{f(\mathfrak{q}/\mathfrak{p})} = (\mathfrak{P}, L/M) = \sigma$$

(first condition for $\mathfrak{q}$ to lie in $T_{M,\sigma}$), and so $\mathfrak{P} \in T_{L,\sigma}$. This proves (a).

Fix a $\mathfrak{p}_0 \in T$, and let $\mathfrak{P}_0 \in T_{L,\sigma}$ lie over $\mathfrak{p}$. Then, for $\tau \in G$,

$$(\tau\mathfrak{P}_0, L/K) = \tau(\mathfrak{P}_0, L/K)\tau^{-1}$$

and so

$$\tau(\mathfrak{P}_0, L/K)\tau^{-1} = \sigma \iff \tau \in C_G(\sigma)$$

(centralizer of σ in G). Therefore the map $\tau \mapsto \tau\mathfrak{P}_0$ is a bijection

$$C_G(\sigma)/G(\mathfrak{P}_0) \to \{\mathfrak{P} \in T_{L,\sigma} \mid \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}_0\}$$

The decomposition group $G(\mathfrak{P}_0)$ equals $\langle\sigma\rangle$, which has order f, and $C_G(\sigma)$ has order $\frac{d}{c}$ because there is a bijection

$$\tau \mapsto \tau\sigma\tau^{-1} : G/C_G(\sigma) \to C.$$

Therefore $(C_G(\sigma) : G(\mathfrak{P}_0)) = \frac{d}{cf}$, and we have shown that, for each $\mathfrak{p} \in T$, there are exactly $\frac{d}{cf}$ primes $\mathfrak{P} \in T_{L,\sigma}$ lying over $\mathfrak{p}$. This proves (b) and completes the proof of the theorem. □

REMARK 7.5 For effective forms of the Chebotarev density theorem, see Lagarias and Odlysko (Algebraic Number Fields, Ed. Fröhlich, 1977). Let L be a finite Galois extension of K, and let

$$\pi_C(x) = |\{\mathfrak{p} | (\mathfrak{p}, L/K) = C, \quad \mathbb{N}\mathfrak{p} \le x\}|.$$

Then

$$\pi_C(x) = \frac{c}{d}\frac{x}{\log x} + \text{ specific error term.}$$

8 Function Fields; Geometric Class Field Theory

We should also include the class field theory of function fields (finite extensions of $\mathbb{F}_p(T)$ for some p). For this, one can either mimic proofs in the number field case (see Artin and Tate 1961) or (better) one can base the proofs on Tsen's theorem (see Milne 2006, Appendix to Chapter I).

Let K be a function field in one variable over a field k, i.e., a finite extension of $k(T)$. Geometric class field theory describes the "geometric" abelian extensions of K, i.e., the abelian extensions "not coming from k". For a list of references for geometric class field theory, see mo73054.

9 Cohomology of Number Fields

We should also include proofs of the theorems of Nakayama and Tate (e.g., J. Tate, The cohomology groups of tori in finite Galois extensions of number fields, Nagoya Math. J., 27, 1966, 709–719) and Poitou and Tate (e.g., Milne 2006, Chapter I).

10 More on L-series

Let χ be a Dirichlet L-series. Then there exist constants $A(\chi) \geq 0$, $a(\chi), b(\chi) \in \mathbb{C}$, such that

$$\Phi(s,\chi) =_{df} A(\chi)^s \Gamma(\frac{s}{2})^{a(\chi)} \Gamma(\frac{s+1}{2})^{b(\chi)} L(s,\chi)$$

satisfies the functional equation

$$\Phi(s,\chi) = W(\chi)\Phi(1-s,\bar{\chi}) \qquad |W(\chi)| = 1.$$

See Narkiewicz 1990.

Artin L-series

Let L be a finite Galois extension of K with Galois group G. Let V be a finite dimensional vector space over $\mathbb{C}$ and let

$$\rho\colon G \to \mathrm{Aut}_{\mathbb{C}}(V)$$

be a homomorphism of G into the group of linear automorphisms of V. We refer to ρ as a ***(finite-dimensional) representation of*** G over $\mathbb{C}$. The ***trace*** of ρ is the map

$$\sigma \mapsto \chi(\sigma) = \mathrm{Tr}(\rho(\sigma)).$$

(Recall that the ***trace*** of an $m \times m$ matrix (a_{ij}) is $\sum a_{ii}$, and the trace of an endomorphism is the trace of its matrix relative to any basis.) For $\sigma \in G$, let

$$P_\sigma(T) = \det(1 - \rho(\sigma)T \mid V) = \prod_{i=1}^{\dim V} (1 - a_i T), \qquad a_i \in \mathbb{C},$$

be the characteristic polynomial of $\rho(\sigma)$. Note that $P_\sigma(T)$ depends only on the conjugacy class of σ, and so for any prime $\mathfrak{p}$ of K unramified in L, we can define

$$P_{\mathfrak{p}}(T) = P_\sigma(T), \quad \sigma = (\mathfrak{P}, L/K) \text{ some } \mathfrak{P}|\mathfrak{p}.$$

For such a $\mathfrak{p}$, let

$$L_{\mathfrak{p}}(s,\rho) = \frac{1}{P_{\mathfrak{p}}(\mathbb{N}\mathfrak{p}^{-s})}$$

and let

$$L(s,\rho) = \prod L_{\mathfrak{p}}(s,\rho).$$

For example, if L/K is abelian, then the representation is diagonalizable[6]

$$\rho \approx \chi_1 \oplus \cdots \oplus \chi_m,$$

where each χ_i is a homomorphism $G \to \mathbb{C}^\times$. When composed with the Artin map

$$C_{\mathfrak{m}} \to G,$$

χ_i becomes a Dirichlet character, and so the Artin L-series becomes identified with a product of Dirichlet L-series. This was the original reason Artin defined his map.

One can show that if $(V, \rho) = \mathrm{Ind}_H^G(V_0, \rho_0)$, then

$$L(s, \rho) = L(s, \rho_0).$$

To handle more general Artin L-series, Artin proved that every character of a finite group G is a linear combination (over $\mathbb{Q}$) of induced characters from cyclic subgroups. Hence

$$L(s, \rho) = \prod (\text{ Dirichlet } L \text{ -series})^{r_i}, \quad r_i \in \mathbb{Q}.$$

Later Brauer proved a stronger theorem that allows one to show that

$$L(s, \rho) = \prod (\text{ Dirichlet } L \text{ -series})^{r_i}, \quad r_i \in \mathbb{Z}.$$

Artin conjectured that, provided ρ does not contain the trivial representation, $L(s, \rho)$ extends to a *holomorphic* function on the whole complex plane. The last formula implies that this is true if the r_i are all positive integers. Little progress was made in this conjecture until Langlands succeeded in proving it in many cases, where V has dimension 2 (see R. Langlands, Base Change for GL(2), Princeton, 1980).

Hecke L-series

A ***Hecke (or Grössen) character*** is a continuous homomorphism from $\mathbb{I}$ into the unit circle in $\mathbb{C}^\times$ such that $\psi(K^\times) = 1$ and, for some finite set S, ψ is 1 on a set $\{(a_v) \mid a_v = 1$ for $v \in S, a_v =$unit for all $v\}$

EXAMPLE 10.1 Let $D \in \mathbb{Z}$, cube-free, and let ζ be primitive cube root of 1. If $p \equiv 2 \mod 3$, then p remains prime in $\mathbb{Q}[\zeta]$, and we set $\psi(p) = 1$. If $p \equiv 1 \mod 3$, then $p = \pi\bar{\pi}$ in $\mathbb{Q}[\zeta]$, and we choose π to be $\equiv 1 \mod 3$. Then $\pi = \frac{1}{2}(a + 3b\sqrt{-3})$ and $4p = 4\pi\bar{\pi} = a^2 + 27b^2$. Now there exists a Hecke character such that $\psi(p) = 1$ for all odd $p \not\equiv 1 \mod 3$ and $\psi(p) = \frac{\pi}{\sqrt{p}}\left(\frac{D}{\pi}\right)$.

For such a character, we define

$$L(s, \psi) = \prod_{v \notin S} \frac{1}{1 - \psi(\pi_v)\mathbb{N}\mathfrak{p}_v^{-s}},$$

[6]By this we mean that, relative to suitable basis for V,

$$\rho(g) = \begin{pmatrix} \chi_1(g) & 0 & \cdots & 0 \\ 0 & \chi_2(g) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \chi_m(g) \end{pmatrix}, \quad g \in G.$$

where π_v is an idèle having a prime element in the v position and 1 elsewhere. The basic analytic properties of Hecke L-series (meromorphic continuation, functional equation etc.) are well understood (e.g., J. Tate, Fourier analysis in number fields and Hecke's zeta function, thesis, 1950; reprinted in Cassels and Fröhlich 1967; or Ramakrishnan and Valenza 1999).

Weil groups and Artin-Hecke L-series

For this topic, see Tate 1979

A theorem of Gauss

Having begun the course with theorem first proved by Gauss, namely, the quadratic reciprocity law, it seems appropriate to end it with another theorem of his.

Consider the elliptic curve $E : X^3 + Y^3 + Z^3 = 0$. Let N_p be the number of points on E with coordinates in $\mathbb{F}_p$. Gauss showed:

(a) if $p \not\equiv 1 \mod 3$, then $N_p = p + 1$;

(b) if $p \equiv 1 \mod 3$, then $N_p = A$, where A is the unique integer $\equiv 1 \mod 3$ for which $4p = A^2 + 27B^2$.

See Silverman and Tate 1992, IV.2.

Gauss's theorem implies that the Weil conjecture holds for $E/\mathbb{F}_p$, namely, that

$$|N_p - p - 1| < 2\sqrt{p}.$$

It also implies the Taniyama conjecture for $E/\mathbb{Q}$, because it shows that the L-series $L(s, E)$ equals $L(s - \frac{1}{2}, \psi)$, where ψ is the Hecke character in the above example associated with $D = -1$.

He wrote to me that algebraic number theory was the most beautiful topic he had ever come across and that the sole consolation in his misery was his lecturing on class field theory.... This was indeed the kind of mathematics he had admired most: the main results are of great scope, of great aesthetic beauty, but the proofs are technically extremely hard.

A. Borel, in: Current Trends in Mathematics and Physics: A Tribute to Harish-Chandra, Editor S.D. Adhikari, Narosa Publishing House, New Dehli, Madras, 1995, p. 213.

Appendix A

Exercises

These were the exercises the students were required to hand in.

A-1 (a) Let K be a finite Galois extension of $\mathbb{Q}$. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is generated by the inertia groups of the prime ideals in $\mathcal{O}_K$. (Hint: show that the fixed field of the subgroup generated by the inertia groups is unramified over $\mathbb{Q}$ at all prime ideals of $\mathbb{Z}$. The inertia group of a prime ideal $\mathfrak{P}$ is the subgroup of the decomposition group $D(\mathfrak{P})$ of elements fixing the residue field. Its order is the ramification index of $\mathfrak{P}$.)

(b) Let $p_1, \dots, p_t$ be distinct odd prime numbers, and let $p_i^* = (-1)^{\frac{p_i-1}{2}} p_i$ (so only p_i ramifies in $\mathbb{Q}[\sqrt{p_i^*}]$). Let $K = \mathbb{Q}[\sqrt{d}]$, $d = \prod p_i^*$.

Let C_+ be the narrow-class group of K, and let L be the class field of C_+^2 (so L is unramified over K at all prime ideals of $\mathcal{O}_K$ and $\mathrm{Gal}(L/K)$ is an elementary abelian 2-group; moreover, L is the largest field for which these statements are true).

Show that L is Galois over $\mathbb{Q}$ and that the inertia group in $\mathrm{Gal}(L/\mathbb{Q})$ of every prime ideal of $\mathcal{O}_L$ is of order 1 or 2. Deduce that $\mathrm{Gal}(L/\mathbb{Q})$ is an elementary abelian 2-group, and that $L = \mathbb{Q}[\sqrt{p_1^*}, \dots, \sqrt{p_t^*}]$. Deduce that $(C_+ : C_+^2) = 2^{t-1}$ (cf. Example 0.7).

A-2 (a) Let $d > 3$ be a square-free integer with $d \equiv 3 \bmod 8$. Show that there exists a field L of degree 3 over $\mathbb{Q}$ with discriminant $-d$ or $-4d$.

(b) Find the cubic extension L of $\mathbb{Q}$ with smallest $|\Delta_{L/K}|$.

(You may assume the main statements of class field theory.)

Hints: Let $K = \mathbb{Q}[\sqrt{-d}]$. For the case that 3 divides the class number of K, ponder the example of the Hilbert class field of $\mathbb{Q}[\sqrt{-31}]$ worked out in class. For the contrary case, show that $2\mathcal{O}_K$ is a prime ideal $\mathfrak{p}$ and that 3 divides the order of the ray class group $C_{\mathfrak{p}}$.

A-3 Do Exercise 3.15, p. 160, in the notes. Note that, in the statement of the Exercise, i is used ambiguously for the (obvious) homomorphisms from $K_{\mathfrak{m},1}$ to $I^{S(\mathfrak{m})}$ and to $I^{S\cup S(\mathfrak{m})}$.

A-4 Prove, or disprove, that every subgroup of finite index in the idèle class group $\mathbf{C}_K = \mathbb{I}_K/K^\times$ of a number field K is open. (This is Exercise 5.11, p. 182, of the notes. You may assume the similar statement for $K_v^\times$ — see I 1.7 of the notes.)

A-5 Let G be a group and A a group (not necessarily commutative) endowed with an action of G, i.e., a homomorphism $G \to \mathrm{Aut}(A)$. As in the commutative case, a crossed homomorphism $\varphi : G \to A$ is defined by the condition $\varphi(\sigma\tau) = \varphi(\sigma) \cdot \sigma\varphi(\tau)$. Two

such homomorphism φ and φ' are said to be equivalent if there exists an $a \in A$ such that $\varphi'(\sigma) = a^{-1} \cdot \varphi(\sigma) \cdot \sigma a$ for all $\sigma \in G$, and the set of equivalence classes is denoted $H^1(G, A)$ (it is a set with a distinguished element). A proof similar to that of Hilbert's Theorem 90 shows that $H^1(G, \mathrm{GL}_n(L)) = 0$ when L/K is a finite Galois extension with Galois group G.

Let K be a field of characteristic $\neq 2$. A ***quadratic space*** over K is a pair (V, Φ) consisting of a finite-dimensional vector space V over K and a nondegenerate quadratic form Φ on V, i.e., the map $x \mapsto \varphi(x, x)$ associated with a nondegenerate symmetric bilinear form φ on V. An ***isometry*** $\alpha : (V, \Phi) \to (V', \Phi')$ is an isomorphism of vector spaces $\alpha : V \to V'$ such that $\Phi'(\alpha(v)) = \Phi(v)$ for all $v \in V$.

Exercise: Let L/K be a finite Galois extension of fields of characteristic $\neq 2$, and let $G = \mathrm{Gal}(L/K)$. Fix a quadratic space (V, Φ) over K, and let $O(\Phi)$ be the group of automorphisms of $(V, \Phi) \otimes_K L$ — it has an obvious G-action. If (V', Φ') is a quadratic space over K and $\alpha : (V, \Phi) \otimes_K L \to (V', \Phi') \otimes_K L$ is an isomorphism of quadratic spaces over L, show that $\sigma \mapsto \alpha^{-1} \circ \sigma\alpha$ is a crossed homomorphism $\varphi : G \to O(\Phi)$ whose equivalence class is independent of the choice of α. Deduce that $H^1(G, O(\Phi))$ classifies the set of isomorphism classes of quadratic spaces over K that become isomorphic to (V, Φ) over L (i.e., there is a one-to-one correspondence between $H^1(G, O(\Phi))$ and the set). Deduce that $H^1(G, O(\Phi)) \neq 0$ when $K = \mathbb{R}$ and $L = \mathbb{C}$ (assuming $\dim V \neq 0$). (You may assume that $H^1(G, \mathrm{GL}_n(L)) = 0$.)

A-6 Let H be a subgroup of finite index in the group G, and choose a map $s : H\backslash G \to G$ such that $Hs(x) = x$, i.e., a representative in G for each right coset of H in G — thus $G = \bigcup_{x \in H\backslash G} Hs(x)$.

(a) For $g \in G$, show that $s(x) \cdot g \cdot s(xg)^{-1} \in H$.

For $g \in G$, define

$$V(g) = \prod_{x \in H\backslash G} s(x) \cdot g \cdot s(xg)^{-1} \mod H^c,$$

where H^c is the commutator subgroup of H. (Note that, because H/H^c is commutative, $V(g)$ is independent of the choice of the ordering of $H\backslash G$ implicit in the product).

(b) Show that $V(g)$ is independent of the choice of s, and that it is a homomorphism $G \to H/H^c$.

Hence, V induces a homomorphism $\mathrm{Ver}: G/G^c \to H/H^c$ — the Verlagerung or transfer map.

(c) For any G-module M, show that the map $m \mapsto \mathcal{N}(m) = \sum_{x \in H\backslash G} s(x) \cdot m$ induces a well-defined homomorphism $\mathrm{Res}: H_0(G, M) \to H_0(H, M)$.

(d) Show that the diagram

$$\begin{array}{ccc} G/G^c & \xrightarrow{\simeq} & I_G/I_G^2 \\ \downarrow{\scriptstyle \mathrm{Ver}} & & \downarrow{\scriptstyle \mathcal{N}} \\ H/H^c & & I_G/I_H I_G \\ \| & & \uparrow \\ H/H^c & \xrightarrow{\simeq} & I_H/I_H^2 \end{array}$$

commutes (the horizontal isomorphisms are those of Lemma II, 2.6; the upward map is induced by inclusion).

[Assuming that the maps $Res : H_r(G, M) \to H_r(H, M)$ exist, are compatible with the boundary maps, and have the description in (c) for $r = 0$, this shows that they agree with the Verlagerung on $H_1(G, \mathbb{Z})$. More precisely, the above diagram can be identified with

$$\begin{array}{ccc} H_1(G,\mathbb{Z}) & \xrightarrow{\delta} & H_0(G, I_G) \\ \downarrow \text{Res} & & \downarrow \text{Res} \\ H_1(H,\mathbb{Z}) & \xrightarrow{\delta} & H_0(H, I_G) \\ \text{id}\uparrow & & \uparrow \\ H_1(H,\mathbb{Z}) & \xrightarrow{\delta} & H_0(H, I_H). \end{array}$$

The boundary maps arise from the augmentation exact sequences for G and H. The top and bottom boundary maps are isomorphisms. The middle boundary map is injective, and becomes an isomorphism in the case that G is finite when $H_0(H, I_G)$ is replaced by $H_T^{-1}(H, I_G)$.]

A-7 This exercise will show that cohomology doesn't commute with inverse limits — in fact, the map $H^1(G, \varprojlim M_n) \to \varprojlim H^1(G, M_n)$ needn't be injective.

Let G be a profinite group, and let

$$\cdots \longrightarrow M_n \xrightarrow{\pi_{n-1,n}} M_{n-1} \longrightarrow \cdots \longrightarrow M_1$$

be a projective system of G-modules. Assume

(a) each map $\pi_{n-1,n} : M_n \to M_{n-1}$ is surjective;

(b) there is a commutative diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & M_n^G & \xrightarrow{\pi_{n-1,n}} & M_{n-1}^G & \longrightarrow & \cdots \\ & & \downarrow \gamma_n & & \downarrow \gamma_{n-1} & & \\ \cdots & \longrightarrow & \mathbb{Z} & \xrightarrow{p} & \mathbb{Z} & \longrightarrow & \cdots \end{array}$$

in which each vertical map is surjective.

For any $c_n \in \mathbb{Z}$, $\sum p^{n-1} c_n$ will converge in $\mathbb{Z}_p$ — choose a sequence c_n, $n \geq 1$, such that $\sum p^{n-1} c_n$ converges to an element c of $\mathbb{Z}_p$ not in $\mathbb{Z}$. For each n, choose elements $x_{n,1}, \ldots, x_{n,n}$ such that

(a) for $1 \leq i \leq n-1$, $\pi_{n-1,n}(x_{n,i}) = x_{n-1,i}$;

(b) $x_{n,n} \in M_n^G$ and $\gamma_n(x_{n,n}) = c_n$.

Define

$$\begin{aligned} x_n &= x_{n,1} + \cdots + x_{n,n} \\ \varphi_n(\sigma) &= \sigma x_n - x_n, \quad \text{for } \sigma \in G. \end{aligned}$$

Thus, φ_n is a principal crossed homomorphism $G \to M_n$. Note that $\pi_{n-1,n}(\varphi_n(\sigma)) = \varphi_{n-1}(\sigma)$ for all n, and so there is an element $\varphi(\sigma)$ in $M \overset{\text{def}}{=} \varprojlim M_n$ whose image in each M_n is $\varphi_n(\sigma)$. Clearly, $\sigma \mapsto \varphi(\sigma)$ is a crossed homomorphism $G \to M$.

Show that φ is not a *principal* crossed homomorphism, i.e., show that there doesn't exist an element $y = (y_n)$ of M such that $\varphi_n(\sigma) = \sigma y_n - y_n$.

Hint: write $y_n = x_n + z_n$ and show that z_1 is fixed by G but $\gamma(z_1) = c \notin \mathbb{Z}$.

Can you construct a system $(M_n, \pi_{n-1,n}, \gamma_n)$ satisfying the conditions?

A-8 Do parts (a)–(d) of Exercise 5.7, p. 144, of the notes (or the whole exercise, if you are feeling energetic). You may use the noncohomological results of Chapter IV, if necessary.

A-9 Let $L_n = \mathbb{Q}_p[\zeta_{p^n}]$, where ζ_{p^n} is a primitive p^nth root of 1. Show that p is a norm from L_n. Deduce that $L_\infty = \bigcup L_n$ is the subfield of $\mathbb{Q}^{\mathrm{ab}}$ fixed by $\mathrm{rec}_{\mathbb{Q}_p}(p)$ (union inside some fixed algebraic closure of $\mathbb{Q}_p$).

A-10 Let L/K be a finite cyclic extension of number fields of degree n. Show that, for each $d|n$, the set of primes $\mathfrak{p}$ of K such that $e(\mathfrak{P}/\mathfrak{p}) = 1$ and $f(\mathfrak{P}/\mathfrak{p}) = d$ for one (hence all) $\mathfrak{P}$ lying over $\mathfrak{p}$ has polar density $\varphi(d)/n$. (Hint: Try induction on d.)

The energetic may find a similarly elementary proof of the Frobenius density theorem (weaker, much earlier form, of the Chebotarev density theorem): Let L/K be a Galois extension with Galois group G, and let σ be an element of G of order n. Show that

$$\{\mathfrak{p} \mid \mathfrak{p} \text{ unramified and } (\mathfrak{p}, L/K) = \sigma^k \text{ for some } k \text{ relatively prime to } n\}$$

has polar density $c\varphi(n)/[L : K]$, where c is the number of conjugates of $\langle\sigma\rangle$ in G. Show also, that $c\varphi(n)$ is the number of conjugates of σ, and so this is consistent with the Chebotarev density theorem. For hints, see Marcus 1977, pp. 207–208.

A-11 Show that 16 is an 8th power in $\mathbb{R}$ and $\mathbb{Q}_p$ for all odd p (but not in $\mathbb{Q}$).

[Hint: Show that $\mathbb{Q}[\zeta_8] = \mathbb{Q}[i, \sqrt{2}]$ is unramified for all odd p, and deduce that, for p odd, $\mathbb{Q}_p$ contains at least one of $1 + i$, $\sqrt{2}$, or $\sqrt{-2}$.]

Note: This violates Grunwald's theorem, which was widely used for 15 years.

Appendix B

Solutions to Exercises

Solution to Exercise A-1.

(a) Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and let $I(\mathfrak{p})$ be its inertia group. Then $M = K^{I(\mathfrak{p})}$ has the property that $\mathfrak{p} \cap \mathcal{O}_M$ is unramified over $\mathfrak{p} \cap \mathbb{Z}$ (ANT, 8.11). Hence any field fixed by all the inertia groups is unramified over $\mathbb{Q}$, and so equals $\mathbb{Q}$ (ANT, 4.9).

(b) The field L is Galois over $\mathbb{Q}$ because it is stable under any automorphism of its Galois closure.

It's clear the inertia groups have order 1 or 2, and so $\mathrm{Gal}(L/\mathbb{Q})$ is generated by elements of order 2. This *doesn't* imply it is abelian (every dihedral group is generated by two elements of order 2), but there is an extension

$$0 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 0,$$

$$\mathrm{Gal}(L/K) \approx (\mathbb{Z}/2\mathbb{Z})^s \text{ some } s, \quad \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

and the generators of the nontrivial inertia groups have image $\neq 1$ in $\mathrm{Gal}(K/\mathbb{Q})$ (otherwise the argument in (a) would show that the ramification occurred in L/K rather than $K/\mathbb{Q}$). Let σ and τ generate inertia groups of order 2. Then $\sigma|K \neq 1$ and $\tau|K \neq 1$, and so $\sigma\tau|K = 1$. Thus $\sigma\tau \in \mathrm{Gal}(L/K)$ and so has order 1 or 2. Hence σ and τ commute, and so $\mathrm{Gal}(L/\mathbb{Q})$ is generated by *commuting* elements of order 2, which implies that it is an elementary abelian 2-group.

Only the primes $p_1, \dots, p_t$ ramify in L, and corresponding to each there is only one inertia group (there may be many prime ideals in L lying over a p_i, but each has the same inertia group because $\mathrm{Gal}(L/\mathbb{Q})$ is abelian). Hence $\mathrm{Gal}(L/\mathbb{Q}) \approx (\mathbb{Z}/2\mathbb{Z})^s$ some $s \leq t$. Since L contains $\mathbb{Q}[\sqrt{p_1^*}, \dots]$, which has degree 2^t over $\mathbb{Q}$, we see that $L = \mathbb{Q}[\sqrt{p_1^*}, \dots]$. The rest is easy.

[Alternative proof that $L = \mathbb{Q}[\sqrt{p_1^*}, \dots]$: Because $\mathrm{Gal}(L/\mathbb{Q})$ is an elementary abelian 2-group, $L = \mathbb{Q}[\sqrt{m_1}, \sqrt{m_2}, \dots]$ for some $m_i \in \mathbb{Z}$ (easy Kummer theory), but it's easy to see that $\mathbb{Q}[\sqrt{p_1^*}, \dots]$ is the largest field of this type whose composite with K is unramified over K.]

Solution to Exercise A-2.

As $d \equiv 3 \mod 8$, $-d \equiv 1 \mod 4$, and so $\Delta_{K/\mathbb{Q}} = -d$. I write "prime" to mean "finite prime".

If 3 divides the class number of K, then there exists an unramified extension L of K of degree 3 (by class field theory). As in the case $d = 31$, L is Galois over $\mathbb{Q}$ and $L = M \cdot K$ with M of degree 3 over $\mathbb{Q}$ and non Galois over $\mathbb{Q}$. By Galois theory, the

unique quadratic extension of $\mathbb{Q}$ contained in the Galois closure of M is $\mathbb{Q}[\sqrt{\Delta_{M/\mathbb{Q}}}]$, and so $\Delta_{M/\mathbb{Q}} = -d \times \text{square}$ (easy Kummer theory). If p doesn't divide d, it doesn't ramify in L (nor in M) and so p doesn't divide $\Delta_{M/K}$. If $p|d$, then $p\mathcal{O}_M = \mathfrak{p}_1^2\mathfrak{p}_2$, which implies (theory of differents) that p divides $\Delta_{M/K}$ but not p^2. Hence $\Delta_{M/\mathbb{Q}} = -d$.

Suppose 3 doesn't divide the class number. Because $-d \equiv 5 \mod 8$, (2) stays prime[1] in $\mathcal{O}_K$, say $2\mathcal{O}_K = \mathfrak{p}$, and 3 divides the order of the ray class group $C_{\mathfrak{p}}$ (the ray class group contains $(\mathcal{O}_K/\mathfrak{p})^\times = \mathbb{F}_4^\times$ — see V 1.5; here we use that $d > 3$ to see that the only units in K are ± 1). We apply the same argument as before with L an extension of K of degree 3 ramified only at $\mathfrak{p}$. Again $L = M \cdot K$ with M as before except that 2 totally ramifies in M, and the argument shows that $\Delta_{M/\mathbb{Q}} = -4d$.

From the table on p. 160 of the notes, we see that $\Delta_{M/\mathbb{Q}} = -23$ is possible. From the Minkowski bound, we see that $|\Delta_{M/\mathbb{Q}}| \geq 13$ (complex primes) or $|\Delta_{M/\mathbb{Q}}| \geq 21$ (no complex prime). Stickelberger eliminates all but $-15, -16, -19, -20, 21$. If M has discriminant $d = -15, -19, 21$, its Galois closure $L = M \cdot \mathbb{Q}[\sqrt{d}]$ is unramified over $\mathbb{Q}[\sqrt{d}]$ (otherwise some prime of $\mathbb{Q}$ ramifies totally in L but not in M), but the class numbers of $\mathbb{Q}[\sqrt{d}]$ are 2, 1, and 1 respectively. For $d = -16, -20$, the same argument shows that only primes lying over 2 could ramify in $L = M \cdot \mathbb{Q}[\sqrt{d}]$, but here the class number is 1 or 2 and the relevant ray class numbers are not divisible by 3 (2 ramifies in $\mathbb{Q}[\sqrt{-1}]$ and $\mathbb{Q}[\sqrt{-5}]$).

Note:

(a) Instead of using differents, one can use the formula in 3.39(a) of ANT (but the proof of that uses differents).

(b) It is not too hard to compute the above class numbers by hand, but the easy way is to use PARI.

Solution to Exercise A-3.

In the notes (and this solution), i is used ambiguously for the (obvious) homomorphisms from $K_{\mathfrak{m},1}$ to $I^{S(\mathfrak{m})}$ and to $I^{S\cup S(\mathfrak{m})}$. These maps make the diagram

$$\begin{array}{ccccc} & & K_{\mathfrak{m},1} & & \\ & & \downarrow & \searrow & \\ \mathbb{Z}S & \longrightarrow & I^{S(\mathfrak{m})} & \longrightarrow & I^{S\cup S(\mathfrak{m})} \end{array}$$

commute — here $\mathbb{Z}S$ is the free abelian group generated by S. The kernel-cokernel exact sequence of the triangle gives

$$\mathbb{Z}S \to I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \to I^{S\cup S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \to 0,$$

and so

$$I^{S(\mathfrak{m})}/\langle S\rangle \cdot i(K_{\mathfrak{m},1}) \simeq I^{S\cup S(\mathfrak{m})}/i(K_{\mathfrak{m},1}).$$

Thus, the subgroups of $I^{S\cup S(\mathfrak{m})}$ containing $i(K_{\mathfrak{m},1})$ are in natural one-to-one correspondence $H \leftrightarrow H'$ with the subgroups of $I^{S(\mathfrak{m})}$ containing $\langle S\rangle \cdot i(K_{\mathfrak{m},1})$. For such a pair H, H', let L be the class field of H'. We get isomorphisms

$$I^{S\cup S(\mathfrak{m})}/H \to I^{S(\mathfrak{m})}/H' \to \mathrm{Gal}(L/K).$$

[1] If $-d \equiv 1 \mod 8$, it would split.

The second map is the Artin map, induced by $\mathfrak{p} \mapsto (\mathfrak{p}, L/K)$. Certainly L/K is abelian, and the primes in S split because they lie in H' (and hence have $(\mathfrak{p}, L/K) = 1$). Moreover, primes not in $S(\mathfrak{m})$ don't ramify. Finally, the composite of the two maps is also the Artin map, and so the primes not in $S \cup S(\mathfrak{m})$ that split are precisely those in H. This shows that L/K is an S-class field of H. We have shown that it has Galois group $I^{S\cup S(\mathfrak{m})}/H$, and it is unique because we know which primes split in it (except possibly for a finite number).

Conversely, any L satisfying (a) is the class field for some modulus $\mathfrak{m}$ such that $S(\mathfrak{m}) \cap S = \emptyset$ and some subgroup H' of $I^{S(\mathfrak{m})}$ containing $\langle S\rangle \cdot i(K_{\mathfrak{m},1})$, from which it follows that it is the S-class group of the subgroup H of $I^{S\cup S(\mathfrak{m})}$ corresponding to H'.

Solution to Exercise A-4.

Alas, it is not true that every subgroup of finite index in the idèle class group is open, even for a number field. As in I 1.5, let V be a product of a countably infinite number of copies of $\mathbb{F}_p$ (or any other finite field), and let $W \subset V$ consist of the elements of V all but a finite number of whose entries are zero (so W is a direct ***sum*** of copies of $\mathbb{F}_p$). With the product topology, V is compact (and uncountable). The subspace W is countable, but dense in V — in fact, it maps onto any finite quotient of V. The quotient V/W is a vector space over $\mathbb{F}_p$, and so has a basis B (this requires the axiom of choice — see Jacobson, Lectures in Abstract Algebra, Vol II, Chap. IX; to say that B is a basis means that every finite subset of B is linearly independent and every element of V/W is a finite linear combination of elements in B). Let S be a nonempty finite subset of B, and let W' be the inverse image in V of the span of $B \smallsetminus S$. Then $V \supset W' \supset W$, and W' is a proper subgroup of finite index in V whose closure is V. It can't be open because otherwise it would be closed.

Recall (notes 5.9) that $\mathbf{C}_{\mathbb{Q}} \simeq \mathbb{R}_{>0} \times \prod \mathbb{Z}_p^{\times}$ (topological isomorphism). Each $\mathbb{Z}_p^{\times}$ has an open subgroup of index 2. On taking the product of the corresponding quotient maps, we get a continuous homomorphism $\prod_p \mathbb{Z}_p^{\times} \to V$, where V is a product of copies of $\mathbb{F}_2$ indexed by the prime numbers. Let W' be a nonclosed (hence nonopen) subgroup of finite index in V. Its inverse image in $\prod \mathbb{Z}_p^{\times}$ is again nonclosed and of finite index, as is its inverse image in $\mathbf{C}_{\mathbb{Q}}$.

A similar argument shows that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ has nonopen subgroups of finite index — consider its quotient group $\mathrm{Gal}(K/\mathbb{Q})$, where $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots]$ (FT 7.26).

Note that in every case we have used the axiom of choice to construct the nonopen subgroup of finite index. Is it possible to avoid the axiom of choice and find explicit examples?

Solution to Exercise A-5.

For a map α between objects on which G acts on the left, $\sigma\alpha \overset{\text{def}}{=} \sigma \circ \alpha \circ \sigma^{-1}$ (this is standard). Clearly, $\sigma(\alpha \circ \beta) = \sigma\alpha \circ \sigma\beta$.

Let V be a vector space over K. If a linear map $\alpha : V \otimes L \to V \otimes L$ has matrix (a_{ij}) relative to some basis of V, then $\sigma\alpha$ has basis (σa_{ij}). Therefore, α is "defined over K", i.e., of the form $\alpha_0 \otimes 1$, if and only if $\sigma\alpha = \alpha$ for all $\sigma \in G$. A similar remark applies to quadratic forms.

In $O(\Phi)$, $\cdot$ is defined to be $\circ$.

Now let $\alpha : (V, \Phi) \otimes L \to (V', \Phi') \otimes L$ be an isomorphism of quadratic spaces, as in the exercise. Let $\varphi(\sigma) = \alpha^{-1} \circ \sigma\alpha$. Then

$$\varphi(\sigma) \cdot \sigma\varphi(\tau) = \alpha^{-1} \circ \sigma\alpha \circ \sigma(\alpha^{-1} \circ \tau\alpha) = \alpha^{-1} \circ \sigma\alpha \circ \sigma\alpha^{-1} \circ \sigma\tau\alpha = \varphi(\sigma\tau).$$

Thus φ is a crossed homomorphism. Any other isomorphism $\alpha' : (V, \Phi) \otimes L \to (V', \Phi') \otimes L$ differs from α by an automorphism of $(V, \Phi) \otimes L$: $\alpha' = \alpha \circ \beta$, $\beta \in O(\Phi)$. The crossed

homomorphism defined by α' is φ' with

$$\varphi'(\sigma) = \beta^{-1} \circ \alpha^{-1} \circ \sigma(\alpha \circ \beta) = \beta^{-1} \circ \varphi(\sigma) \circ \sigma\beta,$$

which shows that φ' is equivalent to φ.

Thus every (V', Φ') defines an element $\gamma(V', \Phi') \in H^1(G, O(\Phi))$, and it is straightforward to verify that if $(V', \Phi') \approx (V'', \Phi'')$ then $\gamma(V', \Phi') = \gamma(V'', \Phi'')$. Conversely, if $\gamma(V', \Phi') = \gamma(V'', \Phi'')$, then it is possible to choose the isomorphisms $\alpha : (V, \Phi) \otimes L \to (V', \Phi') \otimes L$ and $\beta : (V, \Phi) \otimes L \to (V'', \Phi'') \otimes L$ so that they give the same crossed homomorphism — hence $\alpha^{-1} \circ \sigma\alpha = \beta^{-1} \circ \sigma\beta$ for all $\sigma \in G$. Now $\beta \circ \alpha^{-1} : (V', \Phi') \to (V'', \Phi'')$ is an isomorphism such that $\sigma(\beta \circ \alpha^{-1}) = \beta \circ \alpha^{-1}$ for all σ, and so is defined over K.

It remains to show that every element of $H^1(G, O(\Phi))$ arises from a (V', Φ'). Let φ be a crossed homomorphism $G \to O(\Phi)$. Because $H^1(G, GL_n) = 0$, $\varphi(\sigma) = \alpha^{-1} \circ \sigma\alpha$ for some automorphism α of $V \otimes L$. Let Φ' be the quadratic form on $V \otimes L$ such that $\Phi' \circ \alpha = \Phi$. I claim that Φ' is defined over K: in fact,

$$\sigma\Phi' = \sigma(\Phi \circ \alpha^{-1}) = \Phi \circ \sigma\alpha^{-1} = \Phi \circ \varphi(\sigma)^{-1} \circ \alpha^{-1} = \Phi \circ \alpha^{-1} = \Phi'.$$

The quadratic form Φ' was chosen so that α is an isomorphism $(V, \Phi) \to (V, \Phi')$, and it follows that $\gamma(V, \Phi')$ is represented by φ.

For the final statement, note that the quadratic space $(\mathbb{R}^2, x^2 + y^2)$ is not isomorphic to the quadratic space $(\mathbb{R}^2, x^2 - y^2)$ (the former takes only values > 0), but becomes isomorphic to it over $\mathbb{C}$.

Solution to Exercise A-6.

(a) By definition, $x = H \cdot s(x)$ and $xg = H \cdot s(xg)$. On multiplying the first equality by g, we find that $xg = H \cdot s(x)g$. Hence $H \cdot s(x)g = H \cdot s(xg)$, and so $s(x) \cdot g \cdot s(xg)^{-1} \in H$.

(b) Let $(s'(x))$ be a second family of right coset representatives, say, $s'(x) = h(x)s(x)$. Then

$$\begin{aligned}\prod_x s'(x) \cdot g \cdot s'(xg)^{-1} &= \prod_x h(x) \cdot s(x) \cdot g \cdot s(xg)^{-1} \cdot h(xg)^{-1} \\ &\equiv \prod_x s(x) \cdot g \cdot s(xg)^{-1} \prod_x h(x) \left(\prod_x h(xg) \right)^{-1} \mod H^c.\end{aligned}$$

As x runs through the right cosets of H in G, so also does xg, and so $\prod_x h(x) = \prod_x h(xg)$.

For $g, g' \in G$,

$$\begin{aligned}\prod_x s(x) \cdot gg' \cdot s(xgg')^{-1} &\equiv \prod_x s(x) \cdot g \cdot s(xg)^{-1} \cdot \prod_x s(xg) \cdot g' \cdot s(xgg')^{-1} \mod H^c \\ &= \prod_x s(x) \cdot g \cdot s(xg)^{-1} \cdot \prod_x s(x) \cdot g' \cdot s(xg')^{-1}\end{aligned}$$

— we again used that, as x runs through the right cosets of H, so also does xg. Read mod H^c, this equation becomes

$$V(gg') = V(g) \cdot V(g').$$

(c) Let $(s'(x))_x$ be a second family of right coset representatives, say, $s'(x) = h(x)s(x)$. For $m \in M$,

$$\sum_x s'(x)\cdot m = \sum_x s(x)\cdot m + \sum_x (h(x)-1)\cdot s(x)\cdot m \equiv \sum_x s(x)\cdot m \mod I_H M.$$

Thus,

$$m \mapsto \sum s(x)\cdot m : M \to M/I_H M \qquad (*)$$

is independent of the choice of s.

If $(s(x))_x$ is a family of right coset representatives, then so also is $x \mapsto s(xg^{-1})g$ for any fixed $g \in G$, and so

$$\sum_x s(x)\cdot m \equiv \sum_x s(x)gm \mod I_H M.$$

Hence $\sum_x s(x)\cdot(g-1)m \equiv 0 \mod I_H M$, which shows that the map $(*)$ factors through $M/I_G M$.

It is obviously a homomorphism of abelian groups.

(d) As Serre (1962, p. 129) says: "Il n'y a plus maintenant qu'à calculer".

Let $g \in G$. Its image in $I_G/I_H I_G$ the short way is

$$\sum_x s(x)(g-1) \mod I_H I_G,$$

and its image the long way is

$$\sum_x (s(x)\cdot g\cdot s(xg)^{-1} - 1) \mod I_H I_G$$

For each x, there exists an $h_x \in H$ such that

$$s(x)\cdot g = h_x \cdot s(xg)$$

(see the first paragraph of the solution). Now,

$$\begin{aligned}\sum_x s(x)(g-1) &= \sum_x h_x\cdot s(xg) - \sum_x s(xg)\\ &= \sum_x (h_x-1)s(xg)\\ &\equiv \sum_x (h_x-1) \mod I_H I_G\\ &= \sum_x (s(x)\cdot g\cdot s(xg)^{-1}-1).\end{aligned}$$

Alternatively, note that[2]

$$\sum_x s(x)(g-1) = \sum_x s(xg)(g-1),$$

[2]Better (Darij Grinberg), note that

$$\textstyle\sum_x s(x)(g-1) = \sum_x s(x)g - \sum_x s(x) = \sum_x s(x)g - \sum_x s(xg),$$

and that

$$s(x)\cdot g\cdot s(xg)^{-1} - 1 - s(x)\cdot g + s(xg) = \left(s(x)\cdot g\cdot s(xg)^{-1} - 1\right)(1 - s(xg)).$$

and that

$$s(x)\cdot g\cdot s(xg)^{-1}-1-s(xg)g+s(xg)=(s(x)\cdot g\cdot s(xg)^{-1}-1)(1-s(xg)),$$

which visibly lies in $I_H\cdot I_G$.

Solution to Exercise A-7.

Suppose there exists such a $y=(y_n)$. Following the hint, we write $y_n=x_n+z_n$. Since $\sigma y_n-y_n=\sigma x_n-x_n$, $\sigma z_n=z_n$ for all σ and n. By assumption, $\pi_{n-1,n}$ maps y_n onto y_{n-1} and, by calculation, it maps x_n onto $x_{n-1}+\pi_{n-1,n}(x_{n,n})$. Therefore, on applying the π's successively to the equation defining y_n, we find that (with an obvious notation for the π's)

$$\begin{aligned}
y_{n-1}&=x_{n-1}+\pi_{n-1,n}(x_{n,n})+\pi_{n-1,n}(z_n)\\
y_{n-2}&=x_{n-2}+\pi_{n-2,n}(x_{n,n})+\pi_{n-2,n-1}(x_{n-1,n-1})+\pi_{n-2,n}(z_n)\\
&\cdots\cdots\\
y_1&=x_1+\pi_{1,n}(x_{n,n})+\cdots+\pi_{1,2}(x_{2,2})+\pi_{1,n}(z_n).
\end{aligned}$$

On comparing this with equation defining z_1, we find that[3]

$$z_1=x_{1,1}+\pi_{1,2}(x_{2,2})+\cdots+\pi_{1,n}(x_{n,n})+\pi_{1,n}(z_n).$$

On applying γ_1 to this, we find that

$$\gamma_1(z_1)=c_1+pc_2+\cdots+p^{n-1}c_n+\gamma_1(\pi_{1,n}(z_n)).$$

Now, $\gamma_1(\pi_{1,n}(z_n))=p^{n-1}\gamma_n(z_n)$, and so, on letting $n\to\infty$, we find that $\gamma_1(z_1)=c\notin\mathbb{Z}$, which is a contradiction.

We can construct a system $(M_n,\pi_{n-1,n},\gamma_n)$ satisfying the conditions as follows. Let G be a profinite group having quotients $G_n\to G_{n-1}$ with G_n of order p^n and $G_n\to G_{n-1}$ onto (e.g., $G=\mathbb{Z}_p$ and $G_n=\mathbb{Z}/p^n\mathbb{Z}$), and let $M_n=\mathbb{Z}[G_n]$. The map $\pi_{n-1,n}$ is induced by $G_n\to G_{n-1}$. As $M_n^G=\mathbb{Z}(\sum_{\sigma\in G_n}\sigma)$, we can define γ_n to be the map sending $\sum_{\sigma\in G}\sigma$ to 1.

Solution to Exercise A-8.

(a) Let A be a central simple algebra over F. If A is a matrix algebra, then $A\approx H(1,1)$ (see (c) below). Otherwise (Wedderburn) it is a division algebra, which we now assume. Let $i\in A$, $i\notin F$. The $F[i]$ is quadratic field extension of F. After completing the square, we may suppose that $i^2=a\in F$. According to Noether-Skolem, there exists $j\in A$ such that $jij^{-1}=-i$. Now j^2 centralizes $F[i]$, and so $j^2\in F[i]$. Because it commutes with j, it lies in F, say $j^2=b\in F$. It remains to check that $1,i,j,ij$ are linearly independent. Suppose

$$c+di+ej+fij=0,\qquad c,d,e,f\in F.$$

On conjugating by i, we find that

$$c+di-ej-fij=0,$$

so

$$c+di=0,$$

[3]Darij Grinberg suggests deleting $x_{1,1}$ and c_1 from the next two equations.

which implies that $c = 0 = d$. Now $0 = ej + fij = (e + fi)j$, and so $e = 0 = f$. This proves that $A \approx H(a, b)$.

(b) Let $A = H(a, b)$. If $w^2 - ax^2 - by^2 + abz^2 = 0$ for some $w, x, y, z \in F$, not all zero, then $\alpha \stackrel{\text{def}}{=} w + xi + yj + zk$ is a nonzero zero-divisor, and A is not a division algebra. Conversely, suppose that, for all nonzero $\alpha \in A$, $\alpha\bar{\alpha} \neq 0$. Because $\alpha\bar{\alpha} \in F \setminus \{0\}$, it has an inverse, and so α is invertible, with inverse $\bar{\alpha}(\alpha\bar{\alpha})^{-1}$.

(c) Let $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. One checks directly that $I, \alpha, \beta, \alpha\beta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is a basis for $M_2(F)$, $\alpha^2 = I$, $\beta^2 = I$, and $\alpha\beta = -\beta\alpha$. Therefore $M_2(F) \approx H(1, 1)$. Alternatively, this follows from (b) (using Wedderburn's theorem).

(d) The map $i \mapsto xi$, $j \mapsto yj$, defines an isomorphism of F-algebras $H(a, b) \to H(ax^2, by^2)$. (DG suggests the map should be $i \mapsto i/x$, $j \mapsto j/y$.)

(e) Tensoring with L doesn't change the multiplication table of a basis for $H(a, b)$.

(f) Let $A = H(a, b)$. Let I be a proper two-sided ideal in A. Because $F \cap I = \{0\}$, $1 + I, i + I, j + I$, and $ij + I$ have the same multiplication table as the original elements, and so A/I is a quaternion algebra $\approx H(a, b)$. In particular, it has degree 4 over F, which implies that I is zero. Thus, A is simple. It is easy to see that F is the centre of A.

(g) The quadratic form

$$w^2 - ax^2 - (1 - a)y^2 + a(1 - a)z^2$$

has $(t, t, t, 0)$ as a nontrivial zero, any nonzero t in F. Thus, we can apply (b).

(h) The quadratic form

$$w^2 - x^2 - by^2 + bz^2$$

has (t, t, s, s) as a nontrivial zero, any $s, t \in F$ not both zero. The quadratic form

$$w^2 - ax^2 + ay^2 - a^2z^2$$

has (at, s, s, t) as a nontrivial zero, any $s, t \in F$ not both zero. Thus, we can apply (b). (Of course, it is more interesting to do both (g) and (h) directly, without assuming Wedderburn's theorem.)

(i) The map $1 \mapsto 1, i \mapsto i, j \mapsto j, k \mapsto -k$ is an isomorphism $H(a, b) \to H(a, b)^{\text{opp}}$.

(j) If b is a square in F, then $H(a, b) \approx M_2(F)$ by (d) and (h), and $a \in \text{Nm}(F[\sqrt{b}])$. Thus, assume that it isn't. Let (w, x, y, z) be a nontrivial zero of $w^2 - ax^2 - by^2 + abz^2$. If $x^2 - bz^2 = 0$, then $w^2 - by^2 = 0$, and all of w, x, y, z are zero, which is a contradiction. Therefore, $x^2 - bz^2 \neq 0$, and

$$a = \frac{w^2 - by^2}{x^2 - bz^2},$$

which is a norm from $F[\sqrt{b}]$ (being a quotient of two norms). Conversely, if $a = w^2 - by^2$, then $w^2 - a1^2 - by^2 + ab0 = 0$, and so $(w, 1, y, 0)$ is a nontrivial zero of the quadratic form.

(k) Use IV, Lemma 3.15, to prove that $H(a, b) \otimes_k H(a, c) \approx H(a, bc)$.

Solution to Exercise A-9.

The p^n cyclotomic polynomial is

$$\Phi(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = X^{p^{n-1}(p-1)} + \cdots + X^{p^{n-1}} + 1.$$

Its roots are the primitive p^nth roots of 1.

Let $F(X) = \Phi(X+1)$. Then $F(0) = \Phi(1) = p$ and

$$F(X) = \frac{(X+1)^{p^n} - 1}{(X+1)^{p^{n-1}} - 1} \equiv \frac{X^{p^n}}{X^{p^{n-1}}} = X^p \mod p.$$

Hence, $F(X)$ is an Eisenstein polynomial, and so is irreducible over $\mathbb{Q}_p$. Its splitting field is L_n. Clearly $L_n = \mathbb{Q}_p[\zeta - 1]$ and $F(X)$ is the minimal polynomial of $\zeta - 1$. Therefore $\mathrm{Nm}_{L_n/\mathbb{Q}_p}(\zeta - 1) = (-1)^{\deg F} F(0) = p$ (provided $p^{n-1}(p-1)$ is even, which it except in the trivial case $n = 1$, $p = 2$).

The second statement is obvious.

Solution to Exercise A-10.

We have to show that, for each $d|n$, the set of primes $\mathfrak{p}$ of K unramified in L and with $(\mathfrak{p}, L/K)$ of order d has polar density $\varphi(d)/n$. We use induction on d.

If $d = 1$, the set consists of the primes that split completely, which we know has density $1/n = \varphi(1)/n$.

Let H be the subgroup of elements of order dividing d — it is a cyclic subgroup of order d. An element σ of $G = \mathrm{Gal}(L/K)$ has order dividing d if and only if $\sigma|L^H = \mathrm{id}$. Therefore, $(\mathfrak{p}, L/K)$ has order dividing $d \iff (\mathfrak{p}, L/K)|L^H = 1$. But $(\mathfrak{p}, L/K)|L^H = (\mathfrak{p}, L^H/K)$, and so $(\mathfrak{p}, L/K)$ has order dividing d if and only if $\mathfrak{p}$ splits in L^H — the set of such $\mathfrak{p}$ has density d/n. By induction, those of order $d'|d$, $d' \neq d$, have density $\varphi(d')/n$. Thus, the set of $\mathfrak{p}$ such that $(\mathfrak{p}, L/K)$ has order exactly d is

$$\frac{d}{n} - \sum_{d'|d, d' \neq d} \frac{\varphi(d')}{n} = \frac{d - \sum \varphi(d')}{n}.$$

But $\sum_{d'|d} \varphi(d') = d$ (if ζ is a primitive dth root of 1, then ζ^m is a primitive d'th root of 1 for exactly one divisor d' of d), which completes the proof.

Solution to Exercise A-11.

Note that $\zeta_8 = \frac{1+i}{\sqrt{2}}$, and so $\mathbb{Q}[\zeta_8] \subset \mathbb{Q}[i, \sqrt{2}]$. Since they have the same degree, they must be equal.

The discriminants of $X^2 - 1$, $X^2 + 2$, $X^2 - 2$ are divisible only by 2.

Let p be an odd prime. At least one of $-1, 2, -2$ is a square in $\mathbb{F}_p$ because, for example, if -1 and 2 are not squares, their product will be (the squares have index 2 in $\mathbb{F}_p^\times$). Hence at least one of the polynomials splits in $\mathbb{F}_p[X]$, and also in $\mathbb{Q}_p[X]$ by Hensel's lemma. This shows that at least one of $-1, 2, -2$ is a square in $\mathbb{Q}_p$. Since $16 = (1+i)^8 = (\sqrt{2})^8 = (\sqrt{-2})^8$, it follows that 16 is an eighth power in $\mathbb{Q}_p$.

It is also an eighth power in $\mathbb{R}$.

Appendix C

Sources for the history of class field theory

Artin, Emil; Nesbitt, Cecil J.; Thrall, Robert M.: Rings with Minimum Condition. University of Michigan Publications in Mathematics, no. 1. University of Michigan Press, Ann Arbor, Mich., 1944. x+123 pp. MR0010543

Artin, Emil; Tate, John, Class field theory. AMS Chelsea Publishing, Providence, RI, 2009. viii+194 pp

Brauer, Richard: Emil Artin. Bull. Amer. Math. Soc. 73 1967 27–43.

Conrad, Keith: History of class field theory here.

Fenster, Della D.; Schwermer, Joachim: A delicate collaboration: Adrian Albert and Helmut Hasse and the principal theorem in division algebras in the early 1930's. Arch. Hist. Exact Sci. 59 (2005), no. 4, 349–379.

Fenster, D.D.: 2007. Artin in America (1937–1958): A time of transition. In: Reich, K., Kreuzer, A. (Eds.), Emil Artin (1898–1962): Beiträge zu Leben, Werk und Persönlichkeit. Dr. Erwin Rauner Verlag, Augsburg, pp. 99–118.

Frei, Günther: The reciprocity law from Euler to Eisenstein. The intersection of history and mathematics, 67–90, Sci. Networks Hist. Stud., 15, Birkhäuser, Basel, 1994. MR1308080

Frei, Günther: On the history of the Artin reciprocity law in abelian extensions of algebraic number fields: how Artin was led to his reciprocity law. The legacy of Niels Henrik Abel, 267–294, Springer, Berlin, 2004.

Hasse, Helmut: History of class field theory. 1967 Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) pp. 266–279 Thompson, Washington, D.C. MR0218330

Herbrand, J.: Le Développment Moderne de la Théorie des Corps Algébriques Corps de Classes et Lois de Réciprocité, Gauthier-Villars, Paris, 1936.

Iyanaga, Shōkichi: Collected papers. With a survey of Iyanaga's work on number theory by Ichirō Satake. Iwanami Shoten, Tokyo, 1994. xx+363 pp. MR1272246

Iyanaga, Shokichi: Travaux de Claude Chevalley sur la théorie du corps de classes: introduction. [The works of Claude Chevalley on class field theory: an introduction] Jpn. J. Math. 1 (2006), no. 1, 25–85. MR2261061

Jacobson, Nathan: Abraham Adrian Albert (1905–1972). Bull. Amer. Math. Soc. 80 (1974), 1075–1100. MR0342341

Kisilevsky, H: Olga Taussky-Todd's work in class field theory. Olga Taussky-Todd: in memoriam. Pacific J. Math. 1997, Special Issue, 219–224.

Lemmermeyer, Franz: Reciprocity laws. From Euler to Eisenstein. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. xx+487 pp.

Lewis, David W: Quaternion algebras and the algebraic legacy of Hamilton's quaternions. Irish Math. Soc. Bull. No. 57 (2006), 41–64.

Lorenz, Falko; Roquette, Peter: The theorem of Grunwald-Wang in the setting of valuation theory. Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), 175–212, Fields Inst. Commun., 33, Amer. Math. Soc., Providence, RI, 2003.

Mac Lane, Saunders: Origins of the cohomology of groups. Enseign. Math. (2) 24 (1978), no. 1–2, 1–29. MR0497280

Milne, J.S: The Work of John Tate. In Helge Holden and Ragni Piene, editors, The Abel Prize 2008–2012, pages 259–340. Springer, Heidelberg, 2014. (No MR review.)

Miyake, Katsuya: The establishment of the Takagi-Artin class field theory. The intersection of history and mathematics, 109–128, Sci. Networks Hist. Stud., 15, Birkhäuser, Basel, 1994. MR1308082

Class field theory—its centenary and prospect. Papers from the 7th International Research Institute of the Mathematical Society of Japan (MSJ) held in Tokyo, June 3–12, 1998. Edited by Katsuya Miyake. Advanced Studies in Pure Mathematics, 30. Mathematical Society of Japan, Tokyo, 2001. xii+631 pp.

Miyake, Katsuya: Teiji Takagi, founder of the Japanese School of Modern Mathematics. Jpn. J. Math. 2 (2007), no. 1, 151–164.

Parshall, Karen Hunger: Joseph H. M. Wedderburn and the structure theory of algebras. Arch. Hist. Exact Sci. 32 (1985), no. 3-4, 223–349.

Petri, Birgit; Schappacher, Norbert: From Abel to Kronecker: episodes from 19th century algebra. The legacy of Niels Henrik Abel, 227–266, Springer, Berlin, 2004.

Roquette, Peter: Class field theory in characteristic p, its origin and development. Class field theory—its centenary and prospect (Tokyo, 1998), 549–631, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

Roquette, Peter: The Brauer-Hasse-Noether theorem in historical perspective. Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences], 15. Springer-Verlag, Berlin, 2005. vi+92 pp. ISBN: 3-540-23005-X.

Schappacher, Norbert: On the history of Hilbert's twelfth problem: a comedy of errors. Matériaux pour l'histoire des mathématiques au XXe siècle (Nice, 1996), 243–273, Sémin. Congr., 3, Soc. Math. France, Paris, 1998.

Snyder, Noah: Artin's-L-functions: A Historical Approach. Undergrad thesis (B. Gross). Unpublished.

Stevenhagen, P.; Lenstra, H. W.: Chebotarëv and his density theorem. Math. Intelligencer 18 (1996), no. 2, 26–37. MR1395088

Stevenhagen, Peter: Hilbert's 12th problem, complex multiplication and Shimura reciprocity. Class field theory—its centenary and prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

Tate, J: Problem 9: The general reciprocity law. Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Northern Illinois Univ., De Kalb, Ill., 1974), pp. 311–322. Proc. Sympos. Pure Math., Vol. XXVIII, Amer. Math. Soc., Providence, R. I., 1976. MR0429839

Tate, John Number theory in the 20th century: Part 1. Bull. Amer. Math. Soc. (N.S.) 54 (2017), no. 4, 547–550. MR3683622

Bibliography

ARTIN, E. 1927. Beweis des allgemeinen reziprozitätsgesetzes. *Abh. Math. Semin. Hamb. Univ.* 3:353–363.

ARTIN, E. 1951. Algebraic numbers and algebraic functions. I. Institute for Mathematics and Mechanics, New York University, New York.

ARTIN, E. AND TATE, J. 1961. Class field theory. Harvard, Dept. of Mathematics. Notes from the Artin-Tate seminar on class field theory given at Princeton University 1951–52. Reprinted 1968, 1990; second edition AMS Chelsea Publishing, 2009.

ATIYAH, M. F. AND WALL, C. T. C. 1967. Cohomology of groups, pp. 94–115. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C.

BLANCHARD, A. 1972. Les corps non commutatifs. Presses Universitaires de France, Vendôme. Collection Sup: Le Mathématicien, No. 9.

BOREVICH, A. I. AND SHAFAREVICH, I. R. 1966. Number theory. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York.

BUCUR, I. AND DELEANU, A. 1968. Introduction to the theory of categories and functors. With the collaboration of Peter J. Hilton and Nicolae Popescu. Pure and Applied Mathematics, Vol. XIX. Interscience Publication John Wiley & Sons, Ltd., London-New York-Sydney.

CARTAN, H. AND EILENBERG, S. 1956. Homological algebra. Princeton University Press, Princeton, N. J.

CASSELMAN, B. 2001. The L-group, pp. 217–258. *In* Class field theory—its centenary and prospect (Tokyo, 1998), volume 30 of *Adv. Stud. Pure Math.* Math. Soc. Japan, Tokyo.

CASSELS, J. W. S. 1967. Global fields. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pp. 42–84. Thompson, Washington, D.C.

CASSELS, J. W. S. 1986. Local fields, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge.

J. W. S. Cassels and A. Fröhlich (eds.) 1967. Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C.

CHEVALLEY, C. 1940. La théorie du corps de classes. *Ann. of Math. (2)* 41:394–418.

CHEVALLEY, C. 1954. Class field theory. Nagoya University, Nagoya.

COHEN, H. 2000. Advanced topics in computational number theory, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

FARB, B. AND DENNIS, R. K. 1993. Noncommutative algebra, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

FENSTER, D. D. AND SCHWERMER, J. 2005. A delicate collaboration: Adrian Albert and Helmut Hasse and the principal theorem in division algebras in the early 1930's. *Arch. Hist. Exact Sci.* 59:349–379.

FESENKO, I. B. AND VOSTOKOV, S. V. 1993. Local fields and their extensions, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI. A constructive approach, With a foreword by I. R. Shafarevich.

FRÖHLICH, A. AND TAYLOR, M. J. 1991. Algebraic number theory, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge.

GOLD, R. 1981. Local class field theory via Lubin-Tate groups. *Indiana Univ. Math. J.* 30:795–798.

GOLDSTEIN, L. J. 1971. Density questions in algebraic number theory. *Amer. Math. Monthly* 78:342–351.

GRANT, K. AND LEITZEL, J. 1969. Norm limitation theorem of class field theory. *J. Reine Angew. Math.* 238:105–111.

GROTHENDIECK, A. AND SERRE, J.-P. 2001. Correspondance Grothendieck-Serre. Documents Mathématiques (Paris), 2. Société Mathématique de France, Paris. (Editors Colmez, Pierre and Serre, Jean-Pierre). Available at www.grothendieck-circle.org.

HALL, JR., M. 1959. The theory of groups. The Macmillan Co., New York, N.Y.

HARRIS, M. AND TAYLOR, R. 2001. The geometry and cohomology of some simple Shimura varieties, volume 151 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ. With an appendix by Vladimir G. Berkovich.

HAZEWINKEL, M. 1975. Local class field theory is easy. *Advances in Math.* 18:148–181.

HENNIART, G. 2000. Une preuve simple des conjectures de Langlands pour $GL(n)$ sur un corps p-adique. *Invent. Math.* 139:439–455.

HERSTEIN, I. N. 1968. Noncommutative rings. The Carus Mathematical Monographs, No. 15. Published by The Mathematical Association of America.

IWASAWA, K. 1986. Local class field theory. Oxford Science Publications. The Clarendon Press Oxford University Press, New York. Oxford Mathematical Monographs.

IYANAGA, S. 1975. The theory of numbers. North-Holland Mathematical Library, Vol. 8. With contributions by T. Tannaka, T. Tamagawa, I. Satake, Akira Hattori, G. Fujisaki and H. Shimizu, Translated from the Japanese by K. Iyanaga.

JANUSZ, G. J. 1996. Algebraic number fields, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition.

KOCH, H. 1992. Algebraic Number Fields. Springer. (Number theory. II. Algebraic number theory. A translation of Number theory, 2 (Russian), Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1990. Edited by A. N. Parshin and I. R. Shafarevich. Encyclopaedia of Mathematical Sciences, 62. Springer-Verlag, Berlin, 1992. iv+269 pp. ISBN: 3-540-53386-9).

LANG, S. 1970. Algebraic number theory. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont.

LUBIN, J. 1981. The local Kronecker-Weber theorem. *Trans. Amer. Math. Soc.* 267:133–138.

LUBIN, J. AND TATE, J. 1965. Formal complex multiplication in local fields. *Ann. of Math. (2)* 81:380–387.

MAC LANE, S. 1978. Origins of the cohomology of groups. *Enseign. Math. (2)* 24:1–29.

MARCUS, D. A. 1977. Number fields. Springer-Verlag, New York. Universitext.

MILNE, J. S. 2006. Arithmetic duality theorems. BookSurge, LLC, Charleston, SC, second edition.

MILNE, J. S. 2020. Elliptic Curves. World Scientific Press, second edition.

NARKIEWICZ, W. 1990. Elementary and analytic theory of algebraic numbers. Springer-Verlag, Berlin, second edition.

NEUKIRCH, J. 1986. Class field theory, volume 280 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin.

O'MEARA, O. T. 1963. Introduction to quadratic forms. Die Grundlehren der mathematischen Wissenschaften, Bd. 117. Academic Press Inc., Publishers, New York.

RAMAKRISHNAN, D. AND VALENZA, R. J. 1999. Fourier analysis on number fields, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

RASKIND, W. 1995. Abelian class field theory of arithmetic schemes, pp. 85–187. *In K*-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), volume 58 of *Proc. Sympos. Pure Math.* Amer. Math. Soc., Providence, RI.

ROQUETTE, P. 1967. On class field towers, pp. 231–249. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C.

ROQUETTE, P. 2005. The Brauer-Hasse-Noether theorem in historical perspective, volume 15 of *Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences]*. Springer-Verlag, Berlin.

ROSEN, M. 1981. An elementary proof of the local Kronecker-Weber theorem. *Trans. Amer. Math. Soc.* 265:599–605.

ROSENBERG, J. 1994. Algebraic K-theory and its applications, volume 147 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

SCHAPPACHER, N. 1998. On the history of Hilbert's twelfth problem: a comedy of errors, pp. 243–273. *In* Matériaux pour l'histoire des mathématiques au XX^{e} siècle (Nice, 1996), volume 3 of *Sémin. Congr.* Soc. Math. France, Paris.

SERRE, J.-P. 1962. Corps locaux. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris. Translated as Local Fields 1979.

SERRE, J.-P. 1964. Cohomologie Galoisienne, volume 5 of *Lecture Notes in Math.* Springer-Verlag, Berlin. Translated as Galois Cohomology 2002.

SERRE, J.-P. 1967a. Complex multiplication, pp. 292–296. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C.

SERRE, J.-P. 1967b. Local class field theory. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pp. 128–161. Thompson, Washington, D.C.

SERRE, J.-P. 1970. Cours d'arithmétique, volume 2 of *Collection SUP: "Le Mathématicien"*. Presses Universitaires de France, Paris. (Translated as A Course in Arithmetic, 1973).

SHATZ, S. S. 1972. Profinite groups, arithmetic, and geometry. Princeton University Press, Princeton, N.J. Annals of Mathematics Studies, No. 67.

SILVERMAN, J. H. AND TATE, J. 1992. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York.

TATE, J. 1952. The higher dimensional cohomology groups of class field theory. *Ann. of Math. (2)* 56:294–297.

TATE, J. 1979. Number theoretic background, pp. 3–26. *In* Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I.

TATE, J. T. 1967. Global class field theory, pp. 162–203. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C.

WASHINGTON, L. C. 1997. Introduction to cyclotomic fields, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

WEI, W. 1993. Weil numbers and generating large field extensions. PhD thesis, University of Michigan. Available at the library of the University of Michigan, Ann Arbor.

WEI, W. 1994. Moduli fields of CM-motives applied to Hilbert's 12-th problem. 18pp; http://www.mathematik.uni-bielefeld.de/sfb343/preprints/pr94070.ps.gz.

WEIL, A. 1967. Basic number theory. Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag New York, Inc., New York.

WEISS, E. 1969. Cohomology of groups. Pure and Applied Mathematics, Vol. 34. Academic Press, New York.

WIESEND, G. 2007. Class field theory for arithmetic schemes. *Math. Z.* 256:717–729.

Index