CLASS FIELD THEORY

J.S. Milne

Preface.

These[1][2] are the notes for Math 776, University of Michigan, Winter 1997, slightly revised from those handed out during the course. They have been substantially revised and expanded from an earlier version, based on my notes from 1993 (v2.01).

My approach to class field theory in these notes is eclectic. Although it is possible to prove the main theorems in class field theory using neither analysis nor cohomology, there are major theorems that can not 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. When it sheds additional light, I have not hesitated to include more than one proof of a result.

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 not interested in *explicit* local class field theory.

References of the form Math xxx are to course notes available at http://www.math.lsa.umich.edu/∼jmilne.

Please send comments and corrections to me at jmilne@umich.edu.

Books including class field theory

Artin, E., Algebraic Numbers and Algebraic Functions, NYU, **1951**. (Reprinted by Gordon and Breach, 1967).

Artin, E., and Tate, J., Class Field Theory. Notes of a Seminar at Princeton, **1951/52**. (Harvard University, Mathematics Department, 1961; Benjamin, 1968; Addison Wesley, 1991).

Cassels, J.W.S., and Fröhlich, A., (Eds), Algebraic Number Theory, Academic Press, **1967**.

Fesenko, I.B., and Vostokov, S.V., Local Fields and their Extensions, AMS, **1993**.

Goldstein, L.J., Analytic Number Theory, Prentice Hall, **1971**.

Iwasawa, K., Local Class Field Theory, Oxford, **1986**.

Iyanaga, S., (ed.), The Theory of Numbers, North-Holland, **1975**.

Janusz, G.J., Algebraic Number Fields, Academic Press, 1973; Second Edition, AMS, **1996**.

Koch, H., Number Theory II, Algebraic Number Theory, Springer, **1992**. (Encyclopaedia of Mathematical Sciences, Vol. 62, Parshin, A.N., and Shafarevich, I.R., Eds).

Lang, S., Algebraic Number Theory, Addison-Wesley, **1970**.

Neukirch, J., Class Field Theory, Springer, **1985**.

Neukirch, J., Algebraische Zahlentheorie, Springer, **1992**.

Serre, J-P., Corps Locaux, Hermann, **1962**.

[1] May 6, 1997; v3.1

Weil, A., Basic Number Theory, Springer, **1967**.

The articles of Serre and Tate in Cassels and Fröhlich 1967, and Janusz 1973, have been especially useful in the writing of these notes.

Books including an introduction to class field theory

Cohn, H., A Classical Invitation to Algebraic Numbers and Class Fields, Springer, **1978**.

Cox, D.A., Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, Wiley, **1989**.

Marcus, D. A., Number Fields, Springer **1977**.

Sources for the history of algebraic number theory and class field theory

Edwards, H.M., Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Springer, **1977**.

Ellison, W. and F., Théorie des nombres, in Abrégé d'Histoire des Mathématiques 1700–1900, Vol I, (J. Dieudonné, ed.) Hermann, Paris, **1978**, pp 165–334.

Herbrand, J., Le Développment Moderne de la Théorie des Corps Algébriques Corps de Classes et Lois de Réciprocité, Gauthier-Villars, Paris, **1936**.

Smith, H.J.S., Report on the the Theory of Numbers, Reports of the British Association, **1859/1865**. (Reprinted by Chelsea, New York, 1965.)

Weil, Number Theory: An Approach Through History, Birkhäuser, **1984**.

Also: Hasse's article in Cassels and Fröhlich 1967. Appendix 2 in Iyanaga 1975. Iwasawa's appendix to the Collected Papers of Teiji Takagi. Tate's article "Problem 9: The general reciprocity law" in *Mathematical Developments Arising from Hilbert's Problems*, AMS, 1976. Weil's article, Oeuvres 1974c. N. Schappacher, On the history of Hilbert's twelfth problem (preprint). P. Stevenhagan and H.W. Lenstra, Chebotarëv and his density theorem, Math. Intelligencer, 18.2, 1996, 26–37.

For an introduction to nonabelian class field theory: Arthur's article in *1980 Seminar on Harmonic Analysis*, CMS Conference Proceedings Vol 1, AMS, 1981.

Notations: For a ring R (always with 1), $R^\times$ denotes the group of invertible elements. We use $X \stackrel{\text{df}}{=} Y$ to mean "X is defined to be Y" or "$X = Y$ by definition", $X \approx Y$ to mean that X and Y are isomorphic, and $X \cong Y$ to mean X and Y are isomorphic with a given (canonical, or unique) isomorphism.

Contents

Introduction

Class field theory relates the arithmetic of a number field (or local field) to the Galois extensions of the field. For abelian extensions, the theory was developed between roughly 1850 and 1927 by Kronecker, Weber, Hilbert, Takagi, Artin, and others. For nonabelian extensions, serious progress began only about 25 years ago with the work of Langlands. Today, the nonabelian theory is in roughly the state that abelian class field theory was in 100 years ago: there are comprehensive conjectures but few proofs. In this course, we shall be concerned only with abelian class field theory.

Statement of the main problem. For a finite extension L/K of number fields and a finite set S of prime ideals of K containing all those that ramify in L, let $\mathrm{Spl}_S(L/K)$ be the set of prime ideals $\mathfrak{p}$ of K not in S that split completely in L, i.e., such that $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i$ with $f(\mathfrak{P}_i/\mathfrak{p}) = 1$ for all i. For example, if $L = K[\alpha] \cong K[X]/(f(X))$ and S contains the prime ideals dividing the discriminant of f, then $\mathrm{Spl}_S(L/K)$ is the set of prime ideals $\mathfrak{p}$ such that $f(X)$ splits completely modulo $\mathfrak{p}$. If L/K is Galois, then $\mathrm{Spl}_S(L/K)$ has[3] density $1/[L:K]$, and it follows that $\mathrm{Spl}_S(L/K)$ determines[4] L. Thus the problem of classifying the Galois extensions of K ramified only at prime ideals in S becomes that of determining which sets of primes in K arise as $\mathrm{Spl}_S(L/K)$ for some such L/K.

For quadratic extensions $L/\mathbb{Q}$, the answer is provided by the quadratic reciprocity law:

> Let m be a positive integer that is either odd or divisible by 4, and let S be a finite set of prime numbers containing all those that divide m. For a subgroup H of $(\mathbb{Z}/m\mathbb{Z})^\times$ of index 2, let
>
> $$Pr(H) = \{(p) \mid p \text{ a prime number, } p \notin S,\ p \mod m \text{ lies in } H\}.$$
>
> Then the sets $\mathrm{Spl}_S(L/\mathbb{Q})$ for L running over the quadratic extensions of $\mathbb{Q}$ ramified only at primes in S are exactly the sets $Pr(H)$.

For example, let p be an odd prime number, and let S be a finite set of prime numbers containing p. Let $p^* = (-1)^{\frac{p-1}{2}}p$, so that $p^* \equiv 1 \mod 4$. 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

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

and so $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Therefore q splits in $\mathbb{Q}[\sqrt{p^*}]$ if and only if q is a square modulo p. The same is true of $q = 2$. The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, and so has a unique subgroup H of index 2, namely, that consisting of squares. Therefore, the sets $\mathrm{Spl}_S(\mathbb{Q}[\sqrt{p^*}]/\mathbb{Q})$, p an odd prime number not in S, are precisely those of the form $Pr(H)$ with H the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 2. The proof of the general case is left as an exercise.

---

[3] A proof of this, essentially independent of the rest of the course, is given in Chapter VI).

[4] We are considering only the extensions of K contained in some fixed algebraic closure of K.

By extension, any result identifying the sets $\mathrm{Spl}_S(L/K)$ for some class of extensions L/K is usually called a reciprocity law, even when no reciprocity is involved.

Classification of unramified abelian extensions. Let I be the group of fractional ideals of K, i.e., the free abelian group generated by the prime ideals, and let $i : K^\times \to I$ be the map sending $a \in K^\times$ to the principal ideal (a). The class group C of K is $I/i(K^\times)$. To give a subgroup H of C is the same as to give a subgroup $\widetilde{H}$ of I containing $i(K^\times)$.

By a "prime" of K, we mean an equivalence class of nontrivial valuations on K. Thus there is exactly one prime for each 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.

Let H be a subgroup of the class group C of K. An extension L of K is said to be a *class field* for H if

(a) L is a finite abelian extension of K;
(b) no prime of K ramifies in L;
(c) the prime ideals of K splitting in L are those in $\widetilde{H}$.

The condition (b) means that no prime ideal of K ramifies in L and that no real prime of K has a complex prime lying over it, for example, $\mathbb{Q}[\sqrt{-5}]/\mathbb{Q}$ fails the condition at $2, 5, \infty$.

THEOREM 0.1. *A class field exists for each subgroup H of C. It is unique, and $C/H \approx \mathrm{Gal}(L/K)$. Moreover, every extension L/K satisfying (a) and (b) is the class field of some H.*

The existence of a class field for the trivial subgroup of C was conjectured by Hilbert in 1897, and proved by his student Furtwängler in 1907—for this reason, this class field 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 $\mathrm{Gal}(L/K) \approx C$. Hilbert also conjectured that every ideal in K becomes principal in the Hilbert class field, and this was proved by Furtwängler in 1930 (Principal Ideal Theorem) after Artin had reduced the proof to an exercise in group theory.

EXAMPLE 0.2. The class number of $\mathbb{Q}[\sqrt{-5}]$ is 2 (Math 676, 4.6), and its Hilbert class field is $\mathbb{Q}[\sqrt{-5}, \sqrt{-1}]$.

Classification of ramified abelian extensions. In order to obtain ramified abelian extensions, we need to consider more general class groups. A *modulus* $\mathfrak{m}$ is a function

$$m : \{\text{primes of } K\} \to \mathbb{Z}$$

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 a real prime, then $m(\mathfrak{p}) = 0$ or 1; if $\mathfrak{p}$ is complex, then $m(\mathfrak{p}) = 0$.

Traditionally, one writes

$$\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}.$$

Let $S = S(\mathfrak{m})$ be the set of finite primes for which $m(\mathfrak{p}) > 0$, and let I^S be the group of S-ideals (free abelian group generated by the prime ideals not in S). Let $K_{\mathfrak{m}}$ be the set of nonzero elements of K that can be expressed in the form $\frac{a}{b}$ with $(a), (b) \in I^S$, and let $K_{\mathfrak{m},1}$ be the subgroup of $\alpha \in K_{\mathfrak{m}}$ such that

$$\begin{cases} \operatorname{ord}_{\mathfrak{p}}(\alpha - 1) & \geq m(\mathfrak{p}) \quad \text{for all finite } \mathfrak{p} \text{ with } m(\mathfrak{p}) > 0 \\ \alpha & \text{is positive at all real } \mathfrak{p} \text{ with } m(\mathfrak{p}) = 1. \end{cases}$$

Let i denote the map sending an element α of $K_{\mathfrak{m},1}$ to the principal ideal (α) it defines in I^S. The *ray class group* for the modulus $\mathfrak{m}$ is defined to be

$$C_{\mathfrak{m}} = I^S / i(K_{\mathfrak{m},1}).$$

EXAMPLE 0.3. (a) If $m(\mathfrak{p}) = 0$ for all $\mathfrak{p}$, then $C_{\mathfrak{m}}$ is just the usual ideal class group.

(b) If $m(\mathfrak{p}) = 1$ for all real primes and $m(\mathfrak{p}) = 0$ otherwise, then $K_{\mathfrak{m},1}$ consists of the *totally positive* elements of K, i.e., those that are positive in every real embedding of K, and $C_{\mathfrak{m}}$ is called the *narrow class group.*

(c) Let m be an integer that is either odd or divisible by 4, and let $\mathfrak{m} = (m)\infty$ where ∞ denotes the real prime of $\mathbb{Q}$. Then

$$\begin{aligned} S &= \{(p) \mid p|m\}; \\ I^S &= \text{set of ideals of the form } \textstyle\prod (p)^{r(p)},\ \gcd(p, m) = 1,\ r(p) \in \mathbb{Z}; \\ \mathbb{Q}_{\mathfrak{m}} &= \{b/c \mid b, c \in \mathbb{Z}, \quad \gcd(b, m) = 1 = \gcd(c, m)\}; \\ \mathbb{Q}_{\mathfrak{m},1} &= \{a \in \mathbb{Q}_{\mathfrak{m}} \mid a > 0, \quad \operatorname{ord}_p(a - 1) \geq r \text{ if } p^r|m,\ r > 0\}. \end{aligned}$$

If $c \in \mathbb{Z}$ is relatively prime to m, then there exist $d, e \in \mathbb{Z}$ such that $cd+me = 1$, and so c becomes a unit in $\mathbb{Z}/m\mathbb{Z}$. Each $\mathfrak{a} \in I^S$ can be represented $\mathfrak{a} = (b/c)$ with b and c positive integers. Therefore there is a well-defined map[5] map $(b/c) \mapsto [b][c]^{-1} : I^S \to (\mathbb{Z}/m\mathbb{Z})^\times$, which one can show induces an isomorphism $C_{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^\times$.

To give a subgroup H of $C_{\mathfrak{m}}$ is the same as to give a subgroup $\widetilde{H}$ of I^S containing $i(K_{\mathfrak{m},1})$.

Let H be a subgroup of the ray class group $C_{\mathfrak{m}}$ of K, and let $S = S(\mathfrak{m})$. An extension L of K is said to be a *class field* for H if

(a) L is a finite abelian extension of K;
(b) $m(\mathfrak{p}) = 0 \implies \mathfrak{p}$ does not ramify in L;
(c) the prime ideals not in S that split in L are those in $\widetilde{H}$.

THEOREM 0.4. *A class field exists for each subgroup H of $C_{\mathfrak{m}}$. It is unique, and $C_{\mathfrak{m}}/H \approx \operatorname{Gal}(L/K)$. Moreover, every finite abelian extension L/K is a class field for some $\mathfrak{m}$ and H.*

[5]Here, and elsewhere, I use $[x]$ to denote an equivalence class containing x.

Ray class groups were defined by Weber in 1897. Theorem 0.4 was proved by Takagi in a series of papers published between 1915 and 1922—see especially his talk at the 1920 International Congress, where he states his results almost exactly as we have (Collected Papers, p168, QA3.T341).

The class field L for the trivial subgroup of $C_{\mathfrak{m}}$ is called the *ray class field* for $\mathfrak{m}$. It is ramified only at primes dividing $\mathfrak{m}$, and $C_{\mathfrak{m}} \approx \mathrm{Gal}(L/K)$.

EXAMPLE 0.5. 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 $\mathbb{Q}$ at all finite primes (but is ramified at both infinite primes).

For any finite set S of finite primes of K, Takagi's theorem 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.

EXAMPLE 0.6. Let $d = p_1^* \cdots p_t^*$ where the p_i are odd primes and $p_i^* = (-1)^{\frac{p-1}{2}} p_i$, as before. The field $K = \mathbb{Q}[\sqrt{d}]$ is ramified exactly over the primes $p_1, \dots, p_t$. 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 can't 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, we find that

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

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 a only a little more effort one can prove the following:

> 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, 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.

The Artin map. Takagi showed that if L is the class field for H, then $C_{\mathfrak{m}}/H$ is isomorphic to $\mathrm{Gal}(L/K)$. Any modern mathematician looking at this result will immediately ask whether there is a *natural* isomorphism $C/H \to \mathrm{Gal}(L/K)$. Surprisingly, this question seems not to have occurred to Kronecker, Weber, Hilbert, Takagi et al.. Artin did show that there is a natural isomorphism, but even he did this to obtain another result that interested him.

Let L/K be a finite Galois extension with Galois group G. Recall that the decomposition group $D(\mathfrak{P})$ of a prime ideal $\mathfrak{P}$ in $\mathcal{O}_L$ is the set of $\sigma \in G$ such that $\sigma\mathfrak{P} = \mathfrak{P}$. Any $\sigma \in D(\mathfrak{P})$ acts continuously for the $\mathfrak{P}$-adic topology on L, and so extends to the completion $L_{\mathfrak{P}}$ of L at $\mathfrak{P}$. In this way, we obtain an isomorphism

$D(\mathfrak{P}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, $\mathfrak{p} = \mathfrak{P} \cap K$. When $\mathfrak{P}$ is unramified over $\mathfrak{p}$, then the natural map $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(l/k)$ is an isomorphism. Here l and k are the residue fields at $\mathfrak{P}$ and $\mathfrak{p}$. Therefore, there is a unique element $(\mathfrak{P}, L/K) \in D(\mathfrak{P})$ inducing the Frobenius map $x \mapsto x^q$, $q = (\mathcal{O}_K : \mathfrak{p})$, on the residue field. It is the unique $\sigma \in \mathrm{Gal}(L/K)$ such that:

(a) $\sigma\mathfrak{P} = \mathfrak{P}$;
(b) for all $\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^q \mod \mathfrak{P}$.

If $\mathfrak{Q}$ also lies over $\mathfrak{p}$, then $\mathfrak{Q} = \tau\mathfrak{P}$ for some $\tau \in \mathrm{Gal}(L/K)$, and $(\mathfrak{Q}, L/K) = \tau \circ (\mathfrak{P}, L/K) \circ \tau^{-1}$. Therefore, to each prime $\mathfrak{p}$ of K that is unramified in L, we have attached a conjugacy class

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

of elements in $\mathrm{Gal}(L/K)$. Note that each element in $(\mathfrak{p}, L/K)$ has order $f(\mathfrak{P}/\mathfrak{p})$.

In an abelian group, conjugacy classes consist of single elements, and so in this case we can regard $(\mathfrak{p}, L/K)$ as an element of $\mathrm{Gal}(L/K)$.

THEOREM 0.7. *Let L be an abelian extension of K, and let S be the set of finite primes ramifying in L. Then, for some modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, the map*

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

factors through $I^S/i(K_{\mathfrak{m},1})$, and defines an isomorphism $C_{\mathfrak{m}}/H \to \mathrm{Gal}(L/K)$ where H is the ray class group corresponding to L.

If the map were not surjective, then there would be a proper extension of K in which every prime of K splits. It is easy to see analytically (much harder algebraically) that no such extension exists. The difficult point to prove is that there exists a modulus $\mathfrak{m}$ such that kernel of the map $I^S \to \mathrm{Gal}(L/K)$ contains $i(K_{\mathfrak{m},1})$ for some $\mathfrak{m}$.

Theorem 0.7 was proved by Artin (published 1927), and the homomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is called the *Artin (or reciprocity) map*.

EXAMPLE 0.8. Let m be a positive integer that is either odd or divisible by 4, and let $L = \mathbb{Q}[\zeta]$ be the field generated by a primitive m^{th} root of 1. Recall (Math 676, Section 6) that there is an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q}), \quad [n] \mapsto (\zeta \mapsto \zeta^n).$$

Let $\mathfrak{P}$ be a prime of L lying over a prime p not dividing m. Because $\mathcal{O}_L/\mathfrak{P}$ has characteristic p, for any $\alpha = \sum a_i\zeta^i$, $a_i \in \mathbb{Z}$,

$$(\sum a_i\zeta^i)^p \equiv \sum a_i\zeta^{ip} \mod \mathfrak{P}.$$

Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ map ζ to ζ^p. Then this congruence shows that $\alpha \in \mathfrak{P} \implies \sigma\alpha \in \mathfrak{P}$, i.e., that $\sigma\mathfrak{P} = \mathfrak{P}$, and that σ acts $x \mapsto x^p$ on $\mathcal{O}_L/\mathfrak{P}$. Therefore $\sigma = (\mathfrak{P}, L/\mathbb{Q}) = (p, L/\mathbb{Q})$.

Let $\mathfrak{m} = (m)\infty$. It follows easily from the above remarks that $p \mapsto (p, L/\mathbb{Q}) : I^{S(\mathfrak{m})} \to \mathrm{Gal}(L/\mathbb{Q})$ factors through $C_{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$, and defines an isomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L/\mathbb{Q})$.

Explicit class field theory. Takagi's theorem states that with every modulus for K there is associated a ray class field L, but it does not explain how to construct L. For the $\mathbb{Q}$, the ray class field for $\mathfrak{m} = (m)\infty$ is generated by $\zeta = e^{2\pi i/m}$. In the 12^{th} of his famous problems, Hilbert asked whether the ray class fields for other number fields can be generated by the special values of explicit holomorphic functions. There are some very beautiful results on the problem, but they remain rather special: in general, we don't know how to construct class fields explicitly.

Nonabelian class field theory. For abelian extensions, class field theory shows that each set $\mathrm{Spl}_S(L/K)$ is described by congruence conditions. For nonabelian extensions, this is no longer true, and any description of the sets must be analytic. I briefly explain what is expected to be true. For simplicity, I take $K = \mathbb{Q}$.

Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G, and let S be the set of finite primes ramifying in L. From each prime $(p) \notin S$, we obtain a conjugacy class $(p, L/\mathbb{Q})$ of Frobenius elements of G. One group whose conjugacy classes we understand is $\mathrm{GL}_n(\mathbb{C})$—this is the theory of Jordan canonical forms—and so it is natural to fix an injective homomorphism $\rho : G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$. Then ρ maps $(p, L/\mathbb{Q})$ to a conjugacy class $\Phi_p(\rho)$ in $\mathrm{GL}_n(\mathbb{C})$. Note that

$$\mathrm{Spl}_S(L/\mathbb{Q}) = \{(p) \mid \Phi_p(\rho) = \{I\}\}.$$

The elements of $\Phi_p(\rho)$ are diagonalizable, and so $\Phi_p(\rho)$ is determined by the common characteristic polynomial $\det(I - \Phi_p(\rho)T)$ of its elements. Set

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

For example, if $L = \mathbb{Q}$ and $n = 1$, then

$$L(s, \rho) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s).$$

The product converges to a holomorphic function in some right half plane in $\mathbb{C}$, and an elementary lemma on Dirichlet series implies that the factors $\frac{1}{\det(I-\Phi_p(\rho)p^{-s})}$ are uniquely determined by the analytic function $L_S(s, \rho)$. 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 set of L-series, called *automorphic L-series,* and conjectures[6] 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 $\mathbb{Q}$.

The L-functions $L_S(s, \rho)$ were defined by Artin, and so are called *Artin L-series.* 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 0.7.

For $n = 2$, Langlands (and Tunnell) have proved the conjecture in some cases. (Their result played a vital role in Wiles's work on the Taniyama conjecture.)

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

Exercises.

0.1. 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.

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

0.3. Prove that the map $I^S \to (\mathbb{Z}/m\mathbb{Z})^\times$ defined in Example 0.3 has kernel $i(\mathbb{Q}_{\mathfrak{m},1})$, and hence induces an isomorphism $C_\mathfrak{m} \to (\mathbb{Z}/m\mathbb{Z})^\times$.

0.4. Prove the statements in Example 0.5.

0.5. Let $L = \mathbb{Q}[\sqrt{-1}, \sqrt{-5}]$. Then $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 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 20^{th} root of 1.

CHAPTER I

Local Class Field Theory: Statements of the Main Theorems and Lubin-Tate Extensions

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 valuation. Thus 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 (rather than the more customary 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 $m \stackrel{\text{df}}{=} \text{ord}_K(a)$. The residue field k of K has q elements, and its characteristic is p. The normalized valuation on K is defined by $|a| = q^{-\text{ord}_K(a)}$.

We fix a separable algebraic closure K^{al} of K. Throughout the chapter "extension of K" will mean "subfield of K^{al} containing K". Both ord_K and $|\cdot|$ have unique extensions to K^{al}.

1. Statements of the Main Theorems

The composite of two finite abelian extensions of K is again a finite abelian extension of K. 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 $\text{Gal}(K^{\text{al}}/K)$ by the closure of its commutator subgroup. (See the appendix to this chapter for a review of the Galois theory of infinite extensions.)

Let L be a finite unramified extension of K. Then L is Galois over K, and there is a unique element $\sigma \in \text{Gal}(L/K)$ such that $\sigma\alpha \equiv \alpha^q$ for all $\alpha \in \mathcal{O}_L$, i.e., such that σ induces the Frobenius automorphism on the residue field of L. This σ is called the *Frobenius element* of $\text{Gal}(L/K)$, and is denoted $\text{Frob}_{L/K}$. It generates $\text{Gal}(L/K)$. (See Math 676, 7.41 et seqq.)

THEOREM 1.1 (LOCAL RECIPROCITY LAW). *For any nonarchimedian local field, there is a unique homomorphism*

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

with the following properties:

(a) *for any prime element π of K and any finite unramified extension L of K, $\phi_K(\pi)|L = \mathrm{Frob}_{L/K}$;*
(b) *for any 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*

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

Denote $\mathrm{Nm}_{L/K}(L^\times)$ by $\mathrm{Nm}(L^\times)$. Statement (b) says that, for every finite abelian extension L of K, there is a commutative diagram

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

with $\phi_{L/K}$ an isomorphism. I shall refer to ϕ_K (and $\phi_{L/K}$) as the *local Artin map.* Other names in use: (local) reciprocity map, norm residue map (symbol), etc..

THEOREM 1.2 (LOCAL EXISTENCE THEOREM). *A subgroup N of $K^\times$ is of the form $\mathrm{Nm}_{L/K}(L^\times)$ for some finite abelian extension L of K if and only if it is of finite index and open.*

The proofs of these theorems will occupy most of the rest of this chapter and of chapter 3. First, we note an immediate consequence.

COROLLARY 1.3. *The map $L \mapsto \mathrm{Nm}(L^\times)$ is a bijection from the set of finite abelian extensions of K to the set of open subgroups of finite index in $K^\times$. Moreover*

$$\begin{aligned} L_1 \subset L_2 &\iff \mathrm{Nm}(L_1^\times) \supset \mathrm{Nm}(L_2^\times); \\ \mathrm{Nm}(L_1 \cdot L_2) &= \mathrm{Nm}(L_1) \cap \mathrm{Nm}(L_2); \\ \mathrm{Nm}(L_1 \cap L_2) &= \mathrm{Nm}(L_1) \cdot \mathrm{Nm}(L_2). \end{aligned}$$

PROOF. Let $\bar{K}$ be a finite abelian extension of K. According to the Theorem 1.1, $\phi_{\bar{K}/K}$ identifies $K^\times/\mathrm{Nm}(\bar{K}^\times)$ with $\mathrm{Gal}(\bar{K}/K)$ in such a way that a subfield L of $\bar{K}$ is the fixed field of the subgroup $\mathrm{Nm}(L^\times)/\mathrm{Nm}(\bar{K}^\times)$ of $K^\times/\mathrm{Nm}(\bar{K}^\times)$. Moreover, Theorem 1.2 shows that every subgroup H of $K^\times$ containing $\mathrm{Nm}(\bar{K}^\times)$ is a norm group. Therefore, so far as it concerns subfields of $\bar{K}$ and subgroups of $K^\times$ containing $\mathrm{Nm}(\bar{K})$, the corollary is a restatement of the main theorem of Galois theory. The full result is obtained by letting $\bar{K}$ grow. □

REMARK 1.4. Corollary 1.3 also holds 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 $\mathbb{R}_{>0}$. 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. Moreover, there is a unique isomorphism (*local Artin map* in the real case)

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

namely, that sending r to the identity map or complex conjugation according as $r > 0$ or $r < 0$. This verifies the corollary for $K = \mathbb{R}$, and it is even more obvious for $K = \mathbb{C}$.

REMARK 1.5. If K has characteristic zero, then *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 (Math 676, 7.23) applied to $X^m - a$ shows that any $a \in \mathcal{O}_K^\times$ 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.

If K has characteristic $p \neq 0$, then *not* every subgroup of $K^\times$ of finite index is open. Note that an open subgroup is also closed (because its complement is a union of cosets of the group, which are also 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 $\prod_{\mathbb{N}} \mathbb{F}_p$. Let $a = (a_n)_{n\in\mathbb{N}} \in \prod_{\mathbb{N}} \mathbb{F}_p$, and let $a(m) = (a(m)_n)_{n\in\mathbb{N}}$ be such that $a(m)_n = a_n$ for $n \leq m$ and $a(m)_n = 0$ otherwise. Then $a(m) \to a$ as $m \to \infty$, and so $\oplus_{\mathbb{N}}\mathbb{F}_p$ is dense in $\prod_{\mathbb{N}} \mathbb{F}_p$. Therefore any proper subgroup of $\prod_{\mathbb{N}} \mathbb{Z}_p$ containing $\oplus_{\mathbb{N}}\mathbb{Z}_p$ can not be closed. Because $\prod_{\mathbb{N}} \mathbb{F}_p/\oplus_{\mathbb{N}} \mathbb{F}_p$ is a vector space over $\mathbb{F}_p$, it will have subspaces of finite index, and the inverse image of such a subspace in $K^\times$ will be a nonclosed subgroup of finite index.

REMARK 1.6. 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 valuation $|\cdot|$ on K^{un}, and hence induces an automorphism $\bar{\sigma}$ of $\bar{k}/k$. The map $\sigma \mapsto \bar{\sigma}$ is an isomorphism $\mathrm{Gal}(K^{\mathrm{un}}/K) \to \mathrm{Gal}(\bar{k}/k)$. 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 $\alpha \mapsto \mathrm{Frob}_K^\alpha : \widehat{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{un}}/K)$ is an isomorphism of topological groups. Condition (a) of Theorem 1.1 can be re-stated as:

(a) for any prime element π of K, $\phi(\pi)$ acts as Frob_K on K^{un}.

Consequences of Theorems 1.1 and 1.2. Assume K possesses a local Artin map, i.e., a homomorphism $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the properties (a) and (b) of Theorem 1.1, and that Theorem 1.2 holds.

As we just remarked, for any prime element π of K, $\phi_K(\pi)|K^{\mathrm{un}} = \mathrm{Frob}_K$. If $u \in U_K$, then πu is also a prime element, and so

$$\phi_K(u)|K^{\mathrm{un}} = \phi_K(\pi u)|K^{\mathrm{un}} \cdot \phi_K(\pi^{-1})|K^{\mathrm{un}} = \mathrm{id}\,.$$

Therefore, U_K is in the kernel of $a \mapsto \phi_K(a)|K^{\mathrm{un}} : K^\times \to \mathrm{Gal}(K^{\mathrm{un}}/K)$, and $\phi_K(a)|K^{\mathrm{un}} = \mathrm{Frob}_K^{\mathrm{ord}_K(a)}$ for any $a \in K^\times$. In other words, the map $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{un}}/K)$ factors into

$$K^\times \xrightarrow{\mathrm{ord}_K} \mathbb{Z} \xrightarrow{n\mapsto \mathrm{Frob}_K^n} \mathrm{Gal}(K^{\mathrm{un}}/K).$$

If K_m is the unramified extension of K of degree m, then

$$\mathrm{Nm}(K_m^\times) = \{a \in K^\times \mid m|\mathrm{ord}_K(a)\} = U_K \cdot \pi^{m\mathbb{Z}}$$

because this is the kernel of $a \mapsto \phi_K(a)|K_m$.

Choose a prime element π in K. Then any element $a \in K^\times$ can be written uniquely $a = u \cdot \pi^m$, $u \in U_K$, $m \in \mathbb{Z}$. Thus

$$K^\times \approx U_K \times \mathbb{Z}, \quad u \cdot \pi^m \leftrightarrow (u, m).$$

Because U_K is both open and closed in $K^\times$, this is an isomorphism of topological groups (discrete topology on $\mathbb{Z}$). The subgroups $1 + \mathfrak{m}^n$, $n \geq 0$, form a fundamental system of neighbourhoods of 1 in K. Clearly therefore, the subgroups $(1 + \mathfrak{m}^n) \times m\mathbb{Z}$ are open of finite index in $U_K \times \mathbb{Z}$, and every open subgroup of finite index contains one of this type. For a finite abelian extension L of K, the smallest f such that $\mathrm{Nm}(L^\times)$ contains $1 + \mathfrak{m}^f$ is called the *conductor* of L/K, except that, when $\mathrm{Nm}(L^\times) \supset U_K$, the conductor is said to be 0. Thus L/K is unramified if and only if its conductor is 0, and it is tamely ramified if and only if its conductor is ≤ 1.

The homomorphisms

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

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

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

—in particular, there is a one-to-one correspondence between the set of closed subgroups of $\widehat{K^\times}$ and the set of abelian extensions of K. Here $\widehat{K^\times}$ 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 1.2, the norm groups are the open subgroups of finite index in $K^\times$. The norm topology is coarser than the usual topology on $K^\times$—for example, U_K is not open—but it induces the usual topology on U_K. When we complete the terms in the exact sequence

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

with respect to the norm topology, we obtain an exact sequence

$$0 \to U_K \to \widehat{K^\times} \to \widehat{\mathbb{Z}} \to 0.$$

Here $\widehat{\mathbb{Z}}$ is completion of $\mathbb{Z}$ for the topology defined by the subgroups of finite index. Loosely speaking, $\widehat{K^\times}$ can be said to have been obtained from $K^\times$ by completing $\mathbb{Z}$. (See Artin 1951, 9.3, for a detailed discussion of the norm topology on $K^\times$.)

The choice of a prime element π determines a decomposition

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

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

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

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 $\pi \in \mathrm{Nm}(L^\times)$.

ASIDE 1.7. The composite of two totally ramified extensions need not be totally ramified. Consider, for example, $\mathbb{Q}[\sqrt{p}]$ and $\mathbb{Q}[\sqrt{pq}]$ where p and q are odd primes and q is not a square mod p. Then p is totally ramifed in each of these extensions, but not in their composite $\mathbb{Q}[\sqrt{p},\sqrt{q}]$ because it is unramified in the subfield $\mathbb{Q}[\sqrt{q}]$. 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^{al}; there are only the maximal totally ramified extensions K_π, each depending on the choice of π.

Outline of the proof of the main theorems. For $m \geq 1$, let K_m be the unique unramified extension of K of degree m.

In Section 3 of this chapter, we shall prove:

> $(*)$ For each prime element π of K, there is a totally ramified abelian extension $K_\pi = \cup_{n\geq 1} K_{\pi,n}$ of K and a homomorphism
>
> $$\phi_\pi : K^\times \to \mathrm{Gal}(K_\pi \cdot K^{\mathrm{un}}/K)$$
>
> such that
> (a) $\phi_\pi(\pi)|K^{\mathrm{un}} = \mathrm{Frob}_K$;
> (b) $[K_{\pi,n} : K] = (q-1)q^{n-1}$;
> (c) for all m and n, $\phi_\pi(a)|K_{\pi,n}\cdot K_m = \mathrm{id}$ for $a \in (1+\mathfrak{m}^n)\cdot <\pi^m>$.
> (d) for all n, π is a norm from $K_{\pi,n}$.
> Moreover, both $K_\pi \cdot K^{\mathrm{un}}$ and ϕ_π are independent of the choice of π.

Both the fields $K_{\pi,n}$ and the homomorphisms ϕ_π are explicitly constructed.

In Chapter III, we shall prove:

> $(**)$ There exists a homomorphism $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying conditions (a) and (b) of Theorem 1.1.

In the remainder this section, we shall assume these two results, and prove that both Theorem 1.1 and Theorem 1.2 hold, 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.

LEMMA 1.8. *For all $a \in K^\times$, $\phi(a)|K_\pi \cdot K^{\mathrm{un}} = \phi_\pi(a)$.*

PROOF. For any 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 $K' = \cup K_{\pi,n}\cdot K^{\mathrm{un}}$. But the prime elements of K generate $K^\times$ as a multiplicative group ($a \in K^\times$ can be written $a = u\pi^r = (u\pi)\pi^{r-1} = \pi'\pi^{r-1}$), and so this proves the Lemma. □

Now fix a prime element π of K, and let

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

and

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

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

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

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,

$$U_{n,m} = \mathrm{Nm}(K_{n,m}^\times).$$

LEMMA 1.9. *Let L be a finite extension of K, and assume that $\mathrm{Nm}(L^\times)$ is of finite index in $K^\times$. Then $\mathrm{Nm}(L^\times)$ is open in $K^\times$.*

PROOF. Let $U_L = \mathcal{O}_L^\times$. Then U_L is compact, and so $\mathrm{Nm}(U_L)$ is closed in $K^\times$. Since only units have norms that are units, $U_K/\mathrm{Nm}(U_L) \hookrightarrow K^\times/\mathrm{Nm}(L^\times)$. Therefore, $\mathrm{Nm}(U_L)$ is closed of finite index in U_K, and hence is open in U_K (and also in $K^\times$). Thus $\mathrm{Nm}(L^\times)$ contains an open subgroup of $K^\times$, and so is itself open. □

Now let L be a finite abelian extension of K. By assumption $(**)$ $K^\times/\mathrm{Nm}(L^\times) \approx \mathrm{Gal}(L/K)$, and so $\mathrm{Nm}(L^\times)$ is of finite index in $K^\times$. Because it is an open subgroup of finite index in $K^\times$, $\mathrm{Nm}(L^\times)$, contains $U_{n,m}$ for some $n, m \geq 0$. The map

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

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

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

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

This completes the proof that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$ and that $\phi = \phi_\pi$. To complete the proof of the existence theorem, 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 $U_{n,m} = \mathrm{Nm}(K_{n,m})$. Let L be the subfield of $K_{n,m}$ fixed by $\phi_{K_{n,m}/K}(H)$. Then H is the kernel of $\phi : K^\times \to \mathrm{Gal}(L/K)$, and so equals $\mathrm{Nm}(L^\times)$ by $(**)$.

Finally, we prove that there exists at most one homomorphism $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying the conditions (a) and (b) of Theorem 1.1. Let π be a prime element of K. For all n, $\pi \in \mathrm{Nm}(K_{\pi,n}^\times)$, and so condition (b) of the theorem implies that $\phi(\pi)$ acts as the identity on $K_{\pi,n}$. Therefore $\phi(\pi)$ acts as the identity on K_π, and this shows that $\phi(\pi)$ is uniquely determined by the conditions (a) and (b) of the Theorem. Because the prime elements generate the group $K^\times$, this shows that ϕ itself is uniquely determined by the conditions.

EXERCISE 1.10. Use only results from algebraic number theory (e.g., Math 676) 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.

The reader not interested in the explicit generation of K^{ab}, nor in the explicit description of the local Artin map ϕ_K, can skip the rest of this chapter and go directly to Chapters II and III.

2. Lubin-Tate Formal Group Laws

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

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

Addition and multiplication are defined by

$$\begin{aligned} (a_0, a_1, \dots) + (b_0, b_1, \dots) &= (a_0 + b_0, a_1 + b_1, \dots) \\ (a_0, a_1, \dots)(b_0, b_1, \dots) &= (a_0 b_0, \dots, \sum_{i+j=k} a_i b_j, \dots). \end{aligned}$$

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 can not 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 can not do. For the same reason, we can not substitute one power series $g(T)$ into a second $f(T)$ if $g(T)$ has a nonzero constant term. However, if the constant term of $g(T)$ is zero, then $f(g(T))$ is defined—we denote it by $f \circ g$.

LEMMA 2.1. (a) *For all $f \in A[[T]]$, $g, h \in TA[[T]]$, $f \circ (g \circ h) = (f \circ g) \circ h$.*

(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 $a_1 \neq 0$, 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

$$\begin{aligned} a_1b_1 &= 1 \\ a_1b_2 + a_2b_1 &= 0 \\ &\cdots\cdots\cdots \\ a_1b_n + \text{polynomial in } a_2,\dots,a_n,b_1,\dots,b_{n-1} &= 0 \\ &\cdots\cdots\cdots \end{aligned}$$

The first equation shows that, in order for g to exist, a_1 must be invertible. Conversely, 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. 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 any $f = \sum_{i\geq 0} a_iT^i \in A[[T]]$ and any $c \in \mathfrak{m}$, $a_ic^i \to 0$ as $i \to \infty$. Therefore the series $\sum_{i\geq 0} a_ic^i$ converges to an element $f(c) \in \mathfrak{m}$.

We often abbreviate "+terms of degree $\geq m$" to "$+\deg \geq m$".

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

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*. We shall be especially interested in the case that $A = \mathcal{O}_K$, the ring of integers in a nonarchimedean local field K.

REMARK 2.4. 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

$$F(X,0) = X + \deg \geq 2, \qquad F(F(X,0),0) = F(X,0).$$

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

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

EXERCISE 2.5. 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) is redundant.

Let $A = \mathcal{O}_K$, and let $F = \sum_{i,j}^{\infty} a_{ij} X^i Y^j$ be a formal group law over $\mathcal{O}_K$. For any $x, y \in \mathfrak{m}_K$, $a_{ij} x^i y^j \to 0$ 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 any finite extension L of K, and the inclusion $(\mathfrak{m}_K, +_F) \hookrightarrow (\mathfrak{m}_L, +_F)$ is a homomorphism.

EXAMPLE 2.6. (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

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

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

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

(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 J. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986, Chapter IV.

DEFINITION 2.7. 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 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 $f \colon F \to G$ defines a homomorphism

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

for any $L \supset K$.

EXAMPLE 2.8. 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 2.9. (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 with the multiplication $f \circ g$.*

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

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

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 $f, g, h \in \mathrm{End}(F)$,

$$f \circ (g +_F h) \overset{\text{df}}{=} f(F(g(X), h(Y))) = F((f \circ g)(X), (f \circ h)(Y)) = f \circ g +_F f \circ h,$$

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 take $A = \mathcal{O}_K$, the valuation ring in a nonarchimdean local field K, and we choose a prime element π of A.

DEFINITION 2.10. 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 2.11. (a) The polynomial $f(X) = \pi X + X^q$ lies in $\mathcal{F}_\pi$.

(b) Take $K = \mathbb{Q}_p$, $\pi = p$; then

$$f(X) = (1+X)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + pX^{p-1} + X^p \in \mathcal{F}_p.$$

LEMMA 2.12. *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*

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

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

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

The left hand side is

$$f(\phi_r(X_1, \ldots, X_n)) + \pi Q(X_1, \ldots, X_n) + \deg \geq r+2,$$

while the right hand side is

$$\phi_r(g(X_1), \ldots, g(X_n)) + Q(\pi X_1, \ldots, \pi X_n) + \deg \geq r+2.$$

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

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

Thus Q must be the unique polynomial such that

$$\frac{f(\phi_r(X_1,\dots,X_n)) - \phi_r(g(X_1),\dots,g(X_n))}{(\pi^r-1)\pi} = Q + \deg \geq r+2.$$

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 π^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

$$\phi_{r+1} = \phi_r + \deg \geq r+1,$$

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

$$\phi = \phi_r + \deg \geq r+1$$

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

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

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

PROPOSITION 2.13. *For any $f \in \mathcal{F}_\pi$, there is a unique formal group law F_f with coefficients in A admitting f as an endomorphism.*

PROOF. According to Lemma 2.12, 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 2.12 shows that there is only one power series satisfying these conditions. □

EXAMPLE 2.14. Let $K = \mathbb{Q}_p$ and $\pi = p$. Then $f \overset{\text{df}}{=} (1+T)^p - 1 \in \mathcal{F}_p$, and $F \overset{\text{df}}{=} X+Y+XY$ admits f as an endomorphism (see 2.8). Therefore, $F = F_f$.

The F_f's are the *Lubin-Tate formal group laws*. They are exactly the formal group laws that admit an endomorphism reducing mod $\mathfrak{m}$ to the Frobenius $T \mapsto T^q$ and whose derivative at the origin is a prime element of K.

PROPOSITION 2.15. *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 2.12. We have to show that

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

Obviously each $= aX + aY + \deg \geq 2$. 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 2.12 again. □

PROPOSITION 2.16. *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 2.17. *For $f, g \in \mathcal{F}_\pi$, $F_f \approx F_g$.*

PROOF. For any $u \in A^\times$, $[u]_{f,g}$ 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, $[1]_{g,f}$.

COROLLARY 2.18. *For each $a \in A$, there is a unique endomorphism $[a]_f\colon F_f \to F_f$ such that $[a]_f = aT + \deg \geq 2$ 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 2.16 and the obvious fact that $[1]_f = T$. □

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

EXAMPLE 2.19. Let $K = \mathbb{Q}_p$ and $f = (1+T)^p - 1 \in \mathcal{F}_p$, so that $F_f = X+Y+XY$. For any $a \in \mathbb{Z}_p$, define

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

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 2.20. (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 2.21. 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) $[a]_f = aT + \deg \geq 2$, all $a \in A$;
(b) $[a]_f$ commutes with f.

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

3. Construction of the extension K_π of K.

Again $A = \mathcal{O}_K$ 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 K.

According to the discussion in Section 1, there should be a unique totally ramified extension K_π of K 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 m^{th} 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 $m | p^f - 1$. It follows that $K^{\mathrm{un}} = \cup_{p\nmid m} K[\mu_m]$. The Galois group $\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \widehat{\mathbb{Z}}$, and $a \in \widehat{\mathbb{Z}}$ acts K^{un} as follows: for any $\zeta \in \mu_m$ and any integer a_0 sufficiently close to a, $a * \zeta = \zeta^{a_0}$ $\quad (= \mathrm{Frob}_K^a(\zeta))$.

In the case $K = \mathbb{Q}_p$ and $\pi = p$, there is a similar construction for K_π, namely, $(\mathbb{Q}_p)_p = \cup\mathbb{Q}_p[\mu_{p^n}]$—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 $\mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p/p^n\mathbb{Z}_p$, we can regard μ_{p^n} as a cyclic $\mathbb{Z}_p$-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 any K and π.

The valuation $|\cdot|$ on K extends uniquely to any 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 $[\pi]_f^n$.

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

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

in K^{al} with valuation < 1. For simplicity[1], we let f be a polynomial $\pi T + a_2 T^2 + \cdots + T^q$—according to (2.17) it even suffices to take $f = \pi T + T^q$. Then,

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

and

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

From the Newton polygon (see Math 676, 7.35) of $f^{(n)}$, one sees that its roots all have positive ord_K, hence valuation < 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,

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

[1]The p-adic Weierstrass preparation theorem (Washington, Introduction to Cyclotomic Fields, Springer, 1982, 1997, 7.3) implies that any $f \in \mathcal{F}_\pi$ 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 $A[[T]]$.

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

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

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).

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

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

and the sequence $n_1, \dots, n_r$ 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 $q \stackrel{\text{df}}{=} (A:(\pi))$ 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 $A/(\pi^n)$ has order q^n, 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. Moreover, M_n must be cyclic, because otherwise M_1 would not be cyclic. Therefore M_n is a cyclic A-module of order q^n, and every such module is isomorphic to $A/(\pi^n)$. □

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

PROOF. An A-isomorphism $h : F_f \to F_g$ 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 (Math 676, 7.46), and so has q distinct roots, each with valuation < 1. Let $\alpha \in K^{\text{al}}$ have valuation < 1. From the Newton polygon of

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

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

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

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

PROOF. If F is a polynomial, this follows from the fact that τ is a field isomorphism fixing the elements of $\mathcal{O}_K$. We know (Math 676, 7.20 et seqq.) that τ preserves the valuation on L, i.e., $|\tau\alpha| = |\alpha|$ all $\alpha \in L$, and so τ is continuous. Therefore it preserves limits:

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

Let F_m be the polynomial of degree m such that $F = F_m + \deg \geq m+1$. Then

$$\tau(F(\alpha_1, \dots)) = \tau(\lim_{m\to\infty} F_m(\alpha_1, \dots)) = \lim_{m\to\infty} \tau F_m(\alpha_1, \dots) = \lim_{m\to\infty} F_m(\tau\alpha_1, \dots).$$

□

THEOREM 3.6. *Let $K_{\pi,n} = K[\Lambda_n]$, the subfield 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 (Math 676, 7.46) 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 $\mathrm{Sym}(\Lambda_n)$ 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 $\mathrm{Gal}(K[\Lambda_n]/K) \cong (A/\mathfrak{m}^n)^\times$ 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 $f^{[n]}(\pi_n) = f^{[n-1]}(\pi_{n-1}) = \ldots = f(\pi_1) = 0$. Because $f^{[n]}$ is monic of degree $(q-1)q^{n-1} = [K[\pi_n] : K]$, it must be the minimum polynomial of π_n over K. Therefore,

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

In the exceptional case, $K[\Lambda_1] = K$, and so 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

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

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

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

as follows. Let $a \in K^\times$. Because $K_\pi \cap K^{\mathrm{un}} = K$ and $K_\pi \cdot K^{\mathrm{un}} = K^{\mathrm{ab}}$, 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

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

The $^{-1}$ is inserted so the 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.*

Recall that K^{al} is not complete (see Math 676, Problems 10, #4); in fact even K^{un} is not complete. We write $\widehat{K}^{\mathrm{un}}$ for its completion, and B for the valuation ring of $\widehat{K}^{\mathrm{un}}$ (the valuation $|\cdot|$ on K^{un} extends uniquely to $\widehat{K}^{\mathrm{un}}$, 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 $\widehat{K}^{\mathrm{un}}$. For a power series $\theta[[T]] = \sum b_i T^i \in B[[T]]$, $(\sigma\theta)(T) \stackrel{\mathrm{df}}{=} \sum \sigma b_i T^i$.

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) $\theta(T) = \varepsilon T + \deg \geq 2$;
(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*

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

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 (5.7 below). We shall show by induction that the sequence

$$0 \to A/\mathfrak{m}_K^n \to R/\mathfrak{n}^n \xrightarrow{\sigma-1} R/\mathfrak{n}^n \to 0 \quad (*)$$

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

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

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

$$\begin{array}{ccccccccc} 0 & \to & R/\mathfrak{n} & \to & R/\mathfrak{n}^n & \to & R/\mathfrak{n}^{n-1} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & R/\mathfrak{n} & \to & R/\mathfrak{n}^n & \to & R/\mathfrak{n}^{n-1} & \to & 0 \end{array}$$

in which all the vertical maps are induced by $\sigma - 1$. 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 $(*)$ is exact, and, when we pass to the inverse limit over n, the sequence becomes

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

which is therefore exact (see Proposition 5.8 below).

The proofs for $A^\times$ are 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

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

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

$$\sigma\varepsilon T = \varepsilon(uT + \cdots) + \deg \geq 2,$$

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

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

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,

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

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 2.12.

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

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

and, similarly,

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

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

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

Therefore

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

Now the next lemma shows that

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

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 $\widehat{K}^{\mathrm{un}}$ 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 $\widehat{K}^{\mathrm{un}}$ 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 n^{th} root of 1.

(i) 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 t^{th} power of the Frobenius element, and its kernel is $\mathbb{Z}_p^\times \cdot <p^f>$,

(ii) 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 $\{up^m \mid u \equiv 1 \mod p^r, \quad m \in \mathbb{Z}\}$.

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

$$\begin{array}{ccccc} & & \mathbb{Q}_p[\zeta_n] & & \\ & \swarrow & & \searrow & \\ \mathbb{Q}_p[\zeta_{p^r}] & & & & \mathbb{Q}_p[\zeta_m]. \\ & \searrow & & \swarrow & \\ & & \mathbb{Q}_p & & \end{array}$$

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 (Math 676, 7.49 et seqq.) that the i^{th} 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 $i \geq 0$,

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

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

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

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

Let

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

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. *Under the isomorphism* $A^\times/U^{(n)} \xrightarrow{\approx} G$ *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 $u \in U^{(i)} \setminus U^{(i+1)}$. 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 any $i \geq 1$, $\pi_i = \pi\pi_{i+1} + \pi_{i+1}^q = \pi_{i+1}^q(\frac{\pi\pi_{i+1}}{\pi_{i+1}^q} + 1) = \pi_{i+1}^q \times \text{unit}$ because $\text{ord}(\frac{\pi}{\pi_{i+1}^{q-1}}) > 0$. Hence $\pi_{n-i} = \pi_n^{q^i} \times \text{unit}$, 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

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

For $u > 0$,

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

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, Corps Locaux, IV.3, Pptn 14. □

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

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

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, Corps Locaux, 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

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

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

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

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.

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 any 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)

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

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

$$\begin{array}{ccccc}
(G^n : G^{n+1}) & = & ((G/H)^n : (G/H)^{n+1}) & & (G^n \cap H : G^{n+1} \cap H). \\
\leq q & & = q-1 \text{ or } q & &
\end{array}$$

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 $\cap G^n = 1$, 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. Now apply (Math 676, 7.41) 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 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 of degree m. Then there exists a totally ramified abelian extension L_t of K such that*

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

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

$$\mathrm{Gal}(L/K) = <\tau> \times H \quad \text{(direct product)}.$$

for some subgroup H. Let $L_t = L^{<\tau>}$; 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 $L \subset K_\pi \cdot K^{\mathrm{un}}$.

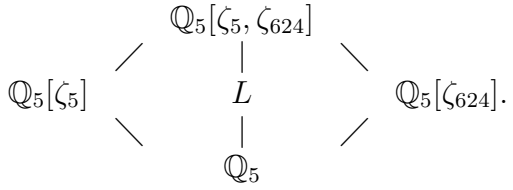
Lemma 4.9 holds with K replaced by K_π. If we apply it to the extension $L \cdot K_\pi/K_\pi$ we find that there exists a totally ramified extension L_t of K_π and an unramified extension L_u of K_π such that

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

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:



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

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

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 $<\sigma^2\tau>$. Then L is a cyclic Galois extension of $\mathbb{Q}_5$ of degree 4. Its maximal unramified subfield

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

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, Local Fields, Cambridge, 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 R. Gold, Local class field theory via Lubin-Tate groups, Indiana Univ. Math. Jour., 30, 1981, 795–798. 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, see M. Rosen, Trans. AMS 265 (1981), 599–605. As Iwasawa points out (Iwasawa 1986, p115), 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 primes 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 Math 676, 4.8). □

PROOF. (of the Kronecker-Weber Theorem; following Cassels, 1986, p236). 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 any 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

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

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

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

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

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

But $(G\colon 1) = [K\colon \mathbb{Q}]$ 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 find 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

$$(I_K^S\colon \operatorname{Nm} I_L^S \cdot i(K_{\mathfrak{m},1})) \leq [L\colon \mathbb{Q}].$$

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 $(m)\infty$.

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 any 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 π, a prime element 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 $f(T) = T^q \mod \mathfrak{m}$. 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.

Notes. The original source for the theory of Lubin-Tate extensions is:

Lubin, J., and Tate, J., Formal complex multiplication in local fields, Ann. of Math., 81 (1965), 380–387.

The theory is also treated by Serre in his article in Cassels and Fröhlich 1967 and in Iwasawa 1986 and Fesenko and Vostokov 1993.

5. Appendix: Infinite Galois Theory and Inverse Limits

We review two topics required for this chapter.

Galois theory for infinite extensions. Fix a field K.

DEFINITION 5.1. 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 5.2. *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 any $\alpha \in \Omega$, the splitting field in Ω of the minimum 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

$$\mathrm{Gal}(\Omega/E), \quad \Omega \supset E \supset K, \quad [E\colon K] < \infty$$

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 5.3. *The group $\mathrm{Gal}(\Omega/K)$ is compact and Hausdorff.*

PROOF. Consider the map

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(\Omega/K) \to \prod \mathrm{Gal}(E/K)$$

where the product runs over all $E \subset \Omega$ with E finite and Galois over K. Proposition 5.2 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

$$\{(\sigma_E) \mid \sigma_{E'}|E = \sigma_E \text{ whenever } E' \supset E\}.$$

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 (σ_E), and $U \cap \mathrm{Im}(\mathrm{Gal}(\Omega/K)) = \varnothing$. □

The topology on $\mathrm{Gal}(\Omega/K)$ is discrete if and only if Ω is a finite extension of K.

THEOREM 5.4. *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, $H \overset{\text{df}}{=} \mathrm{Gal}(\Omega/E)$ 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 $\sigma \mapsto \sigma|\Omega : \mathrm{Gal}(\Omega/K) \to \mathrm{Hom}_K(E, \Omega)$ 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 closed (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 $E = \cup E_i$ where the E_i run over the finite extensions of K contained in E. Correspondingly, $\mathrm{Gal}(\Omega/E) = \cap \mathrm{Gal}(\Omega/E_i)$, 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 any open subgroup U of $\mathrm{Gal}(\Omega/K)$, $UH = UH'$, and so $\bar{H} = \cap UH = \cap UH' = H'$. □

EXAMPLE 5.5. (a) Endow $\mathbb{Z}$ with the topology for which the subgroups of finite index form a fundamental system of neighbourhoods, and let $\widehat{\mathbb{Z}}$ be the completion. Then $\widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$, and $\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}} = \mathbb{Z}/m\mathbb{Z}$ for every m. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$. There is a canonical isomorphism

$$\widehat{\mathbb{Z}} \to \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$$

sending $1 \in \widehat{\mathbb{Z}}$ to the automorphism $x \mapsto x^q$. The extension of $\mathbb{F}_q$ of degree m corresponds to the subgroup $m\widehat{\mathbb{Z}}$ of $\widehat{\mathbb{Z}}$. Let σ be the automorphism of $\mathbb{F}/\mathbb{F}_q$ such that $\sigma(x) = x^q$. For $\alpha \in \widehat{\mathbb{Z}}$, define σ^α to be the element of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ such that, for any m, $\sigma^\alpha|\mathbb{F}_{q^m} = \sigma^a$ where $a \in \mathbb{Z}$ is chosen to be close to α. The above isomorphism sends

α to σ^α. (For a detailed description of $\widehat{\mathbb{Z}}$ and the isomorphism $\widehat{\mathbb{Z}} \to \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$, 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 $u = a_0 + a_1 p + a_2 p^2 + \cdots$, $0 \le a_i < p-1$, and define

$$\zeta_{p^r}^u = \zeta_{p^r}^{a_0 + a_1 p + \cdots a_s p^s}, \text{ any } s > r.$$

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

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

It can be described as follows: if ζ is an n^{th} root of 1 and $u \in \widehat{\mathbb{Z}}^\times$, then

$$\zeta^u = \zeta^m \text{ for any } m \in \mathbb{Z} \text{ with } \quad m \equiv u \mod n.$$

(d) Let $\Omega_p = \cup \mathbb{Q}[\zeta_{p^r}]$, as in (b). Then

$$\mathbb{Z}_p^\times \cong \Delta_p \times C_p$$

where $\Delta_p = (\mathbb{Z}/(p-1))^\times$ 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 $\mathrm{Gal}(\Omega'/\mathbb{Q}) \approx \prod \mathbb{Z}_p \cong \widehat{\mathbb{Z}}$.

(e) For any 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 $\widehat{\mathbb{Z}}$. But any such subgroup is again isomorphic to $\widehat{\mathbb{Z}}$ (because it is again the completion of a subgroup of $\mathbb{Z}$ of finite index). Therefore $\mathrm{Gal}(K \cdot \Omega'/K) \approx \widehat{\mathbb{Z}}$. If we fix an isomorphism, and let K_m be the field corresponding to $m\widehat{\mathbb{Z}}$, 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 5.6. In general, there may exist subgroups of finite index in $\mathrm{Gal}(\Omega/K)$ which are not open[2] (and hence not closed). For example, $K = \mathbb{F}_p((T))$ has a Galois extension Ω such that $\mathrm{Gal}(\Omega/K) = \mathbb{F}_p^{\mathbb{N}}$ (product of an infinite countable number copies of a cyclic group of order p)—see Remark 1.5. Let M be the subgroup of $\mathbb{F}_p^{\mathbb{N}}$ consisting of the elements (a_n) such that $a_n = 0$ for all but finitely many n. Thus M is equal to a *direct sum* of a countable number of copies of a cyclic group of order p. The closure of M is $\mathrm{Gal}(\Omega/K)$, and so any subgroup H of finite index in $\mathrm{Gal}(\Omega/K)$ containing M is not closed (and hence not open).

[2]My recollection is that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ has such subgroups, but I don't know a reference.

Inverse limits. A partially ordered set $(I, \leq)$ is said to be *directed* if, for any $\alpha, \beta \in I$, there exists $\gamma \in I$ such that $\alpha, \beta \leq \gamma$. For example, the set of positive integers ordered by divisibility, $m \leq n \iff m|n$, 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 $\alpha \leq \beta$, a map $\varphi_{\alpha,\beta} : S_\beta \to S_\alpha$ such that

(a) for all $\alpha \in I$, $\varphi_{\alpha,\alpha}$ is the identity map;
(b) for all $\alpha \leq \beta \leq \gamma$ in I, $\varphi_{\alpha,\beta} \circ \varphi_{\beta,\gamma} = \varphi_{\alpha,\gamma}$.

A set S together with, for each $\alpha \in I$, a map $\varphi_\alpha : S \to S_\alpha$ 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, $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$.

EXAMPLE 5.7. The completion $\widehat{R}$ of a discrete valuation ring R is $\cong \varprojlim R/\mathfrak{m}^n$, 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 5.8. *The inverse limit of an inverse system of exact sequences of finite abelian groups is again exact.*

REMARK 5.9. 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, Cohomologie Galoisienne, Springer, 1964, or Shatz, Profinite Groups, Arithmetic, and Geometry, Princeton, 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

$$(g, m) \mapsto gm \colon G \times M \longrightarrow M$$

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 $G \to \mathrm{Aut}(M)$.

A *homomorphism* of G-modules (or a *G-homomorphism)* is a map $\alpha \colon M \to N$ 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

$$\sum n_g g, \quad n_g \in \mathbb{Z}, \quad g \in G,$$

and

$$(\sum n_i g_i)(\sum n'_j g_j) = \sum n_i n'_j (g_i g_j).$$

To endow an abelian group M with a G-module structure is the same as to endow it with a $\mathbb{Z}[G]$-module structure. Thus the category $\mathbf{Mod}_G$ of G-modules can be identified with the category of modules over the ring $\mathbb{Z}[G]$. In particular, $\mathbf{Mod}_G$ is an abelian category.

If M and N are G-modules, then the set $\mathrm{Hom}(M,N)$ of homomorphisms $\varphi : M \to N$ (regarded only as abelian groups) becomes a G-module with the structures

$$\begin{aligned}(\varphi+\varphi')(m) &= \varphi(m)+\varphi'(m)\\ (g\varphi)(m) &= g(\varphi(g^{-1}m)).\end{aligned}$$

Induced modules. Let G be a group and H a subgroup. For an H-module M, we define $\mathrm{Ind}_H^G(M)$ to be the set of maps[1] $\varphi : G \to M$ 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

$$\begin{aligned}(\varphi+\varphi')(x) &= \varphi(x)+\varphi'(x)\\ (g\varphi)(x) &= \varphi(xg).\end{aligned}$$

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 any G-module M and H-module N,*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M,N).$$

(b) *The functor*

$$\mathrm{Ind}_H^G : \mathbf{Mod}_H \to \mathbf{Mod}_G$$

is exact.

PROOF. (a) Given a G-homomorphism $\alpha : M \to \mathrm{Ind}_H^G(N)$, we define $\beta(m) = \alpha(m)(1_G)$, where 1_G is the identity element in G. The various definitions show that, for any $g \in G$,

$$\beta(gm) = (\alpha(gm))(1_G) = (g(\alpha(m)))(1_G) = \alpha(m)(g).$$

Because $\alpha(m) \in \mathrm{Ind}_H^G(M)$, 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 $M \to \mathrm{Ind}_H^G(M)$ 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 $G = \cup_{s\in S} Hs$, 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. □

[1]The φ's are not required to be homomorphisms.

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 a $\mathrm{Ind}^G(M_0)$ for some abelian group M_0.

REMARK 1.3. Let G be a finite group. Then a G-module M is induced if and only if there exists an abelian group $M_0 \subset M$ such that

$$M = \oplus_{g\in G} gM_0 \qquad \text{(direct sum of abeliangroups).}$$

Also, 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

$$g(z \otimes m) = gz \otimes m.$$

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 $G = \cup_{s\in S} Hs$; if $M = \oplus_{g\in G} gM_0$, then $M = \oplus_{h\in H} hM_1$ with $M_1 = \oplus_{s\in S} sM_0$.

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

$$\mathbb{Z}[G] \otimes M_0 \to M, \quad (\textstyle\sum n_g g) \otimes m \mapsto \sum n_g gm.$$

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* $\mathbf{Mod}_G$ *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 $\mathbf{Mod}_G$ is the category of abelian groups, this is proved in the Appendix (Proposition 4.3). 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

$$M \hookrightarrow \mathrm{Ind}^G(M_0), \quad m \mapsto (\text{function } g \mapsto gm).$$

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 this follows from the fact that Ind^G has an exact left adjoint, namely, the forgetful functor (see Proposition 4.5). □

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

$$M \mapsto M^G \colon \mathbf{Mod}_G \to \mathbf{Ab}$$

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. 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 r^{th} *cohomology group of G with coefficients in M* to be

$$H^r(G, M) = \frac{\mathrm{Ker}(d^r)}{\mathrm{Im}(d^{r-1})}.$$

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 $H^0(G, M) \overset{\text{df}}{=} \frac{\mathrm{Ker}(d^0)}{\mathrm{Im}(d^{-1})} = \mathrm{Ker}(d^0)$.

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. For any homomorphism $\alpha : M \to N$ of G-modules and any injective resolutions $M \to I^{\cdot}$ and $N \to J^{\cdot}$, α extends to a map of complexes

$$\begin{array}{ccc} M & \to & I^{\cdot} \\ \downarrow \alpha & & \downarrow \widetilde{\alpha} \\ N & \to & J^{\cdot} \end{array},$$

and the homomorphisms

$$H^r(\widetilde{\alpha}) : H^r(I^{\cdot}) \to H^r(J^{\cdot})$$

are independent of the choice of $\widetilde{\alpha}$. On applying this statement to the identity map $\mathrm{id} : M \to M$, we find that the groups $H^r(G, M)$ are well-defined up to a canonical isomorphism. The general statement then implies 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.

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, 1.8, 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 $\alpha : \mathbb{Z} \to M$ 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

$$\mathrm{Hom}_G(\mathbb{Z}, M) \cong M^G.$$

PROPOSITION 1.11 (SHAPIRO'S LEMMA). [2] *Let H be a subgroup of G. For any H-module N, there is a canonical isomorphism*

$$H^r(G, \mathrm{Ind}_H^G(N)) \to H^r(H, N),$$

all $r \geq 0$.

PROOF. For $r = 0$, the isomorphism is the composite

$$N^H \cong \mathrm{Hom}_H(\mathbb{Z}, N) \overset{1.2}{\cong} \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G(N)) \cong \mathrm{Ind}_H^G(N)^G.$$

Now choose an injective resolution $N \to I^{\cdot}$ of N. On applying the functor Ind_H^G, we obtain an injective resolution $\mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^{\cdot})$ of the G-module $\mathrm{Ind}_H^G(N)$, (because Ind_H^G is exact (1.2) and preserves injectives (proof of 1.5). Hence

$$H^r(G, \mathrm{Ind}_H^G(N)) = H^r((\mathrm{Ind}_H^G(I^{\cdot}))^G) = H^r(I^{\cdot H}) = H^r(H, N).$$

□

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

$$H^r(G, M) = H^r(\{1\}, M_0) = 0 \quad \text{for } r > 0.$$

□

[2] For the origin of this elementary but very useful result see Weil, Oeuvres I, pp 577-578.

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

$$0 \to M^G \to J^G \to N^G \to H^1(G, M) \to 0$$

and

$$H^r(G, N) \xrightarrow{\approx} H^{r+1}(G, M), \quad r \geq 1.$$

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 have already noted, M can be identified with the G-submodule of M_* consisting of maps of the form $g \mapsto gm$, $m \in M$, and we let $M_\dagger = M_*/M$. On applying the above remark to the sequence

$$0 \to M \to M_* \to M_\dagger \to 0$$

we find that

$$H^r(G, M_\dagger) \cong H^{r+1}(G, M), \quad \text{all } r \geq 1.$$

More generally, if

$$0 \to M \to J^1 \to \cdots \to J^s \to N \to 0$$

is exact and $H^r(G, J^i) = 0$ for all $r, i > 0$, then there are canonical isomorphisms

$$H^r(G, N) \xrightarrow{\approx} H^{r+s}(G, M), \quad \text{all } r \geq 1.$$

To prove this, break the sequence up into short exact sequences

$$\begin{gathered} 0 \to M \to J^1 \to N^1 \to 0 \\ 0 \to N^1 \to J^2 \to N^2 \to 0 \\ \cdots \\ 0 \to N^{s-1} \to J^s \to N \to 0 \end{gathered}$$

and note that we have isomorphisms

$$H^r(G, N) \cong H^{r+1}(G, N^{s-1}) \cong H^{r+2}(G, N^{s-2}) \cong \cdots$$

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

$$H^r(G, M) = H^r(J^{\cdot G}).$$

This remark applies to any resolution of M by induced modules.

Description of the cohomology groups by means of cochains. Let M be a G-module. Let P_r, $r \geq 0$, be the free $\mathbb{Z}$-module with basis the $(r+1)$-tuples $(g_0, \dots, g_r)$ of elements of G, endowed the action of G such that

$$g(g_0, \dots, g_r) = (gg_0, \dots, gg_r).$$

Note that P_r is also free as a $\mathbb{Z}[G]$-module, with basis $\{(1, g_1, \dots, g_r) \mid g_i \in G\}$. Define a homomorphism $d_r : P_r \to P_{r-1}$ by the rule

$$d_r(g_0, \dots, g_r) = \sum_{i=0}^{r} (-1)^i (g_0, \dots, \widehat{g_i}, \dots, g_r)$$

where the symbol $\widehat{\cdot}$ means that $\cdot$ is omitted. Let $P.$ 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 $P. \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ 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 any G-module M,*

$$H^r(G, M) \cong H^r(\mathrm{Hom}_G(P., M)).$$

PROOF. This follows from the fact that $P. \to M$ is a projective resolution of M—see Example 4.14. □

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 $\widetilde{C}^r(G, M)$ of φ's satisfying this condition. Such φ are called *homogeneous r-cochains of G with values in M*. The boundary map $\widetilde{d}^r : \widetilde{C}^r(G, M) \to \widetilde{C}^{r+1}(G, M)$ induced by d_r is

$$(\widetilde{d}^r \varphi)(g_0, \dots, g_{r+1}) = \sum (-1)^i \varphi(g_0, \dots, \widehat{g_i}, \dots, g_{r+1}).$$

Proposition 1.16 says that

$$H^r(G, M) \cong \frac{\mathrm{Ker}(\widetilde{d}^r)}{\mathrm{Im}(\widetilde{d}^{r-1})}.$$

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

$$Z^r(G,M) = \operatorname{Ker}(d^r) \qquad \textit{(group of } r\textit{-cocycles)}$$

and

$$B^r(G,M) = \operatorname{Im}(d^{r-1}) \qquad \textit{(group of } r\textit{-coboundaries).}$$

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

$$H^r(G,M) \cong \frac{Z^r(G,M)}{B^r(G,M)}.$$

PROOF. For $\varphi \in \widetilde{C}^r(G,M)$, 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 $\widetilde{C}^r(G,M) \to C^r(G,M)$ transforming the boundary maps in $\widetilde{C}^{\cdot}(G,M)$ into the boundary maps in $C^{\cdot}(G,M)$. □

EXAMPLE 1.18. (a) A map $\varphi\colon G \to M$ is a *crossed homomorphism* if $\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma)$. For example, for any $m \in M$, 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 (i.e, $\sigma m = m$ all $\sigma \in G$, $m \in M$), then a crossed homomorphism is a homomorphism, and zero is the only principal crossed homomorphisms. Thus, in this case,

$$H^1(G,M) = \operatorname{Hom}(G,M).$$

(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

$$1 \to M \to E \xrightarrow{\pi} G \to 1.$$

If $s(\sigma) \in E$ maps to $\sigma \in G$, then we set

$$\sigma m = s(\sigma)\cdot m \cdot s(\sigma)^{-1}, \quad m \in M.$$

Because M is commutative, σm depends only on σ, and so this defines an action of G on M. Note that

$$s(\sigma)\cdot m = \sigma m \cdot s(\sigma), \quad \text{all } \sigma \in G, \quad m \in M.$$

Choose a section s to π, i.e., a map (not necessarily a homomorphism) $s\colon G \to E$ such that $\pi \circ s = \mathrm{id}$. Then $s(\sigma)s(\sigma')$ and $s(\sigma\sigma')$ both map $\sigma\sigma' \in G$, 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

$$[\sigma\varphi(\sigma',\sigma'')]\varphi(\sigma,\sigma'\sigma'') = \varphi(\sigma,\sigma')\varphi(\sigma\sigma',\sigma''),$$

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, and so $H^2(G,M)$ classifies the isomorphism classes of extensions of G by M with a fixed action of G on M.

EXAMPLE 1.19. Let G be a cyclic group of order m, and let M be a G-module. Define $\mathrm{Nm}_G\colon M \to M$ to be $m \mapsto \sum_{\sigma\in G}\sigma m$. Choose a generator σ for G. I claim that $\varphi \mapsto \varphi(\sigma)$ defines an isomorphism

$$H^1(G,M) \to \mathrm{Ker}(\mathrm{Nm}_G)/(\sigma-1)M.$$

Let φ be a crossed homomorphism. Observe that

$$\varphi(1) = \varphi(1\times 1) = 1\varphi(1) + \varphi(1) = 2\varphi(1)$$

and so $\varphi(1) = 0$. Hence,

$$0 = \varphi(\sigma^m) = \varphi(\sigma^{m-1}\sigma) = \sigma\varphi(\sigma^{m-1}) + \varphi(\sigma) = \sigma^2\varphi(\sigma^{m-2}) + \sigma\varphi(\sigma) + \varphi(\sigma) = \mathrm{Nm}_G\,\varphi(\sigma),$$

and so $\varphi(\sigma) \in \mathrm{Ker}(\mathrm{Nm}_G)$. Finally note that

$$\varphi \text{ is principal } \iff \varphi(\sigma) = \sigma m - m \text{ some } m \iff \varphi(\sigma) \in (\sigma-1)M.$$

REMARK 1.20. 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 $\widetilde{\varphi} : G^r \to N$ lifting φ; because $d\varphi = 0$, $d\widetilde{\varphi}$ 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 1.21. *Let L/K be a finite Galois extension with Galois group G. Then $H^1(G,L^\times) = 0$.*

PROOF. Let $\varphi\colon G \to L^\times$ be a crossed homomorphism, i.e.,

$$\varphi(\tau\sigma) = \tau\varphi(\sigma)\cdot\varphi(\tau).$$

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 is an a for which $b \neq 0$. Recall (Math 594f, 5.13):

> (Dedekind's theorem on the independence of characters.) Let L be a field and H a group; then any finite set $\{f_i\}$ of distinct homomorphisms $H \to L^\times$ is linearly independent over L, i.e.,
>
> $$\sum a_i f_i(\alpha) = 0 \quad \text{all } \alpha \in H \implies a_1 = a_2 = \cdots = a_n = 0.$$

When we apply this with $H = L^\times$ and $\sum_{\sigma\in G}\varphi(\sigma)\sigma$, we find that there exists an a such that $b \neq 0$. □

COROLLARY 1.22. *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 $1 = H^1(G, L^\times) = \mathrm{Ker}(\mathrm{Nm}_G)/(\sigma - 1)L^\times$. □

Corollary 1.22 occurs as Satz 90 of Hilbert's book, Die Theorie der algebraischen Zahlkörper, 1894/95, and Theorem 1.21 is Emmy Noether's generalization. Both are usually referred to as Hilbert's Theorem 90.

PROPOSITION 1.23. *Let L/K be a finite Galois extension with Galois group G. Then $H^r(G, L) = 0$ for all $r > 0$.*

PROOF. The Normal Basis Theorem (see below) states that $L \approx K[G]$ as a G-module. But $K[G] = \mathrm{Ind}_{\{1\}}^G K$, and so $H^r(G, L) = H^r(\{1\}, K) = 1$ for $r > 0$. □

LEMMA 1.24 (NORMAL BASIS THEOREM). *Let L/K be a finite Galois extension (of arbitrary fields) with Galois group G. Then there exists an $\alpha \in L$ such that $\{\sigma\alpha \mid \sigma \in G\}$ is a basis*[3] *for L as a K-vector space.*

PROOF. We give two proofs, the first of which assumes that K is infinite and the second that G is cyclic. Since every finite Galois extension of a finite field is cyclic, this covers all cases.

Assume that K is infinite. This has the consequence that, for $f(X_1, \dots, X_m) \in K[X_1, \dots, X_m]$,

$$f(a_1, \dots, a_m) = 0 \text{ all } a_1, \dots, a_m \in K \implies f(X_1, \dots, X_m) = 0.$$

[3] A basis of this form is said to *normal*.

This can be proved by induction. For $m = 1$ it follows from the fact that a nonzero polynomial in one variable has only finitely many roots. For $m > 1$, write

$$f = \sum c_i(X_1, \dots, X_{m-1})X_m^i.$$

When we substitute values $a_1, \dots, a_{m-1}$ for the $X_1, \dots, X_{m-1}$, the resulting polynomial in X_m has infinitely many roots, and therefore each of its coefficients is zero, i.e., $c_i(a_1, \dots, a_{m-1}) = 0$. Since this holds for all $(a_1, \dots, a_{m-1})$, the induction hypothesis shows that $c_i(X_1, \dots, X_{m-1})$ is zero.

Now number the elements of G as $\sigma_1, \dots, \sigma_m$ (with $\sigma_1 = 1$).

Let $f(X_1, \dots, X_m) \in K[X_1, \dots, X_m]$ have the property that

$$f(\sigma_1\alpha, \dots, \sigma_m\alpha) = 0$$

for all $\alpha \in L$. For a basis $\alpha_1, \dots, \alpha_m$ of L over K, let

$$g(Y_1, \dots, Y_m) = f(\textstyle\sum_{i=1}^m Y_i\sigma_1\alpha_i, \sum_{i=1}^m Y_i\sigma_2\alpha_i, \dots).$$

The hypothesis on f implies that $g(a_1, \dots, a_m) = 0$ for all $a_i \in K$, and so $g = 0$. But the matrix $(\sigma_i\alpha_j)$ is invertible (see Math 676, 2.25). Since g is obtained from f by an invertible linear change of variables, f can be obtained from g by the inverse linear change of variables. Therefore it also is zero.

Write $X_i = X(\sigma_i)$, and let $A = (X(\sigma_i\sigma_j))$, i.e., A is the $m \times m$ matrix having X_k in the $(i, j)^{th}$ place if $\sigma_i\sigma_j = \sigma_k$. Let $f(X_1, \dots, X_m) = \det(A)$. Then $f(1, 0, \dots, 0)$ is the determinant of a matrix having exactly one 1 in each row and each column and its remaining entries 0. Hence the rows of the matrix are a permutation of the rows of the identity matrix, and so its determinant is ± 1. Hence f is not identically zero, and so there exists an $\alpha \in L^\times$ such that $f(\sigma_1\alpha, \dots, \sigma_m\alpha)$ $(= \det(\sigma_i\sigma_j\alpha))$ is nonzero. Now suppose

$$\textstyle\sum_{j=1}^m a_j\sigma_j\alpha = 0$$

for some $a_j \in K$. On applying $\sigma_1, \dots, \sigma_m$ successively, we obtain a system of m-equations

$$\textstyle\sum a_j\sigma_i\sigma_j\alpha = 0$$

in the m "unknowns" a_j. Because this system of equations is nonsingular, the a_j's are zero. We have shown that the $\sigma_j\alpha$'s are linearly independent over K. This completes the proof of the lemma in the case that K is infinite.

Now assume that G is cyclic generated, say, by an element σ_0 of order n. We regard σ_0 as an endomorphism of L considered as a K-vector space. The characteristic polynomial $P(X)$ of σ_0 is the monic polynomial in $K[X]$ of least degree such that $P(\sigma_0) = 0$ (as an endomorphism of L). It has the property that it divides every polynomial $Q(X) \in K[X]$ such that $Q(\sigma_0) = 0$. Since $\sigma_0^n = 1$, $P(X)$ divides $X^n - 1$. On the other hand, Dedekind's theorem on the independence of characters (see above) implies that $\mathrm{id}, \sigma_0, \dots, \sigma_0^{n-1}$ are linearly independent over K, and so $\deg P(X) > n - 1$. We conclude that $P(X) = X^n - 1$. Therefore, as a $K[X]$-module with X acting as σ_0, L is isomorphic to $K[X]/(X^n - 1)$. For any generator α of L as a $K[X]$-module, $\alpha, \sigma_0\alpha, \dots, \sigma_0\alpha^{n-1}$ is a K-basis for L. □

The cohomology of products. A product $M = \prod M_i$ 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 any G-modules M_i,*

$$H^r(G, \prod M_i) = \prod H^r(G, M_i).$$

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

$$\mathrm{Hom}_G(\cdot, I) \cong \Pi_i \mathrm{Hom}_G(\cdot, I_i)$$

is exact. Let $M_i \to I_i^{\cdot}$ be an injective resolution of M_i. Then $\prod M_i \to \prod I_i^{\cdot}$ is an injective resolution of $\prod M_i$, and

$$H^r(G, \prod M_i) = H^r((\prod I_i^{\cdot})^G) = H^r(\prod (I_i^{\cdot G})) = \prod H^r(I_i^{\cdot G}) = \prod H^r(G, M_i).$$

□

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

$$\alpha\colon G' \to G, \quad \beta\colon M \to M'$$

are said to be *compatible* if

$$\beta(\alpha(g)m) = g(\beta(m)).$$

Then (α, β) defines a homomorphism of complexes

$$C^{\cdot}(G, M) \to C^{\cdot}(G', M'), \quad \varphi \mapsto \beta \circ \varphi \circ \alpha^r,$$

and hence homomorphisms

$$H^r(G, M) \to H^r(G', M').$$

EXAMPLE 1.27. (a) Let H be a subgroup of G. For any H-module M, the map

$$\beta : \mathrm{Ind}_H^G(M) \to M, \quad \beta(\varphi) = \varphi(1),$$

is compatible with the inclusion $H \hookrightarrow G$, and the induced homorphism

$$H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(H, M)$$

is the isomorphism in Shapiro's Lemma.

(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*

$$\mathrm{Res}\colon H^r(G, M) \to H^r(H, M).$$

They can also be constructed as follows: let $M \to \mathrm{Ind}_H^G(M)$ be the homomorphism sending m to the map φ_m with $\varphi_m(g) = gm$; the restriction map is the composite

of the homomorphism it defines on cohomology with the isomorphism in Shapiro's Lemma,

$$H^r(G,M) \to H^r(G,\mathrm{Ind}_H^G(M)) \xrightarrow{\approx} H^r(H,M).$$

(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*

$$\mathrm{Inf}\colon H^r(G/H,M^H) \to H^r(G,M).$$

(d) For any $g_0 \in G$, the homomorphisms $\alpha\colon G \to G$, $\sigma \mapsto g_0\sigma g_0^{-1}$, and $\beta\colon M \to M$, $m \mapsto g_0^{-1}m$, 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

$$m \mapsto g^{-1}m\colon M^G \to M^G,$$

which is obviously the identity. Let $r > 0$, and suppose the statement is known for $r-1$. From the sequence

$$0 \to M \to M_* \to M_\dagger \to 0, \quad M_* = \mathrm{Ind}^G(M_0),$$

in (1.13) we obtain a diagram

$$\begin{array}{ccccc} H^{r-1}(G,M_*) & \to & H^{r-1}(G,M_\dagger) & \to & H^r(G,M) \to 0 \\ \downarrow & & \downarrow & & \downarrow \\ H^{r-1}(G,M_*) & \to & H^{r-1}(G,M_\dagger) & \to & H^r(G,M) \to 0. \end{array}$$

The 0s 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 any 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, $G = \cup_{s\in S} sH$. Let M be a G-module. For any $m \in M^H$,

$$\mathrm{Nm}_{G/H}\, m \stackrel{\mathrm{df}}{=} \sum_{s\in S} sm$$

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*

$$\mathrm{Cor}\colon H^r(H,M) \to H^r(G,M)$$

for all r as follows: for any G-module M, there is a canonical homomorphism of G-modules

$$\varphi \mapsto \textstyle\sum s\varphi(s^{-1}) : \mathrm{Ind}_H^G M \to M;$$

the map on cohomology which it defines, when composed with the isomorphism in Shapiro's lemma, gives Cor,

$$H^r(H,M) \xrightarrow{\approx} H^r(G,\operatorname{Ind}_H^G M) \longrightarrow H^r(G,M).$$

PROPOSITION 1.30. *Let H be a subgroup of G of finite index. The composite*

$$\operatorname{Cor}\circ\operatorname{Res}\colon H^r(G,M) \longrightarrow H^r(G,M)$$

is multiplication by $(G\colon H)$.

PROOF. The map $\operatorname{Cor}\circ\operatorname{Res}$ is the map on cohomology defined by the composite of

$$M \to \operatorname{Ind}_H^G(M) \to M, \quad m \mapsto \varphi_m \mapsto \sum_s s\varphi_m(s^{-1}) = \sum_s m = (G:H)m.$$

□

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. □

For any abelian group A and prime 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 any G-module M, the restriction map*

$$\operatorname{Res} : H^r(G,M) \to H^r(G_p,M)$$

is injective on the p-primary component of $H^r(G,M)$.

PROOF. By definition, $(G : H)$ is not divisible by p. The composite

$$\operatorname{Cor}\circ\operatorname{Res} : H^r(G,M) \to H^r(G_p,M) \to H^r(G,M)$$

is multiplication by $(G : H)$, 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 $H^i(H, M) = 0$ for all i with $0 < i < r$, 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 $H^r(H, M)$ 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 $G/H \to M^H$. This shows that the sequence is exact at $H^1(G, M)$. The exactness at $H^1(G/H, M^H)$ is even easier to prove.

Now assume that $r > 1$ and that the statement is true for $r-1$. Consider the exact sequence (1.13)

$$0 \to M \to M_* \to M_\dagger \to 0.$$

Then

$$H^i(H, M_\dagger) \cong H^{i+1}(H, M), \quad i > 0,$$

and so $H^i(H, M_\dagger) = 0$ for $0 < i \leq r - 1$. 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. For the experts, the Hochschild-Serre (alias Lyndon) spectral sequence has the form

$$H^r(G/H, H^s(H, M)) \implies H^{r+s}(G, M).$$

It defines a filtration on each of the groups $H^r(G, M)$, and expresses each quotient of the filtration in terms of the cohomologies of G/H and H. It implies the above proposition. Without any hypotheses, one can show that there is an exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H} \to$$
$$H^2(G/H, M^H) \to H^2(G, M)^* \to H^1(G/H, H^1(H, M))$$

where $H^2(G, M)^* = \text{Ker}(\text{Res}\colon H^2(G, M) \to H^2(H, M))$.

EXAMPLE 1.36. Let Ω/K and L/K be Galois extensions, with $L \subset \Omega$. Then $H \overset{\text{df}}{=} \text{Gal}(\Omega/L)$ is a normal subgroup of $G \overset{\text{df}}{=} \text{Gal}(\Omega/K)$. According to Proposition 1.21, $H^1(H, \Omega^\times) = 0$, 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. 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 1.37. *There exists one and only one family of bi-additive pairings*

$$(m, n) \mapsto m \cup n : H^r(G, M) \times H^s(G, N) \longrightarrow H^{r+s}(G, M \otimes N),$$

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*

$$(m, n) \mapsto m \otimes n \colon M^G \otimes N^G \longrightarrow (M \otimes N)^G;$$

(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 $H^r(G, M'') \longrightarrow H^{r+1}(G, M')$ or $H^{r+s}(G, M'' \otimes N) \longrightarrow H^{r+s+1}(G, M' \otimes N)$.
(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. 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 cocycles φ and ψ; then $m \cup n$ is represented by the cocycle

$$(g_1, \dots, g_{r+s}) \mapsto \varphi(g_1, \dots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \cdots, g_{r+s}).$$

□

PROPOSITION 1.38. *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 $x \in H^r(G, M)$, $y \in H^s(G, N)$;*
(c) $\operatorname{Res}(x \cup y) = \operatorname{Res}(x) \cup \operatorname{Res}(y)$;
(d) $\operatorname{Cor}(x \cup \operatorname{Res} y) = \operatorname{Cor}(x) \cup y$.

PROOF. In each case, one verifies the formula when $x, y, \dots$ 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 Cassels and Fröhlich, 1967, IV, Proposition 9. □

A pairing

$$x, y \mapsto (x, y) : M \times N \to P$$

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 also be referred to as cup-product pairings.

2. Homology; the Tate Groups

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

$$M \mapsto M_G \colon Mod_G \to Ab$$

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.

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, any 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, i.e., that $\mathbf{Mod}_G$ has enough projectives.

Let M be a G-module, and choose a projective resolution

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to M \to 0$$

of M. The complex

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \to (P_0)_G \to 0$$

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. $H_0(G,M) = M_G$, 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 $P_\cdot \to M$ and $Q_\cdot \to N$ be projective resolutions of G-modules M and N. Then any homomorphism $\alpha : M \to N$ of G-modules extends to a morphism of complexes

$$\begin{array}{ccc} P_\cdot & \to & M \\ \downarrow \widetilde{\alpha} & & \downarrow \alpha \\ Q_\cdot & \to & N \end{array},$$

and the homomorphisms

$$H_r(\widetilde{\alpha}) : H_r(P_\cdot) \to H_r(Q_\cdot)$$

are independent of the choice of $\widetilde{\alpha}$. When we apply this to the identity map $\mathrm{id} : M \to M$, we see that the groups $H_r(G,M)$ are well-defined up to a canonical isomorphism. The general statement then implies 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

$$\cdots \to H_r(G,M) \to H_r(G,M'') \to H_{r-1}(G,M') \to \cdots \to H_0(G,M'') \to 0.$$

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 properties (2.1–2.4) determine the functors $H^r(G,\cdot)$.

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

$$\mathbb{Z}[G] \to \mathbb{Z}, \quad \textstyle\sum n_g g \mapsto \sum n_g.$$

Its kernel is called the *augmentation ideal* I_G. Clearly I_G is a free $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ with basis $\{g-1 \mid g \in G\}$, and

$$M/I_G M = M_G \overset{\text{df}}{=} H_0(G,M).$$

Consider the exact sequence:

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

The G-module $\mathbb{Z}[G]$ is projective (because it is free, hence projective, as a $\mathbb{Z}[G]$-module), and so $H_1(G,\mathbb{Z}[G]) = 0$. Therefore we obtain an exact sequence of homology groups

$$0 \to H_1(G,\mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G\mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

The middle map is induced by the inclusion $I_G \hookrightarrow \mathbb{Z}[G]$, and so is zero. Therefore the sequence shows that

$$H_1(G,\mathbb{Z}) \xrightarrow{\approx} I_G/I_G^2 \qquad (*)$$

and

$$\mathbb{Z}[G]_G = \mathbb{Z}$$

i.e., $\mathbb{Z}$ is the largest quotient of $\mathbb{Z}[G]$ on which G acts trivially. Note that $I_G^2 \overset{\text{df}}{=} I_G \cdot I_G$ is the $\mathbb{Z}$-submodule of M 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*

$$\frac{G}{G^c} \to \frac{I_G}{I_G^2}.$$

PROOF. Consider the map

$$g \mapsto (g-1) + I_G \colon G \to I_G/I_G^2.$$

This is a homomorphism because

$$gg' - 1 = (g-1)(g'-1) + (g-1) + (g'-1) \equiv (g-1) + (g'-1) \mod I_G^2.$$

Since I_G/I_G^2 is commutative, the map factors through G^{ab}. To prove it is an isomorphism, we construct an inverse. Recall that I_G is freely generated by the elements $g-1$. Consider the homomorphism $I_G \to G^{\text{ab}}$ 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*

$$H_1(G,\mathbb{Z}) \to G^{\text{ab}}.$$

PROOF. Combine the isomorphism $(*)$ with that in the lemma. □

REMARK 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 (J. Rosenberg, Algebraic K-Theory and Its Applications, Springer, 1994, 5.1.16, 5.1.27). Therefore the proposition simply states that $H_1(BG, \mathbb{Z})$ is the maximal abelian quotient of the fundamental group of BG.

The Tate groups. For the remainder of this section, we require G to be finite. For any G-module M, the *norm map* $\mathrm{Nm}_G\colon M \to M$ 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 gg' and $g'g$, and so

$$\mathrm{Nm}_G(g'm) = \mathrm{Nm}_G(m) = g'(\mathrm{Nm}_G(m)).$$

Hence

$$I_G M \subset \operatorname{Ker} \mathrm{Nm}_G, \qquad \operatorname{Im}(\mathrm{Nm}_G) \subset M^G.$$

As $H_0(G, M) = M/I_G M$ and $H^0(G, M) = M^G$, it follows that Nm_G defines a homomorphism

$$\mathrm{Nm}_G : H_0(G, M) \to H^0(G, M).$$

For any short exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

we get a diagram

$$\begin{array}{ccccccccccc}
H_1(G,M'') & \longrightarrow & H_0(G,M') & \longrightarrow & H_0(G,M) & \longrightarrow & H_0(G,M'') & \longrightarrow & 0 & & \\
 & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & & & \\
0 & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,M'') & \longrightarrow & H^1(G,M') & \longrightarrow & \cdots
\end{array}$$

On applying the extended snake lemma (4.1) to the middle part of the diagram, we get a (very) long exact sequence

$$\cdots \to H^r_T(G, M') \to H^r_T(G, M) \to H^r_T(G, M) \xrightarrow{\delta} H^{r+1}_T(G, M) \to \cdots \quad -\infty < r < \infty.$$

where

$$H^r_T(G, M) \overset{\text{df}}{=} \begin{cases} H^r(G, M) & r > 0 \\ M^G/\mathrm{Nm}_G(M) & r = 0 \\ \operatorname{Ker}(N_G)/I_G M & r = -1 \\ H_{-r-1}(G, M) & r < -1. \end{cases}$$

Since it causes no ambiguity, we often omit the subscript T when $r \neq 0$.

Most of the results we proved for the groups $H^r(G, M)$ with $r \geq 0$ extend to all r. For example, Shapiro's lemma and its consequences are true, and the maps we defined in (1.27) and (1.29) extend to all the Tate cohomology groups. Specifically, there are canonical homomorphisms:

Res: $H^r_T(G, M) \to H^r_T(H, M)$ (H a subgroup of G);

Cor: $H^r_T(H, M) \to H^r_T(G, M)$ (H a subgroup of G);

Inf: $H^r_T(G/H, M^H) \to H^r_T(G, M)$ (H a normal subgroup of G).

Moreover, there is a natural action of G/H on M^H.

The composite Res ∘ 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 m for all r.

Note that $H_T^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) \cong G/G^c$.

PROPOSITION 2.9. *Let H be a subgroup of G.*

(a) *The map* Cor : $H^{-2}(H, \mathbb{Z}) \to H^{-2}(G, \mathbb{Z})$ *corresponds to the map* $H/H^c \to G/G^c$ *induced by the inclusion* $H \hookrightarrow G$.
(b) *The map* Res : $H^{-2}(G, \mathbb{Z}) \to H^{-2}(H, \mathbb{Z})$ *corresponds to the Verlagerung map* $G/G^c \to H/H^c$.

PROOF. See E. Weiss, Cohomology of Groups, Academic Press, 1969, 3-5. □

There is a uniform explicit description of all the groups $H^r(G, M)$. In fact, there is an explicit complex $L.$ of G-modules (infinite in both directions) such that

$$H_T^r(G, M) = H^r(\mathrm{Hom}_G(L., M)).$$

For $r > 0$ this leads directly to the description we gave above of $H^r(G, M)$ in terms of inhomogeneous cocycles and coboundaries.

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.

The cohomology of finite cyclic groups. We first compute the cohomology of $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{Q}/\mathbb{Z}$, each regarded as a G-module with the trivial action.

LEMMA 2.10. *For any finite group G,*

(a) $H_T^r(G, \mathbb{Q}) = 0$ *all r ($\mathbb{Q}$ regarded as a G-module with the trivial action);*
(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 integers m, multiplication by $m\colon \mathbb{Q} \to \mathbb{Q}$ is an isomorphism. Therefore the map $H^r(m) : H_T^r(G, \mathbb{Q}) \to H_T^r(G, \mathbb{Q})$, which is also multiplication by m, is an isomorphism. Now take $m = (G\colon 1)$. Then multiplication by m on $H_T^r(G, M)$ is both zero (see 1.30) and an isomorphism—this is possible only if $H_T^r(G, M) = 0$.

(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 1.18), but, because $\mathbb{Z}$ is torsion-free, there are no nonzero such homomorphisms.

(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,

$$H_T^0(G,M) = \frac{\mathrm{Ker}(\sigma-1)}{\mathrm{Im}(\mathrm{Nm}_G)}$$

and

$$H_T^{-1}(G,M) = H_0(G,M) = \frac{\mathrm{Ker}(\mathrm{Nm}_G)}{\mathrm{Im}(\sigma-1)}.$$

Note that $H_T^{-1}(G,M) = H_T^1(G,M)$ (see 1.19). In fact, the cohomology groups are periodic with period 2.

PROPOSITION 2.11. *Let G be a cyclic group of finite order, and let M be a G-module. Then, for all r, there exists an isomorphism*

$$H_T^r(G,M) \xrightarrow{\approx} H_T^{r+2}(G,M)$$

depending only on the choice of a generator for G.

PROOF. Let σ generate G. Then the sequence

$$0 \to \mathbb{Z} \xrightarrow{m\mapsto m1_G} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\sigma^i\mapsto 1} \mathbb{Z} \to 0$$

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 $H^r(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} M) = 0$ for all r. Therefore (see 1.13), the sequence defines isomorphisms

$$H_T^r(G,M) \xrightarrow{\approx} H_T^{r+2}(G,M)$$

for all r. □

REMARK 2.12. Let γ be the element of $H^2(G,\mathbb{Z})$ corresponding under the isomorphism $H^2(G,\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ to the map sending the chosen generator σ of G to $1/m$. Then the map $H^r(G,M) \to H^{r+2}(G,M)$ is $x \mapsto x \cup \gamma$.

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*

$$h(M) = \frac{\#H_T^0(G,M)}{\#H_T^1(G,M)}.$$

PROPOSITION 2.13. *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,

$$0 \to K \to H^0(M') \to H^0(M) \to H^0(M'') \to H^1(M') \to H^1(M) \to H^1(M'') \to K' \to 0$$

where

$$K = \operatorname{Coker}(H^{-1}(M) \to H^{-1}(M'')) \approx \operatorname{Coker}(H^1(M) \to H^1(M'')) \approx K'.$$

The first statement is now obvious, and the second follows from the next lemma. □

LEMMA 2.14. *Let*

$$0 \to A_0 \to A_1 \to \cdots \to A_r \to 0$$

be a finite sequence of finite groups. Then

$$\frac{\#A_0 \# A_2 \cdots}{\#A_1 \# A_3 \cdots} = 1.$$

PROOF. For a short exact sequence, that is, $r = 3$, this is obvious, but any exact sequence can be broken up into short exact sequences,

$$0 \to A_0 \to A_1 \to C_1 \to 0$$

$$0 \to C_1 \to A_2 \to C_2 \to 0$$

$$\cdots$$

$$0 \to C_{r-1} \to A_{r-1} \to A_r \to 0.$$

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

$$1 = \frac{\#A_0 \# C_1}{\#A_1} = \frac{\#A_0 \# A_2}{\#A_1 \# C_2} = \cdots .$$

□

PROPOSITION 2.15. *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

$$0 \to H^{-1}(M) \to M_G \xrightarrow{\mathrm{Nm}_G} M^G \to H^0(M) \to 0$$

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 $H^{-1}(M)$ and $H^0(M)$ have the same order. □

COROLLARY 2.16. *Let $\alpha\colon M \to N$ 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.

THEOREM 2.17. *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 $H^r(G,M) = 0$ 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 $\mathrm{Nm}_H(z) = x$. 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 (1.13)

$$0 \to M \to M_* \to M_\dagger \to 0.$$

Because M_* is induced as an H-module (see 1.3), $H^r(H,M_*) = 0$ for all r and all subgroups H of G, and so

$$H^r(H,M) = H^{r-1}(H,M_\dagger)$$

for all r and all H. Therefore, $M_\dagger$ satisfies the hypotheses of the theorem, and so (by what we have proved) $H^r(G,M_\dagger) = 0$ for $r \geq 0$. In particular,

$$0 = H^0(G,M_\dagger) = H^{-1}(G,M).$$

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 2.18. *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

$$H^r(G,\mathbb{Z}) \to H^{r+2}(G,C)$$

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 $H^r(H,C)$ 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

$$\begin{aligned}H^1(H,I_G) &\cong H^0(H,\mathbb{Z}) \cong \mathbb{Z}/(H:1)\mathbb{Z},\\ H^2(H,I_G) &\cong H^1(H,\mathbb{Z}) = 0\end{aligned}$$

Define α to be the additive map $C(\varphi) \to \mathbb{Z}[G]$ such that

$$\begin{aligned}\alpha(c) &= 0 \text{ for all } c \in C(\varphi)\\ \alpha(x_\sigma) &= \sigma - 1.\end{aligned}$$

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 2.17 that $H^r(H, C(\varphi)) = 0$ for all r. On splicing the two short exact sequences together, we obtain an exact sequence

$$0 \to C \to C(\varphi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

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 2.19. 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

$$H^r(G, M) \to H^{r+2}(G, M \otimes C).$$

REMARK 2.20. The map $H^r(G, \mathbb{Z}) \to H^{r+2}(G, C)$ is cup-product with the chosen element $\gamma \in H^2(G, C)$.

EXAMPLE 2.21. 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 $u_{L/K}$, called the *(local) fundamental class*. Moreover, in a tower of fields $L \supset K' \supset K$, $\mathrm{Res}(u_{L/K}) = u_{L/K'}$. Since we know $H^1(G, L^\times) = 0$ (Hilbert's Theorem 90), Tate's theorem shows that cup-product with $u_{L/K}$ is an isomorphism

$$G^{\mathrm{ab}} = H^{-2}(G, \mathbb{Z}) \to H^0(G, L^\times) = K^\times / \operatorname{Nm} L^\times.$$

The reverse map is the local Artin map. The global Artin map can be obtained by a similar argument.

3. 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 3.1. *For any direct system of exact sequences*

$$A_i \longrightarrow B_i \longrightarrow C_i,$$

the sequence

$$\varinjlim A_i \longrightarrow \varinjlim B_i \longrightarrow \varinjlim C_i$$

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[4] 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 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

$$G \times M \longrightarrow M$$

is continuous when M is endowed with the discrete topology, i.e., the topology in which every subset is open. Equivalent conditions:

(a) $M = \cup M^H$, H runs through the open subgroups of G;
(b) 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 $H^r_{\mathrm{cts}}(G, M)$ by taking injective resolutions, just as before. Moreover, the groups can be calculated using *continuous* cocycles: 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 $B^r_{\mathrm{cts}}(G, M) = \mathrm{Im}(d^{r-1})$.

[4]Following Bourbaki, I require compact spaces to be Hausdorff.

Let $\varphi : G^r \to M$ be a continuous r-cochain. Then $\varphi(G^r)$ is compact, but M is discrete, and so $\varphi(G^r)$ is finite, and hence 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 $H_1 = \cap_{m\in\varphi(G^r)}H(m)$. 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.

PROPOSITION 3.2. *The maps* $\text{Inf} : H^r(G/H, M^H) \to H^r_{\text{cts}}(G, M)$ *realize* $H^r_{\text{cts}}(G, M)$ *as the direct limit of the groups* $H^r(G/H, M^H)$ *as* H *runs through the open normal subgroups* H *of* G*:*

$$\varinjlim H^r(G/H, M^H) = H^r_{\text{cts}}(G, M).$$

Explicitly, the statement means that each element of $H^r_{\text{cts}}(G, M)$ 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 $H^r_{\text{cts}}(G, M)$, then they map to the same element in $H^r(G/H'', M^{H''})$ for some open subgroup $H'' \subset H \bigcap H'$.

PROOF. The above argument shows that

$$C^r_{\text{cts}}(G, M) = \varinjlim C^r(G/H, M^H).$$

The proposition then follows from the fact that passage to the direct limit commutes with the formation of kernels and cokernels, and hence with the formation of cohomology. □

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 3.3. *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 $M = \bigcup M_i$, any 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 3.1 shows that

$$H^r(C^{\cdot}(G, M)) = \varinjlim H^r(C^{\cdot}(G, M_i)).$$

□

ASIDE 3.4. (For the experts.) Let G be a profinite group, let $\mathbf{M}(G)$ be the category of all G-modules, and $\mathbf{C}(G)$ the category of discrete G-modules. Then $\mathbf{C}(G)$ is a full subcategory of $M(G)$. Moreover, there is a functor

$$M \mapsto M^* \stackrel{\text{df}}{=} \bigcup_{H \text{ open in } G} M^H \colon \mathbf{M}(G) \to \mathbf{C}(G).$$

Clearly,

$$\text{Hom}_G(M, N^*) = \text{Hom}_G(M, N)$$

for M a discrete G-module. The inclusion functor $i \colon \mathbf{C}(G) \to \mathbf{M}(G)$ 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 $\mathbf{C}(M)$ 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 S. MacLane, Origins of the cohomology of groups, Enseign. Math. (2) 24, 1978, 1–29.

Our proof of Tate's theorem follows Tate's original proof (Ann. of Math., 56 (1952), 294–297). 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, Princeton Univ. Press, 1956, following Tate's ideas.

The best source for the above material is Serre 1961, Part 3. There is a somewhat abbreviated version of the same material in Cassels and Fröhlich 1967, Chapter IV. See also Iyanaga 1975, Chapter I, and E. Weiss, Cohomology of Groups, Academic Press, 1969. For the cohomology of profinite groups, see J.-P. Serre, Cohomologie Galoisienne, Springer, 1964, and S. Shatz, Profinite Groups, Arithmetic, and Geometry, Princeton University Press, 1972.

4. Appendix: Some Homological Algebra

Some exact sequences. [5]

[5]Based on F. Lemmermeyer, The Snake Lemma.

LEMMA 4.1 (THE EXTENDED SNAKE LEMMA). *Every commutative diagram of abelian groups*

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 \longrightarrow A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

with exact rows gives rise to an exact sequence

$$0 \to \operatorname{Ker} f \to \operatorname{Ker}\alpha \to \operatorname{Ker}\beta \to \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha \to \operatorname{Coker}\beta \to \operatorname{Coker}\gamma \to \operatorname{Coker} g' \to 0.$$

PROOF. Except for the first and last terms, this standard. A small diagram chase shows that $\operatorname{Ker} f \subset \operatorname{Ker}(\alpha)$, from which exactness at $\operatorname{Ker}\alpha$ follows. The proof of exactness at $\operatorname{Coker}\gamma$ is similarly straightforward. □

LEMMA 4.2 (KERNEL-COKERNEL LEMMA). *Every pair of homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ of abelian groups gives rise to an exact sequence*

$$0 \to \operatorname{Ker} f \to \operatorname{Ker} g\circ f \xrightarrow{f} \operatorname{Ker} g \to \operatorname{Coker} f \to \operatorname{Coker} g\circ f \to \operatorname{Coker} g \to 0.$$

PROOF. Apply the extended snake lemma to

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \longrightarrow & \operatorname{Coker} f & \longrightarrow & 0 \\ \downarrow{\scriptstyle g\circ f} & & \downarrow{\scriptstyle g} & & \downarrow & & \\ 0 \longrightarrow C & \xrightarrow{\mathrm{id}} & C & \longrightarrow & 0 & & \end{array}$$

□

The language of category theory. A *category* $\mathbf{C}$ consists of a nonempty class $\operatorname{ob}(\mathbf{C})$ of objects, a set $\operatorname{Hom}(A, B)$ for each pair of objects A, B (called the set of *morphisms* from A to B), and a map

$$(\alpha, \beta) \mapsto \beta \circ \alpha : \operatorname{Hom}(A, B) \times \operatorname{Hom}(B, C) \to \operatorname{Hom}(A, C)$$

for each triple of objects A, B, C, satisfying the following conditions:

(a) composition of morphisms is associative;
(b) for each object A, $\operatorname{Hom}(A, A)$ has an element id_A that is a left and right identity for composition.

It is understood that the sets $\operatorname{Hom}(A, B)$ are disjoint, so that a morphism determines its source and target.

A *covariant functor* $F : \mathbf{C} \to \mathbf{D}$ is a "map" that with each object A of $\mathbf{C}$ associates an object $F(A)$ of $\mathbf{D}$ and with each morphism $\alpha : A \to B$ a morphism $F(\alpha) : F(A) \to F(B)$ such that $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ and $F(\mathrm{id}_A) = F(\mathrm{id}_{F(A)})$.

A functor $F : \mathbf{C} \to \mathbf{D}$ is *left adjoint* to the functor $G : \mathbf{D} \to \mathbf{C}$ if

$$\operatorname{Hom}_{\mathbf{D}}(F(A), B) \approx \operatorname{Hom}_{\mathbf{C}}(A, G(B))$$

functorially.

If the sets $\operatorname{Hom}(A, B)$ 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 $\mathbf{C}$ has a direct sum, then $\mathbf{C}$ (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 $i_A : A \to A \oplus B$, $i_B : B \to A \oplus B$, $p_A : A \oplus B \to A$, $p_B : A \oplus B \to B$ such that:

$$\begin{aligned} p_A \circ i_A = \mathrm{id}_A \qquad & p_B \circ i_B = \mathrm{id}_B \\ p_A \circ i_B = 0 \qquad & p_B \circ i_A = 0 \\ i_A p_A + i_B p_B = 1_{A \oplus B}. & \end{aligned}$$

Let $\mathbf{C}$ 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.

Let $\mathbf{C}$ be an additive category in which every morphism has both a kernel and a cokernel. Let $\alpha : A \to B$ 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 canonical map from the coimage of α to the image of α, and if this is always an isomorphism, then $\mathbf{C}$ is called an *abelian category.*

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 *exact* if it maps exact sequences to exact sequences.

For example, for any ring R, the category of R-modules is an abelian category, and, for any topological space X, the category of sheaves of abelian groups on X is an abelian category.

In the remainder of this section, $\mathbf{C}$ will be an abelian category. The reader will lose little (so far as this course is concerned) by taking $\mathbf{C}$ 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 $\mathbf{C}$ be an abelian category. An object I of $\mathbf{C}$ 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 $\mathbf{C}$ implies that

$$0 \to \mathrm{Hom}(C, I) \to \mathrm{Hom}(B, I) \to \mathrm{Hom}(A, I) \to 0$$

is exact. This sequence is automatically exact except at $\mathrm{Hom}(A, I)$, and so to say that I is injective means that every homomorphism $A \to I$ extends to B.

PROPOSITION 4.3. *The category of abelian groups has enough injectives.*

LEMMA 4.4. *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. Let $m \in M$, and consider the map $x \mapsto xm : R \to M$. The map $x \mapsto rx : R \to R$ is injective, and any extension of $x \mapsto xm$ to R will send 1 to an element m' such that $rm' = m$. Therefore, if M is injective, it is divisible.

Conversely, suppose that M is divisible, and consider a homomorphism $\alpha : A \to M$ where A is a submodule of B. On applying Zorn's lemma to the set of pairs (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 $A_1 \neq B$, there exists a $b \in B \setminus A_1$, and we define $I = \{r \in R \mid rb \in A_1\}$. Because M is divisible, the map $r \mapsto \alpha_1(rb) : I \to M$ extends to R, but this implies that α_1 extends to $A_1 + Rb$, which contradicts the maximality of (A_1, α_1). □

The lemma shows that $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module. For an arbitrary $\mathbb{Z}$-module M, define $M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$. Check that the canonical map $M \to M^{\vee\vee}$ is injective, and that $M^{\vee\vee}$ is divisible.

PROPOSITION 4.5. *Any functor $F : \mathbf{C} \to \mathbf{D}$ that admits an exact left adjoint preserves injectives.*

PROOF. Let F' be an exact left adjoint to F. For any injective object I in $\mathbf{C}$, the functor $\mathrm{Hom}_{\mathbf{D}}(\cdot, F(I))$ is isomorphic to the functor $\mathrm{Hom}_{\mathbf{C}}(F'(\cdot), I)$, which is exact because it is the composite of two exact functors, namely, F' and $\mathrm{Hom}_{\mathbf{C}}(\cdot, I)$. □

Right derived functors. Let $\mathbf{C}$ be an abelian category with enough injectives, and let $F : \mathbf{C} \to \mathbf{D}$ be a left exact functor from $\mathbf{C}$ to a second abelian category. Thus, a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

in $\mathbf{C}$ gives rise to an exact sequence

$$0 \to F(M') \to F(M) \to F(M'')$$

in $\mathbf{D}$. The theory of derived functors provides a natural extension of this last sequence to a long exact sequence.

Let M be an object of $\mathbf{C}$. A *resolution* of M is a long exact sequence

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^r \to \cdots .$$

If the I^r's are injective objects of $\mathbf{C}$, then it is called an *injective resolution*. We sometimes abbreviate this complex to $M \to I^\cdot$.

LEMMA 4.6. *An injective resolution $M \to I^\cdot$ of M exists, and if $M \to J^\cdot$ is a second injective resolution, then there is a homomorphism from $M \to I^\cdot$ to $M \to J^\cdot$, i.e., there is 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

$$0 \longrightarrow M \longrightarrow I^0$$

with I^0 injective. Let B^1 be the cokernel of the map. Then we know that there is an inclusion

$$0 \longrightarrow B^1 \longrightarrow I^1$$

with I^1 injective. Now

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1$$

is exact. Let $B^2 = \mathrm{Coker}(B^1 \to I^1)$, and continue in this fashion.

A morphism of resolutions can be constructed step by step, using the definition of an injective object. □

Let $M \to I^{\cdot}$ be an injective resolution of M. On applying the functor F, we obtain a complex

$$F(I^{\cdot}) : F(I^0) \to F(I^1) \to \cdots \to F(I^r) \xrightarrow{d^r} F(I^{r+1}) \to \cdots$$

which may no longer be exact. Define

$$(R^r F)(M) = H^r(F(I^{\cdot})) \stackrel{\mathrm{df}}{=} \frac{\mathrm{Ker}(d^r)}{\mathrm{Im}(d^{r-1})}.$$

PROPOSITION 4.7. *Let $\alpha : M \to N$ be a morphism of objects of C. For any injective resolutions $M \to I^{\cdot}$ and $N \to J^{\cdot}$, there exists a morphism $\alpha^{\cdot} : I^{\cdot} \to J^{\cdot}$ making*

$$\begin{array}{ccc} M & \longrightarrow & I^{\cdot} \\ \downarrow & & \downarrow \\ N & \longrightarrow & J^{\cdot} \end{array}$$

commute. The morphism $H^r(I^{\cdot}) \to H^r(J^{\cdot})$ is independent of the choice of $\alpha^{\cdot}$.

We discuss the proof below.

The proposition (applied to the identity map $M \to M$) implies that the objects $(R^r F)(M)$ are well-defined up to a canonical isomorphism. Moreover, a morphism $\alpha : M \to N$ gives rise to a well-defined morphism $(R^r F)(M) \to (R^r F)(N)$, and, in fact, the $R^r F$ are functors. They are called the *right derived functors* of F.

EXAMPLE 4.8. Because F is left exact,

$$0 \to F(M) \to F(I^0) \xrightarrow{d^0} F(I^1)$$

is exact. Therefore,

$$(R^0 F)(M) \stackrel{\mathrm{df}}{=} \mathrm{Ker}(d^0) = F(M).$$

In other words, $R^0 F = F$.

The next two lemmas prove something a little more precise than the proposition.

LEMMA 4.9. *Let $M \to I^{\cdot}$ and $N \to J^{\cdot}$ be resolutions of objects M and N of $\mathbf{C}$. If $N \to J^{\cdot}$ is an injective resolution, then any morphism $\alpha : M \to N$ extends to morphism*

$$\begin{array}{ccc} M & \longrightarrow & I^{\cdot} \\ \downarrow & & \downarrow \\ N & \longrightarrow & J^{\cdot} \end{array}$$

of complexes.

PROOF. Bucur and Deleanu 1968, 7.5. □

Two morphisms $\alpha^{\cdot}, \beta^{\cdot} : I^{\cdot} \to J^{\cdot}$ of complexes are said to be *homotopic* if there exists a family of morphisms $k^r : I^r \to J^{r-1}$ such that

$$\alpha^r - \beta^r = d^{r-1} \circ k^r + k^{r+1} \circ d^r$$

for all r.

Note that, for any $x \in Z^r(I^{\cdot}) \stackrel{\text{df}}{=} \operatorname{Ker}(d^r)$,

$$\alpha^r(x) - \beta^r(x) = d^{r-1}(k^r(x)) \in B^r(I^{\cdot}).$$

Therefore $\alpha^r(x)$ and $\beta^r(x)$ have the same image in $H^r(J^{\cdot})$, and so homotopic morphisms define the same morphism on cohomology.

LEMMA 4.10. *Let $M \to I^{\cdot}$ be a resolution of M, and let $N \to J^{\cdot}$ be an injective resolution N. Any two extensions $\alpha^{\cdot}$ and $\beta^{\cdot}$ of morphisms $M \to N$ to $I^{\cdot} \to J^{\cdot}$ are homotopic.*

PROOF. Ibid.. □

PROPOSITION 4.11. *A short exact sequence*

$$0 \to A \to B \to C \to 0$$

in $\mathbf{C}$ 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

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

gives rise to a commutative diagram

$$\begin{array}{ccccccccccc} \cdots & \to & R^{r-1}F(C) & \to & R^rF(A) & \to & R^rF(B) & \to & R^rF(C) & \to & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \to & R^{r-1}F(C') & \to & R^rF(A') & \to & R^rF(B') & \to & R^rF(C') & \to & \cdots \end{array}$$

For the proof of the proposition, see Bucur and Deleanu 1968, 7.6.

REMARK 4.12. The right derived functors of F are characterized by the three properties:

(a) $R^0F = F$;
(b) $R^rF(I) = 0$, $r > 0$, I injective;
(c) the property in (4.11).

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 $\mathbf{C}$ be an abelian category.

Let $A \in \mathbf{C}$. If $\mathbf{C}$ 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 $B \to I^{\cdot}$ of B, and set

$$\mathrm{Ext}^r(A, B) = H^r(\mathrm{Hom}(A, I^{\cdot})).$$

Let $B \in \mathbf{C}$. If $\mathbf{C}$ 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 $P^{\cdot} \to A$ of A, and we set

$$\mathrm{Ext}^r(A, B) = H^r(\mathrm{Hom}(P^{\cdot}, B).$$

PROPOSITION 4.13. *If* $\mathbf{C}$ *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 $\mathrm{Hom}(P^{\cdot}, I)$ is exact, and so

$$\mathrm{Ext}^r(A, I) \stackrel{\mathrm{df}}{=} H^r(\mathrm{Hom}(P^{\cdot}, I)) = 0.$$

Finally, if

$$0 \to B' \to B \to B'' \to 0$$

is exact, then because $P^{\cdot} \to A$ is a resolution of A by projectives, the sequence of complexes

$$0 \to \mathrm{Hom}(P^{\cdot}, B') \to \mathrm{Hom}(P^{\cdot}, B) \to \mathrm{Hom}(P^{\cdot}, B'') \to 0$$

is exact. By a standard procedure, we get out of this a long exact sequence

$$\cdots \to H^r(\mathrm{Hom}(P^{\cdot}, B')) \to H^r(\mathrm{Hom}(P^{\cdot}, B)) \to H^r(\mathrm{Hom}(P^{\cdot}, B'') \to \cdots .$$

□

EXAMPLE 4.14. Let G be a group. Then $\mathbf{Mod}_G$ has both enough injectives and enough projectives. For any 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:

$$\mathrm{Ext}^r_G(\mathbb{Z}, M) = H^r(G, M).$$

The last proposition allows us to compute these groups by choosing a projective resolution $P^{\cdot} \to \mathbb{Z}$ of $\mathbb{Z}$ and setting

$$H^r(G, M) = H^r(\mathrm{Hom}_G(P^{\cdot}, M)).$$

REMARK 4.15. It would shorten the exposition in this chapter a little by adopting the last formula as the definition of $H^r(G, M)$—this is the approach taken in Chapter IV of Cassels and Fröhlich, 1967. However, it is not the natural definition.

References. For the general notion of derived functors, see Chapter 7 of

Bucur, I., and Deleanu, A., Introduction to Categories and Functors, Wiley, 1968,

or Chapter 4 of

Hilton, P.J., and Stammbach, U., A Course in Homological Algebra, Springer, 1971.

CHAPTER III

Local Class Field Theory: Cohomology and Completion of the Proofs

We develop enough of the cohomological approach to local class field theory to complete the proofs of the main theorems. Throughout this chapter, "local field" will mean "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.3).

1. Introduction

Recall that, after Chapter I, to complete the proof of the main theorems of class field theory, it remains to show that, for any local field K, there exists a homomorphism (local Artin map)

$$\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{al}}/K)$$

with the following properties:

(a) for any prime element π of K, $\phi_K(\pi)|K^{\mathrm{un}} = \mathrm{Frob}_K$;
(b) for any 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

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

For a Galois extension of fields L/K (possibly infinite), set

$$H^2(L/K) = H^2(\mathrm{Gal}(L/K), L^\times).$$

In the next chapter we shall see that $H^2(L/K)$ has an explicit interpretation as the relative Brauer group of L/K. Because of Hilbert's Theorem 90, 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 $E \supset L \supset K$ (II.1.36).

We shall prove:

THEOREM 1.1. *For any local field K, there exists a canonical isomorphism*

$$\mathrm{inv}_K : H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}.$$

Moreover, if $[L:K]=n<\infty$, *then the diagram*

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \\ & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes, and therefore defines an isomorphism

$$\mathrm{inv}_{L/K}: H^2(L/K)\to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

The proof of Theorem 1.1 will occupy the next two sections. In the remainder of this section, we shall explain how it (together with Proposition 1.6 below) implies the existence of a local Artin map with the required properties.

Thus, assume Theorem 1.1. The element $u_{L/K}$ of $H^2(L/K)$ corresponding to $\frac{1}{n}$ mod $\mathbb{Z}$ under the isomorphism $\mathrm{inv}_{L/K}$ is called the *fundamental class* of the extension L/K.

LEMMA 1.2. *Let* $E\supset L\supset K$ *be a tower of finite Galois extensions. Then*

$$\begin{aligned} \mathrm{Res}(u_{E/K}) &= u_{E/L}, \\ \mathrm{Inf}(u_{L/K}) &= [E:L]u_{E/K}. \end{aligned}$$

PROOF. Consider

$$\begin{array}{ccccc} H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/E) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} & & \downarrow{\scriptstyle \mathrm{inv}_E} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[E:L]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The vertical maps are isomorphisms. On applying the kernel-cokernel lemma to the rows, we obtain a commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\mathrm{Inf}} & H^2(E/K) & \xrightarrow{\mathrm{Res}} & H^2(E/L) \\ & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{E/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{E/L}} \\ 0 & \longrightarrow & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{[L:K]} & \frac{1}{[E:L]}\mathbb{Z}/\mathbb{Z}. \end{array}$$

The commutativity of the two squares implies the two equalities. □

Now let L/K be a finite Galois extension of local fields with Galois group G. For any subgroup H of G,

(a) $H^1(H,L^\times)=0$ (Hilbert's theorem 90);
(b) $H^2(H,L^\times)$ is cyclic of order $(H:1)$, with a canonical generator u_{L/L^H} $(=\mathrm{Res}(u_{L/K}))$.

The pair $(G,L^\times)$ thus satisfies the hypotheses of Tate's theorem (II.2.18).

COROLLARY 1.3. *Let L/K be a finite Galois extension of local fields with Galois group G. For all r, there exists a canonical isomorphism*

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

namely, cup product with $u_{L/K}$. When $r=2$, this becomes an isomorphism

$$G^{\mathrm{ab}} \cong K^\times/\operatorname{Nm}_{L/K}(L^\times).$$

COROLLARY 1.4 (NORM LIMITATION THEOREM). *Let E be a finite Galois extension of K, and let L be the largest abelian extension of K contained in E; then $\operatorname{Nm}_{E/K}(E^\times) = \operatorname{Nm}_{L/K}(L^\times)$.*

PROOF. Because $\operatorname{Nm}_{E/K} = \operatorname{Nm}_{E/L}\circ\operatorname{Nm}_{L/K}$, certainly $\operatorname{Nm}_{E/K}(E^\times) \subset \operatorname{Nm}_{L/K}(L^\times)$. However, $\operatorname{Gal}(L/K) = \operatorname{Gal}(E/K)^{\mathrm{ab}}$, and so the preceding corollary shows that the norm groups have the same index in $K^\times$. This implies that they are equal. □

Local class field classifies the abelian extensions of a local field by means of the norm groups of the fields. The corollary shows that this approach fails to classify the nonabelian extensions.

For a finite abelian extension L/K, we define the *local Artin map*

$$\varphi_{L/K} : K^\times/\operatorname{Nm}(L^\times) \to \operatorname{Gal}(L/K)$$

to be the inverse of the isomorphism in Corollary 1.3.

PROPOSITION 1.5. *If $E \supset L \supset K$ is a tower of finite abelian extensions of K, then $\varphi_{E/K}(a)|L = \varphi_{L/K}(a)$ for all $a \in K$.*

PROOF. This can be checked directly from the definition of the local Artin maps, using that $\operatorname{Inf}(u_{L/K}) = [E:L]u_{E/K}$. □

Define $\varphi_K : K^\times \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ to be the homomorphism such that, for every finite abelian extension L/K, $\varphi_K(a)|L = \varphi_{L/K}(a)$ all $a \in K^\times$—Proposition 1.5 shows that this definition makes sense. By its very definition, φ_K satisfies condition (b) to be the local Artin map, and the next proposition implies that it also satisfies condition (a).

PROPOSITION 1.6. *When L/K is unramified, $\varphi_{L/K}$ maps every prime element of K to $\operatorname{Frob}_{L/K}$.*

This will be proved in the next section.

Thus, to complete the proofs of the main theorems of local class field theory, it remains to prove Theorem 1.1 and Proposition 1.6.

REMARK 1.7. To a finite Galois extension L/K of local fields, we have attached the groups $K^\times/\operatorname{Nm}(L^\times)$ and $H^2(L/K)$. When L/K is cyclic, they are canonically (up to the choice of generator for $G = \operatorname{Gal}(L/K)$) 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.

2. The Cohomology of Unramified Extensions

The cohomology of the units.

PROPOSITION 2.1. *Let L/K be a finite unramified extension with Galois group G, and let U_L be the group of units in L. Then*

$$H_T^r(G, U_L) = 0, \quad \text{all } r.$$

Let π be a prime element of K. Then π is also a prime element in L, and

$$L^\times \cong U_L \times \pi^{\mathbb{Z}}.$$

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), this shows that $H^1(G, U_L) = 0$. Because G is cyclic, to complete the proof of the theorem, it suffices (by II.2.11) to show that $H_T^0(G, U_L) = 0$. This is accomplished by the next proposition.

PROPOSITION 2.2. *For any finite unramified extension L/K, the norm map $\mathrm{Nm}_{L/K} : U_L \to U_K$ is surjective.*

Let ℓ and k be the residue fields of L and K. The action of G on $\mathcal{O}_L$ identifies G with $\mathrm{Gal}(\ell/k)$.

LEMMA 2.3. *For $m > 0$, let $U_L^{(m)} = 1 + \mathfrak{m}_L^m$. Then*

$$\begin{aligned} U_L/U_L^{(1)} &\xrightarrow{\approx} \ell^\times \\ U_L/U_L^{(m)} &\xrightarrow{\approx} \ell \end{aligned}$$

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

$$\begin{aligned} u \mapsto u \mod \mathfrak{m}_L &: U_L \to \ell^\times \\ 1 + a\pi^m \mapsto a \mod \mathfrak{m}_L &: U_L^{(m)} \to \ell \end{aligned}$$

induce the required isomorphisms. □

LEMMA 2.4. *For all r, $H_T^r(G, \ell^\times) = 0$. In particular, the norm map $\ell^\times \to k^\times$ is surjective.*

PROOF. By Hilbert's Theorem 90, $H^1(G, \ell^\times) = 0$, and because $\ell^\times$ is finite, its Herbrand quotient $h(\ell^\times) = 1$ (see II.2.15)). Therefore $H^2(G, \ell^\times) = 0$, and this implies that all the groups are zero (see II.2.11). □

LEMMA 2.5. *The group $H_T^r(G, \ell) = 0$ for all r. In particular, the trace map $\ell \to k$ is surjective.*

PROOF. See Proposition II.1.23. □

We now prove Proposition 2.2. Consider $u \in U_K$. Because the norm map $\ell^\times \to k^\times$ is surjective, there exists a $v_0 \in U_L$ such that $\mathrm{Nm}(v_0) \equiv u \mod U_K^{(1)}$. Because the trace map $\ell \to k$ is surjective, so also is the norm map $U_L^{(1)}/U_L^{(2)} \to U_K^{(1)}/U_K^{(2)}$, and so 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 $v_0, v_1, v_2, v_3, \ldots, v_i \in U_K^{(i)}$, such that $u/\mathrm{Nm}(v_0 \cdots v_i) \in U_K^{(i+1)}$. Let $v = \lim_{m\to\infty} \prod_{j=1}^m v_j$. Then $u/\mathrm{Nm}(v) \in \cap U_K^{(i)} = \{1\}$.

REMARK 2.6. Let L be an infinite unramified extension of K. Then L is Galois over K, and, for $r \geq 0$,

$$H^r(\mathrm{Gal}(L/K), U_L) = \varinjlim_{K'} H^r(\mathrm{Gal}(K'/K), U_{K'})$$

where the limit is over the finite extensions K' of K contained in L. Therefore

$$H^r(\mathrm{Gal}(L/K), U_L) = 0$$

for all $r > 0$ (continuous cohomology).

The invariant map. Let L be an unramified extension of K (possibly infinite), and let $G = \mathrm{Gal}(L/K)$.

From the cohomology sequence of G-modules

$$0 \longrightarrow U_L \longrightarrow L^\times \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \longrightarrow 0,$$

we obtain (using 2.6) an isomorphism

$$H^1(G, L^\times) \longrightarrow H^1(G, \mathbb{Z}).$$

From the cohomology sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

(trivial G-actions) we obtain an isomorphism

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}).$$

Recall that

$$H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z}).$$

If $[L : K] = n < \infty$, then G is a cyclic group of order n with generator $\mathrm{Frob}_{L/K}$, and the map

$$f \mapsto f(\mathrm{Frob}_{L/K}) : \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$$

is an isomorphism from $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ onto the unique cyclic subgroup $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$ of order n; if $[L : K] = \infty$, then G is generated in the topological sense by $\mathrm{Frob}_{L/K}$, i.e., G is the closure of the group $\{\mathrm{Frob}_{L/K}^i \mid i \in \mathbb{Z}\}$, and $f \mapsto f(\mathrm{Frob}_{L/K})$ is an isomorphism of $\mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z})$ onto an infinite subgroup of $\mathbb{Q}/\mathbb{Z}$ (in fact, the whole of $\mathbb{Q}/\mathbb{Z}$ if $L = K^{\mathrm{un}}$, because the image contains $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ for all n).

The composite of

$$H^2(L/K) \xrightarrow{\approx} H^2(G, \mathbb{Z}) \xleftarrow[\approx]{\delta} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}$$

is called the invariant map

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}.$$

Now consider a tower of field extensions

$$E \supset L \supset K$$

with both E and L unramified (hence Galois) over K. Then

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\text{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \text{Inf} & & \| \\ H^2(E/K) & \xrightarrow{\text{inv}_{E/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes, because all the maps in the definition of inv are compatible with Inf.

In particular, there is a canonical isomorphism

$$\text{inv}_K : H^2(K^{\text{un}}/K) \to \mathbb{Q}/\mathbb{Z},$$

with the property that, for any $L \subset K^{\text{un}}$ of finite degree n over K, inv_K induces an isomorphism

$$\text{inv}_{L/K} : H^2(L/K) \to \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

We next need to prove that the diagram in Theorem 1.1 commutes with K^{al} replaced by K^{un}. In fact, we shall prove a more general result.

PROPOSITION 2.7. *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:*

$$\begin{array}{ccc} H^2(K^{\text{un}}/K) & \xrightarrow{\text{Res}} & H^2(L^{\text{un}}/L) \\ \big\downarrow{\scriptstyle \text{inv}_K} & & \big\downarrow{\scriptstyle \text{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\ n\ } & \mathbb{Q}/\mathbb{Z}. \end{array}$$

PROOF. To obtain the largest unramified extension of a local field, we only have to adjoin the mth roots of 1 for m not divisible by the residue characteristic. Therefore, $L^{\text{un}} = L \cdot K^{\text{un}}$, and so

$$\tau \mapsto \tau | K^{\text{un}} \colon \text{Gal}(L^{\text{un}}/L) \to \text{Gal}(K^{\text{un}}/K)$$

is injective. The map denoted Res in the above diagram is that defined by the compatible homomorphisms:

$$\begin{array}{ccc} \text{Gal}(K^{\text{un}}/K) & \leftarrow & \text{Gal}(L^{\text{un}}/L) \\ K^{\text{un}\times} & \to & L^{\text{un}\times}. \end{array}$$

Let $\Gamma_K = \text{Gal}(K^{\text{un}}/K)$ and $\Gamma_L = \text{Gal}(L^{\text{un}}/L)$. Consider the diagram:

$$\begin{array}{ccccccc} H^2(K^{\text{un}}/K) & \xrightarrow{\approx} & H^2(\Gamma_K, \mathbb{Z}) & \xleftarrow[\approx]{\delta} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \big\downarrow{\scriptstyle \text{Res}} & & \big\downarrow{\scriptstyle e\,\text{Res}} & & \big\downarrow{\scriptstyle e\,\text{Res}} & & \big\downarrow{\scriptstyle fe} \\ H^2(L^{\text{un}}/L) & \xrightarrow{\approx} & H^2(\Gamma_L, \mathbb{Z}) & \xleftarrow[\approx]{\delta} & H^1(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Here e and f are the ramification index and residue class degree for L/K. The left hand square is obtained from the commutative square

$$\begin{array}{ccc} K^{\mathrm{un}\times} & \xrightarrow{\mathrm{ord}_K} & \mathbb{Z} \\ \downarrow & & \downarrow e \\ L^{\mathrm{un}\times} & \xrightarrow{\mathrm{ord}_L} & \mathbb{Z}. \end{array}$$

The second square expresses the fact that the restriction map commutes with the boundary map. Apart from the factor "e", the third square is

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi\mapsto\varphi(\mathrm{Frob}_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \varphi\mapsto\varphi|\Gamma_L} & & \downarrow f \\ \mathrm{Hom}(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi\mapsto\varphi(\mathrm{Frob}_L)} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

The Frobenius elements are determined by the fact that they induce $x \mapsto x^q$ and $x \mapsto x^{q^f}$ on the residue fields, where $q = \#k$ and $q^f = \#\ell$. Hence $\mathrm{Frob}_L\,|K = \mathrm{Frob}_K^f$. It is now clear that the square commutes, and since $n = ef$, this proves the proposition. □

Computation of the local Artin map. Let L be a finite unramified extension of K with Galois group G, and let $n = [L : K]$. From the last subsection, we know that $(G, L^\times)$ satisfies the hypotheses of Tate's theorem (II.2.18), and so we have a canonical isomorphism

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) & \to & H^0(G, L^\times) \\ \| & & \| \\ G & & K^\times/\,\mathrm{Nm}(L^\times). \end{array}$$

We now compute this map explicitly.

If π is a prime element of L, then every element of $L^\times$ can be written uniquely in the form $\alpha = u\pi^m$, $u \in U$, $m \in \mathbb{Z}$; thus

$$L^\times = U \times \pi^{\mathbb{Z}} \cong U \times \mathbb{Z}.$$

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 the above decomposition is a decomposition of G-modules (G acting trivially on $\pi^{\mathbb{Z}} \approx \mathbb{Z}$).

Lemma 2.8. *For any group G and G-modules M, N,*

$$H^r(G, M \oplus N) = H^r(G, M) \oplus H^r(G, N).$$

Proof. This was proved in Proposition II.1.25. Alternatively, 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 II.4). These maps and relations persist when we apply the additive functor $H^r(G, \cdot)$. □

Thus

$$H^r(G, L^\times) = H^r(G, U_L) \oplus H^r(G, \pi^{\mathbb{Z}}).$$

Choose a generator σ of G (e.g., the Frobenius generator), and let

$$f \in H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

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

$$\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}).$$

According to the description of δ in (II.1.20, to construct δf, we first choose a lifting of f to 1-cochain $\widetilde{f} : G \to \mathbb{Q}$. We take $\widetilde{f}$ to be the map $\sigma^i \mapsto \frac{i}{m}$ where $0 \le i < m-1$. Then

$$d\widetilde{f}(\sigma^i, \sigma^j) = \sigma^i \widetilde{f}(\sigma^j) - \widetilde{f}(\sigma^{i+j}) + \widetilde{f}(\sigma^i) = \begin{cases} 0 & \text{if} \quad i+j \le n-1 \\ 1 & \text{if} \quad i+j > n-1. \end{cases}$$

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:

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if} \quad i+j \le n-1 \\ \pi & \text{if} \quad i+j > n-1 \end{cases}$$

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.2.18) 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 $L^\times \oplus \bigoplus_{\sigma \in G, \sigma \ne 1} \mathbb{Z} x_\sigma$ of φ.

Finally, $H^{-2}(G, \mathbb{Z}) \overset{\text{df}}{=} H_1(G, \mathbb{Z}) \cong G$ (II.2.7).

Proposition 2.9. *Under the composite*

$$\begin{array}{ccc} H^{-2}(G, \mathbb{Z}) & \to & H^0(G, L^\times) \\ \| & & \| \\ G & & K^\times / \mathrm{Nm}_G L^\times \end{array},$$

of the above maps, σ maps to $\pi \mod \mathrm{Nm}(L^\times)$.

Note that, because $H^0(G, U_L) = 0$, $U_L \subset \mathrm{Nm}_{L/K}(L^\times)$, and the class of π mod $\mathrm{Nm}(L^\times)$ is independent of the prime element π. On the other hand, $L^\times(\varphi)$ and the map depend on the choice of the generator σ for G.

PROOF. From the construction of the isomorphism $H^{-2}(G,\mathbb{Z}) \cong G$, 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 'x_σ'$= \varphi(1,1) = 1$ 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 2.10. The above proof of Proposition 2.9, 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.

3. The Cohomology of Ramified Extensions

LEMMA 3.1. *If L/K is Galois of finite degree n, then $H^2(L/K)$ has a subgroup of order n.*

PROOF. Consider the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Ker(Res)} & \longrightarrow & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\
0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L)
\end{array}$$

Since the two restriction maps are injective, so also is the first vertical map, but (2.7) shows that the kernel of the restriction map on the top row is $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

To complete the proof of Theorem 1.1, it suffices to prove that the map $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(L/K)$ is an isomorphism (see the last paragraph of this section). There are two different approaches to proving this. In the next chapter on Brauer groups, we shall show that $H^2(K^{\mathrm{al}}/K^{\mathrm{un}}) = 0$; this implies that the restriction maps in the diagram are isomorphisms, and hence also that the first vertical map is an isomorphism. The second proof, which we now present, shows that $\#H^2(L/K) \leq n$.

LEMMA 3.2. *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 $H^r(G,V) = 0$ all $r > 0$.*

PROOF. Let $\{x_\tau \mid \tau \in G\}$ be a normal basis for L over K (see II.1.24). The x_τ have a common denominator d in $\mathcal{O}_K$ (see Math 676, 2.4). After replacing each x_τ with $d \cdot x_\tau$, we may suppose that they lie in $\mathcal{O}_L$. Take $V = \sum \mathcal{O}_L x_\tau$. Then

$$V \cong \mathcal{O}_L[G] = \mathrm{Ind}^G \mathcal{O}_L,$$

and so $H^r(G,V) = 0$ for all $r > 0$. □

LEMMA 3.3. *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. (Assume $\mathrm{char}K = 0$.) The power series

$$e^x = 1 + x + \cdots + x^n/n! + \cdots$$

converges for $\mathrm{ord}(x) > \mathrm{ord}(p)/(p-1)$. It defines an isomorphism of an open neighbourhood of 0 in L onto an open neighbourhood of 1 in $L^\times$, with inverse mapping $\log(x) = (x-1) - (x-1)^2/2 + (x-1)^3/3 - \cdots$. Clearly both maps commute with the actions of G. If V' is an open neighbourhood of 0 as in (3.2), 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 on $\pi^M V'$. □

LEMMA 3.4. *Let L/K be a cyclic extension of degree n; then $h(U_L) = 1$ and $h(L^\times) = n$.*

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 group U_L/V is finite, and so $h(U_L) = h(V) = 1$ (see II.2.16). Finally $h(L^\times) = h(U) \cdot h(\mathbb{Z}) = h(\mathbb{Z})$, and

$$h(\mathbb{Z}) = \#H^0_T(G,\mathbb{Z})/\#H^1(G,\mathbb{Z}) = \#H^0_T(G,\mathbb{Z}) = \#(\mathbb{Z}/n\mathbb{Z}) = n.$$

□

LEMMA 3.5. *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 (see Math 676, 7.50), there will be a Galois extension K'/K with $L \supsetneqq K' \supsetneqq K$. From the exact sequence

$$0 \to H^2(K'/K) \to H^2(L/K) \to H^2(L/K')$$

we find that

$$\#H^2(L/K) \leq \#H^2(K'/K)\#H^2(L/K') = n.$$

□

We now complete the proof of Theorem 1.1. From the diagram in the proof of (3.1) we see that, for any 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. Therefore, the invariant map $\mathrm{inv}_K : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ defines an isomorphism $H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}$. It follows from (3.1) that this homomorphism has the property required for Theorem 1.1. Moreover, Proposition 2.9 (with σ taken to be the Frobenius generator) shows that the homomorphism has the properties required for Proposition 1.6. This completes the proofs of the main theorems of local class field theory.

4. Complements

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 very 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 4.1. *For any $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ and $a \in K^\times$,*

$$\chi(\phi_{L/K}(a)) = \mathrm{inv}_K(a \cup \delta\chi).$$

Proof. Omitted. (See Serre, Local Fields, "Annexe" to Chapter XI, and his article in Cassels-Fröhlich, p140.) □

Using this, we can get another proof of Proposition 1.6.

Lemma 4.2. *If L/K is unramified, $\phi_{L/K}$ sends $a \in K^\times$ to $\mathrm{Frob}^{ord_K a}$.*

PROOF. Recall that inv_K is defined to be the composite

$$H^2(G,L^\times) \xrightarrow{\text{ord}} H^2(G,\mathbb{Z}) \xleftarrow{\delta} \text{Hom}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\chi\mapsto\chi(\sigma)} \mathbb{Q}/\mathbb{Z}.$$

Because of the functoriality of cup-products

$$\text{ord}(a\cup\delta\chi) = \text{ord}(a)\cup\delta\chi, \quad a\in K^\times, \quad \chi\in\text{Hom}(G,\mathbb{Q}/\mathbb{Z})$$

where, on the left ord denotes the map on H^2 induced by $\text{ord}_L\colon L^\times \twoheadrightarrow \mathbb{Z}$, and on the right it is the map itself. Let $a\in H^0(G,L^\times) = K^\times$, and let $m = \text{ord}_L(a)$. For any $\chi\in\text{Hom}(G,\mathbb{Q}/\mathbb{Z})$, in the above diagram,

$$a\cup\delta\chi \mapsto \text{ord}(a)\cup\delta\chi \mapsto m\chi \mapsto \chi(\sigma^m), \quad \sigma = \text{Frob},$$

i.e., $\text{inv}_K(a\cup\delta\chi) = \chi(\sigma^m)$. On combining this with the formula in (4.1) we find that

$$\chi(\phi(\alpha)) = \chi(\sigma^{\text{ord}(\alpha)})$$

for all $\chi\in\text{Hom}(G,\mathbb{Q}/\mathbb{Z})$, and so $\phi(\alpha) = \sigma^{\text{ord}(\alpha)}$. □

For any character χ of G, we get a character $a\mapsto \text{inv}_K(a\cup\delta\chi)$ of $K^\times$. By duality we get a map $K^\times\to G$. Proposition 4.1 shows that this map is $\phi_{L/K}: K^\times\to\text{Gal}(L/K)$.

The Hilbert symbol. Let $a,b\in\mathbb{Q}_p^\times$ with p a prime number or infinity (we let $\mathbb{Q}_\infty = \mathbb{R}$). The *Hilbert symbol* of a and b relative to $\mathbb{Q}_p$ is defined by

$$(a,b)_p = \begin{cases} 1 & \text{if } z^2 = ax^2+by^2 \text{ has a nonzero solution in } \mathbb{Q}_p \\ -1 & \text{otherwise.}\end{cases}$$

Then $a,b\mapsto(a,b)$ is a nondegenerate bilinear pairing

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\to\{\pm1\}.$$

It has many interesting properties, the most profound being the product formula (proved by Hilbert). For fixed $a,b\in\mathbb{Q}$, $(a,b)_p = 1$ for all but finitely many primes p, and

$$\prod_{p\le\infty}(a,b)_p = 1.$$

This proof of the product formula uses the quadratic reciprocity law. The product formula has an interpretation in terms of Brauer groups (see the next chapter), and has implications for the theory of quadratic forms over $\mathbb{Q}$ (see Chapter VIII).

We can define Hilbert symbols for any local field K. Let μ_n be the group of nth roots of 1 in K^{al} (if the characteristic of K is $p\neq 0$, then n should not be divisible by p). Let $G = \text{Gal}(K^{\text{al}}/K)$. There is an exact sequence of G-modules,

$$1\to\mu_n\to K^{\text{al}\times}\xrightarrow{n}K^{\text{al}\times}\to 1,$$

and hence an exact cohomology sequence

$$K^\times\xrightarrow{n}K^\times\to H^1(G,\mu_n)\to 0\to 0\to H^2(G,\mu_n)\to H^2(K^{\text{al}}/K)\to H^2(K^{\text{al}}/K).$$

Thus:

$$\begin{aligned} H^1(G,\mu_n) &\cong K^\times/K^{\times n} \\ H^2(G,\mu_n) &\cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}\cong\mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

There is a cup-product pairing

$$H^1(G,\mu_n)\times H^1(G,\mu_n)\to H^2(G,\mu_n\otimes\mu_n).$$

In the case that K contains an nth root ζ of 1, the cup-product pairing

$$H^2(G,\mu_n)\times H^0(G,\mu_n)\to H^2(G,\mu_n\otimes\mu_n)$$

defines an isomorphism

$$H^2(G,\mu_n)\otimes\mu_n\to H^2(G,\mu_n\otimes\mu_n),$$

and hence an isomorphism

$$H^2(G,\mu_n\otimes\mu_n)\to H^2(G,\mu_n)\otimes\mu_n\to(\mathbb{Z}/n\mathbb{Z})\otimes\mu_n=\mu_n.$$

Therefore, in this case, the pairing becomes

$$a,b\mapsto(a,b):K^\times/K^{\times n}\times K^\times/K^{\times n}\to\mu_n.$$

This pairing is again called the *Hilbert symbol*. Class field theory shows that it has most of the properties of the first pairing defined above.

PROPOSITION 4.3. *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 any $\tau\in\mathrm{Gal}(K[a^{\frac{1}{n}}]/K)$, $\tau a^{\frac{1}{n}}=\zeta a^{\frac{1}{n}}$ 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 4.1.

Other Topics. At this point, it would not be difficult to give a proof of the Local Existence Theorem (I.1.2) that is independent of Chapter II—see Serre 1962, 11.5, 14.6.

The reader who is interested in understanding the (conjectural) statement of *non-abelian* local class field theory should look first at Chapter VII of C.J. Moreno, Advanced Analytic Number Theory, Part I: Ramification Theoretic Methods, AMS, 1983.

Notes. It follows from Krasner's lemma (see Math 676, 7.51) that every finite abelian extension of local fields arises by completing a finite abelian extension of global fields. In the 1930's Hasse was 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 1940's, 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, Local Fields, 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 1981 Gold and Rosen independently gave "elementary" proofs that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{un}}$. In his book (Local Class Field Theory, 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, Local class field theory is easy, Adv. Math. 18 (1975), 148–181), (Neukirch, Class Field Theory, Springer, 1986), and (Fesenko and Vostokov, Local Fields and Their Extensions: A constructive approach, AMS, 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.

In this chapter, we have largely followed Serre 1962 and Serre's article in Cassels and Fröhlich 1967.

CHAPTER IV

Brauer Groups

In this chapter, we 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.

Terminology for k-algebras. By a *k-algebra* we mean 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 $\varphi : A \to B$ 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 $\alpha \cdot \beta = \beta\alpha$. If A is a k-subalgebra of a k-algebra E, then the *centralizer* of A in E, sometimes denoted $C(A)$ or $C_E(A)$, is the set of $\gamma \in E$ such that $\gamma\alpha = \alpha\gamma$ for all $\alpha \in A$. It is again a k-subalgebra of B. For example, $C_A(A)$ is the centre of A. 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. 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 said to be *simple* if it is nonzero and contains no A-submodules apart from the obvious two, namely, V and 0, and it is said to be *semisimple* if it can

be written as 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. Some authors use "irreducible" and "completely reducible" for "simple" and "semisimple" respectively.

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 $L_1 \stackrel{\text{df}}{=} \left\{ \begin{pmatrix} * \\ 0 \end{pmatrix} \right\}$ and $L_2 \stackrel{\text{df}}{=} \left\{ \begin{pmatrix} 0 \\ * \end{pmatrix} \right\}$. 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: there are no subspaces of k^2 stable under $M_2(k)$ apart from 0 and V.

THEOREM 1.2. *Any A-module V admits a filtration*

$$V \supset V_1 \supset \cdots \supset V_r = 0$$

whose quotients V_i/V_{i+1} are simple A-modules. If

$$V \supset V_1' \supset \cdots \supset V_{r'}' = 0$$

is a second such filtration, then $r = r'$ and there is a bijection $i \mapsto i'$ such that $V_i/V_{i+1} \approx V_{i'}'/V_{i'+1}'$ 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 (in fact, the statement is a special case of the Jordan-Hölder theorem with operators) (see, for example, Math 594g, Section 6.4). □

For example, the simple summands S_i occurring in a decomposition $V = \oplus S_i$ of a semisimple A-module are unique up to isomorphism and renumbering.

PROPOSITION 1.3. *Let V be a* semisimple *A-module, say $V = \oplus_{i=1}^{r} S_i$ with the S_i simple. For any submodule W of V, there is a subset I of $\{1, \dots, r\}$ such that $V = W \oplus \oplus_{i \in I} S_i$.*

PROOF. For a subset I of $\{1, \dots, r\}$, define $S_I = \oplus_{i \in I} S_i$. Let I be maximal among the subsets of $\{1, \dots, r\}$ such that $W \cap S_I = 0$. I claim that $W + S_I$ equals V. To prove this, it suffices to show that each S_i is contained in $W + S_I$. Because S_i is simple, $S_i \cap (W + S_I)$ equals S_i or 0. In the first case, $S_i \subset W + S_I$, and in the second

$W \cap (S_I + S_i) = 0$, which contradicts the definition of I. Therefore $V = W + S_I$, and because $W \cap S_I = 0$, the sum is direct. □

COROLLARY 1.4. *Every submodule and every quotient module of a semisimple module is semisimple.*

PROOF. The proposition shows that $V/W \approx S_I$ and that $W \approx V/S_I \approx S_{I'}$ where I' is the complement of I in $\{1, 2, \dots, r\}$. □

Simple k-algebras. A k-algebra A is said to be *simple* if it contains no two-sided ideals except for the obvious two, namely, 0 and A. We shall make frequent use of the following observation:

> The kernel of a homomorphism $f : A \to B$ of k-algebras is an ideal in A not containing 1; therefore, if A is simple, then f is injective.

EXAMPLE 1.5. Consider the matrix algebra $M_n(k)$. For $A, B \in M_n(k)$, the jth column $(A \cdot B)_j$ of $A \cdot B$ is $A \cdot B_j$ where B_j is the jth column of B. Therefore, a given matrix B,

$$\begin{aligned} B_j = 0 &\implies (A \cdot B)_j = 0 \\ B_j \neq 0 &\implies (A \cdot B)_j \text{ arbitrary.} \end{aligned}$$

It follows that the left ideals of $M_n(k)$ are 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 $j \notin I$. In particular, the minimal left ideals are the sets $L(\{j_0\})$. Similar statements hold for the right ideals, from which it follows that any nonzero two-sided ideal in $M_n(k)$ is the whole ring: $M_n(k)$ is a simple k-algebra.

EXAMPLE 1.6. 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.

If D is a division algebra, then, as in (1.5), the left ideals in $M_n(D)$ are the sets of the form $L(I)$ and $M_n(D)$ is simple.

EXAMPLE 1.7. For $a, b \in k^\times$, let $H(a, b)$ be the k-algebra with basis $1, i, j, \kappa$ (as a k-vector space) and with the multiplication table:

$$\begin{array}{cccc} 1 & i & j & \kappa \\ i & a & k & aj \\ j & -\kappa & b & -bi \\ \kappa & -aj & bi & -ab \end{array}$$

i.e., $i^2 = a$, $j^2 = b$, $ij = \kappa = -ji$ ($\implies i\kappa = iij = aj$ etc.). 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 5.1) that $H(a, b)$ is either a division algebra or it is isomorphic to $M_2(k)$. In particular, it is simple.

REMARK 1.8. 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. Let V be a D-module of dimension 1, so that $V = De_0$ for some $e_0 \in V$. A D-linear map $\varphi : V \to V$ is determined by its value at e_0, $\varphi(e_0) = ae_0$, and $\varphi \mapsto a$ is a bijection $\mathrm{End}_D(V) \to D$. If $\varphi(e_0) = ae_0$ and $\psi(e_0) = be_0$, then

$$(\varphi \circ \psi)(e_0) \stackrel{\text{df}}{=} \varphi(\psi(e_0)) = \varphi(be_0) = b(\varphi(e_0)) = bae_0,$$

and so $\varphi \mapsto a$ is an isomorphism of k-algebras $\mathrm{End}_D(V) \to D^{\mathrm{opp}}$. Similarly, if V is a D-module of dimension n, then the choice of a basis for V determines an isomorphism of k-algebras $\mathrm{End}_D(V) \to M_n(D^{\mathrm{opp}})$.

THEOREM 1.9. *Any simple k-algebra 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.

Thus, we can regard A as a subalgebra of $E \stackrel{\text{df}}{=} \mathrm{End}_k(S)$, the ring of k-linear map $S \to S$. Note that the centralizer $C_E(A)$ of A in E is equal to $\mathrm{End}_A(S)$, the ring of A-linear maps $S \to S$, and that S can be regarded as a $C_E(A)$-module. We shall complete the proof of the theorem by proving:

(a) $D \stackrel{\text{df}}{=} C_E(A)$ is a division algebra;
(b) A is the centralizer of D in E, i.e., $A = \mathrm{End}_D(S)$.

It will then follow from the Remark 1.8 that $\mathrm{End}_D(S) \approx M_r(D^{\mathrm{opp}})$ □

LEMMA 1.10 (SCHUR'S LEMMA). *For any k-algebra A and any simple A-module S, $\mathrm{End}_A(S)$ 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 1.11 (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 $\mathrm{End}_k(V)$).*

EXAMPLE 1.12. Let $V = k^n$. In the following, centralizers will be taken in $\mathrm{End}_k(V) = M_n(k)$.

(a) Let $A = k$ acting by left multiplication on $V = k^n$. Then $C(A) = M_n(k)$, and $C(C(A))$ is the centre of $M_n(k)$. To see this, let $\alpha = (a_{ij})$ lie in the centre of $M_n(k)$. Let e_{ij} be the matrix with 1 in the (i,j)th position and zeros elsewhere, so that
$$e_{ij}e_{lm} = \begin{cases} e_{im} & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$
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 $\alpha e_{lm} = e_{lm}\alpha$, then $a_{il} = 0$ 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).
(b) Let A be the set of diagonal matrices in $M_n(k)$, and let $V = k^n$. Then $C(A) = A$, and so $C(C(A)) = C(A) = A$.

PROOF. In the situation of the proposition, let $D = C(A)$ and let $B = C(D)$. 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 1.13. *Under the hypotheses of the proposition, 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 1.3) 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 $bv_1 \in Av_1$.

We now prove the general case. Let W be the direct sum of n copies of V with A acting diagonally, i.e.,

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n), \quad a \in A, \quad x_i \in V.$$

Then W is again a semisimple A-module. 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 $\mathrm{End}_k(A)$ is $M_n(D)$. An argument as in the above example, 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. □

Modules over simple k-algebras. When we regard A as a k-vector space and let A act on it by left multiplication, then we obtain a homomorphism $A \to \mathrm{End}_{k-\mathrm{linear}}(A)$—this is called the *regular representation* of A.

PROPOSITION 1.14. *For any simple k-algebra A, the simple submodules of A (regarded as a left A-module) are the minimal left ideals in A; any two such ideals are isomorphic as left A-modules, and A is a direct sum of its minimal left ideals.*

PROOF. After Theorem 1.9, we may assume that $A = M_n(D)$ for some division algebra D. An A-submodule M of A is a left ideal, and M will be simple if and only if it is minimal. We saw in (1.6) that the minimal left ideals in $M_n(D)$ are those of the form $L(\{j_0\})$. Clearly $A = \oplus_{1 \le j \le n} L(\{j\})$ and each $L(\{j\})$ is isomorphic to D^n with its natural action of $M_n(D)$. □

THEOREM 1.15. *Let A be a simple k-algebra, and let S be a simple A-module. Then any A-module V is isomorphic to a direct sum of copies of S. In particular, it is semisimple.*

PROOF. Let S_0 be a minimal left ideal of A. The proposition shows that, as a left A-module, $A \approx S_0^n$ for some n.

Let $e_1, \dots, e_r$ be a set of generators for V as an A-module. The map

$$(a_1, \dots, a_r) \mapsto \sum a_i e_i$$

realizes V as a quotient of the A-module A^r, and hence as a quotient of S_0^{nr}. Now Proposition 1.3 shows that $V \approx S_0^m$ for some m. □

COROLLARY 1.16. *If A is a simple k-algebra, then any two simple A-modules are isomorphic, and any two A-modules having the same dimension over k are isomorphic.*

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 and associative in the sense that, for any two k-algebras A, B, there is a unique isomorphism

$$A \otimes_k B \to B \otimes_k A$$

sending $a \otimes b$ to $b \otimes a$, and for any three k-algebras A, B, C, there is a unique isomorphism

$$A \otimes_k (B \otimes_k C) \to (A \otimes_k B) \otimes_k C$$

sending $a \otimes (b \otimes c)$ to $(a \otimes b) \otimes c$.

EXAMPLE 2.1. For any k-algebra A, $A \otimes_k M_n(k) \cong M_n(A)$. To see this, note that a ring B containing a subring R 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, $A \otimes_k M_n(A') \cong M_n(A \otimes_k A')$ for any k-algebras A and A'.

EXAMPLE 2.2. For any m, n, $M_m(k) \otimes M_n(k) \cong M_{mn}(k)$. To see this, note that according to the preceding example, $M_m(k) \otimes_k M_n(k) \cong M_m(M_n(k))$, 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_{lm}) be standard bases for $M_m(k)$ and $M_n(k)$, and check that $(e_{ij} \otimes f_{lm})$ has the correct multiplication properties.

Centralizers in tensor products.

PROPOSITION 2.3. *Let A and A' be k-algebras, with subalgebras B and B', and let $C(B)$ and $C(B')$ respectively be the centralizers of B and B' in A and A'. Then the centralizer of $B \otimes_k B'$ in $A \otimes_k A'$ is $C(B) \otimes_k C(B')$.*

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 $C(B) \otimes C(B')$, which therefore contains $C(B \otimes B')$. □

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 (1.9) shows that every simple k-algebra is isomorphic to $M_n(D)$ for some division algebra D. Now $M_n(D) \cong M_n(k) \otimes_k D$, and so $Z(M_n(D)) \cong k \otimes_k Z(D) \cong Z(D)$. □

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, 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 $J(v)$ to be the set of $i \in I$ such that $a_i \neq 0$. Let W be a subspace of V. An element $w \in W$ is said to be *primordial* (relative to V and the basis $(e_i)_{i\in I}$) if

(a) $J(w)$ is minimal among the sets $J(w')$ for w' a nonzero elements of W, and
(b) in the expression $w = \sum b_i x_i$, at least one $b_i = 1$.

PROPOSITION 2.5. (a) *Let $w \in W$ be primordial, and let $w' \in V$. Then $J(w') \subset J(w)$ if and only if $w' = cw$ for some $c \in k$, in which case $w' = 0$ or $J(w') = J(w)$.*
(b) *The set of primordial elements of W generates it.*

PROOF. (a) Let $w = \sum_{i\in J(w)} a_i e_i$ and $w' = \sum_{i\in J(w')} a'_i e_i$ be elements of W with $J(w') \subset J(w)$. We may assume $w' \neq 0$, so that $J(w') \neq \emptyset$. Choose an $i_0 \in J(w')$, and set $c = a_{i_0} \cdot a'^{-1}_{i_0}$. Then $J(w - cw') \subset J(w)$ and $i_0 \notin J(w - cw')$, and so $w - cw' = 0$.

(b) Let $w = \sum_{i\in J(w)} a_i e_i \in W$. We shall use induction on the number n of elements in $J(w)$ to prove that w lies in the subspace generated by the primordial elements. For $n = 0$ the statement is obvious, and so suppose $n > 0$. Among the nonzero elements w' of W with $J(w') \subset J(w)$, choose one w_0 such that $J(w_0)$ has the fewest elements. After replacing it by a scalar multiple, we may assume that w_0 is primordial, say $w_0 = \sum b_i e_i$ with $b_{i_0} = 1$. Then $w - a_{i_0} w_0 \in W$ but $J(w - a_{i_0} w_0)$ has at most $n - 1$

elements. By induction, $w - a_{i_0}w_0$ is a linear combination of primordial elements, and so therefore is w. □

The results (and proofs) of this section do not require V to be finite-dimensional over k, and they 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 (1.9), 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. If $A \otimes_k D$ is simple, say, $A \otimes_k D \approx M_m(D')$ with D' a division algebra, then

$$A \otimes_k M_n(D) \cong M_n(A \otimes_k D) \approx M_n(M_m(D')) \cong M_{mn}(D'),$$

which is simple. Thus the proposition follows from the next lemma. □

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 vector space over D) by $\mathfrak{a} \stackrel{\text{df}}{=} \mathfrak{A} \cap (A \otimes 1)$.*

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, $J(\delta\alpha) = J(\alpha)$, and so $\alpha\delta = \delta'\alpha$ for some $\delta' \in D$ (Proposition 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. □

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

$$a \otimes a' \mapsto aa' : A \otimes_k A^{\text{opp}} \to \text{End}_k(V).$$

As $A \otimes_k A^{\text{opp}}$ is simple and the kernel of the homomorphism does not contain 1, it is injective. On counting degrees, we find that

$$[A \otimes_k A^{\text{opp}} : k] = [A : k]^2 = n^2 = [\text{End}_k(V) : k],$$

and so the homomorphism is an isomorphism. We have shown:

COROLLARY 2.9. *For any central simple k-algebra A,*

$$A \otimes_k A^{\text{opp}} \cong \text{End}_k(A) \approx M_n(k), \quad n = [A : k].$$

The Noether-Skolem Theorem.

THEOREM 2.10 (NOETHER-SKOLEM). *Let $f, g : A \to B$ be homomorphisms from the k-algebra A to the k-algebra B. If A is simple, and B is central and simple over k, then there exists an invertible element $b \in B$ such that $f(a) = b \cdot g(a) \cdot b^{-1}$ for all $a \in A$.*

PROOF. If $B = M_n(k) = \text{End}_k(k^n)$, 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 (1.16), 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

$$f \otimes 1, g \otimes 1 : A \otimes_k B^{\text{opp}} \to B \otimes_k B^{\text{opp}}.$$

Because $B \otimes_k B^{\text{opp}}$ is a matrix algebra over k, the first part of the proof shows that there exists a $b \in B \otimes_k B^{\text{opp}}$ such that

$$(f \otimes 1)(a \otimes b') = b \cdot (g \otimes 1)(a \otimes b') \cdot b^{-1}$$

for all $a \in A$, $b' \in B^{\text{opp}}$. On taking $a = 1$ in this equation, we find that $(1 \otimes b') = b \cdot (1 \otimes b') \cdot b^{-1}$ for all $b' \in B^{\text{opp}}$. Therefore (see 2.3), $b \in C_{B \otimes_k B^{\text{opp}}}(k \otimes B^{\text{opp}}) = B \otimes_k k$, 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 g is the identity map $B_1 \to B_1$. □

COROLLARY 2.12. *All automorphisms of a central simple k-algebra are inner.*

For example, the automorphism group of $M_n(k)$ is $\text{PGL}_n(k) \stackrel{\text{df}}{=} \text{GL}_n(k)/k^\times I_n$.

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 any 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.

EXAMPLE 2.13. (a) If k is algebraically closed, then $\mathrm{Br}(k) = 0$, for let D be a central division algebra over k. We have to show that $D = k$. 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) The Brauer group of $\mathbb{R}$ is cyclic of order 2. Its elements are represented by k and the usual quaternion algebra. (See Section 4 below.)

(c) The Brauer group of a finite field is zero (Theorem 4.1).

(d) The Brauer group of a nonarchimedean local field is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$ (Proposition 4.3).

(e) If K is a number field, then there is an exact sequence

$$0 \to \mathrm{Br}(K) \to \oplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

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 Chapter VIII).

REMARK 2.14. (a) Wedderburn's theorem (1.9) shows that every central simple algebra over k is isomorphic to $M_n(D)$ for some central division algebra D. Moreover, D is the opposite algebra of $\mathrm{End}_A(S)$ for any simple A-module S. Because any two simple A-algebras are isomorphic (see 1.16), this shows 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 representing the same similarity class are isomorphic.

(b) We should verify[1] that the similarity classes form a set, and not merely a class. For each $n > 0$, consider the families $(a_{ij}^l)_{1 \le i,j,l \le n}$ 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.

[1] 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 everything.

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, any two-sided ideal in $A\otimes_k K$ is generated as an A-module by its intersection with K, and therefore is 0 or $A\otimes_k K$. A general $A\approx M_n(D)$, and

$$A\otimes_k K\approx M_n(D)\otimes_k K\approx M_n(k)\otimes_k(D\otimes_k K)\approx M_n(D\otimes_k K)\approx M_n(K)\otimes_K(D\otimes_k K)$$

which is simple. □

COROLLARY 2.16. *For any 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

$$M_n(k)\otimes L\cong M_n(L),$$

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 (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 any field k, $\mathrm{Br}(k)=\cup\mathrm{Br}(K/k)$, where K runs over the finite extensions of K contained in some fixed algebraic closure k^{al}.*

PROOF. Let A be a central simple algebra over k. Then $A\otimes_k k^{\mathrm{al}}\approx M_n(k^{\mathrm{al}})$, i.e., 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 $A\otimes_k k^{\mathrm{al}}=\cup_{[K:k]<\infty}A\otimes_k K$, the $e_{ij}\in A\otimes_k K$ 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 $H^2(L/k)\approx\mathrm{Br}(L/k)$, 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.

THEOREM 3.1. *Let A be a central simple algebra over k, and let B be a simple subalgebra over 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 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 to the two embeddings $b \mapsto b \otimes 1, 1 \otimes b$ 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

$$u \cdot C(B \otimes 1) \cdot u^{-1} = C(1 \otimes B)$$

(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 any 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 1.11 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. 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 $[A:k] = [L:k]^2$.

The equivalence of (b) with (c) follows from the observation that any commutative k-subalgebra of A containing L is contained in $C(L)$. □

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, and let L be a field of finite degree over k. Then L splits A if and only if there exists an algebra B similar to A containing L and such that $[B:L] = [L:k]^2$.*

PROOF. Suppose L splits A. Then L also splits A^{opp}, say, $A^{\text{opp}} \otimes_k L = \text{End}_L(V)$. This equality states that $A^{\text{opp}} \otimes_k L$ is the centralizer of L in $\text{End}_L(V)$, and so L is the centralizer of $A^{\text{opp}} \otimes_k L$ in $\text{End}_L(V)$ (see 3.1). Let B be the centralizer of A^{opp} in $\text{End}_k(V)$. I claim that B satisfies the required conditions. Certainly, $B \supset L$, and Corollary 3.3 shows that B is central simple and that $B \otimes_k A^{\text{opp}} \cong \text{End}_k(V)$. On tensoring both sides with A and using that $A \otimes_k A^{\text{opp}}$ 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, $L = L^{\text{opp}} \subset B^{\text{opp}}$, and because $[L:k] = \sqrt{[B:k]}$, L is equal to its centralizer in B^{opp}. Therefore the centralizer of $1 \otimes L$ in $B \otimes_k B^{\text{opp}}$ is $B \otimes_k L$. When we identify $B \otimes_k B^{\text{opp}}$ with $\text{End}_k(B)$ (endomorphisms of B as a k-vector space—see 2.9), the centralizer of L becomes identified with $\text{End}_L(B)$ (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 splits D, then there is 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 2.14a), and the condition on the degrees implies that $m = 1$. □

PROPOSITION 3.8. *Any division algebra over k contains a maximal subfield separable over k.*

PROOF. We omit the proof, because we are mainly interested in fields of characteristic zero and finite fields, for which the problem doesn't arise. □

COROLLARY 3.9. *For any field k, $\text{Br}(k) = \cup \text{Br}(L/k)$ 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 $\text{Br}(k)$ is split by a finite separable extension, and therefore by a finite Galois extension. □

Central simple algebras and 2-cocycles. First, we need a remark that should have been made in Chapter II. 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 $\sigma \mapsto \varphi_m$. Then

$$(d\varphi_m)(\sigma,\tau) = \sigma m - m + m = \sigma m.$$

In particular, $(d\varphi_m)(1,1) = m$. 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.*

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 any $\sigma \in G$, Corollary 2.11 of the Noether-Skolem theorem shows that there exists an element $e_\sigma \in A$ such that

$$\sigma a = e_\sigma a e_\sigma^{-1} \text{ for all } a \in L \qquad (*).$$

Moreover, e_σ is determined by $(*)$ 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 $(*)$ can be written as

$$e_\sigma \cdot a = \sigma a \cdot e_\sigma \text{ for all } a \in L \qquad (*')$$

which says that moving e_σ past $a \in L$ replaces it with σa. Clearly $e_\sigma e_\tau$ has the property $(*)$ for $\sigma\tau$, and so

$$e_\sigma e_\tau = \varphi(\sigma,\tau) e_{\sigma\tau} \qquad (**)$$

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 $A \mapsto \gamma(A) : \mathcal{A}(L/k) \to H^2(L/k)$.

THEOREM 3.10. *The map $A \mapsto \gamma(A)$ defines a bijection*

$$\mathcal{A}(L/k)/\approx \;\to\; H^2(L/k).$$

We first need a lemma.

LEMMA 3.11. *Let $A \in \mathcal{A}(L/k)$, and define e_σ to satisfy $(*)$. Then the set $(e_\sigma)_{\sigma\in L}$ is a basis for A as a left vector space over L.*

PROOF. Note that

$$\dim_L(A) = \dim_k(A)/\dim_k(L) = n,$$

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

$$e_\tau = \sum a_\sigma \sigma$$

for some $a_\sigma \in L$. Let $a \in L$. When we compute $e_\tau a$ in two different ways,

$$e_\tau a = \tau a \cdot e_\tau = \sum_{\sigma\in J} \tau a \cdot a_\sigma e_\sigma,$$

$$e_\tau a = \sum_{\sigma\in J} a_\sigma e_\sigma a = \sum_{\sigma\in J} a_\sigma \cdot \sigma a \cdot e_\sigma$$

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 $(*)$ and $(**)$.

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 $(*)$ and $(**)$ 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 $(**)$ for A, then $f(e_\sigma)$ satisfies $(**)$ 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 $(*)$ and $(**)$. 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 3.12. *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 (**) 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 any $a \in L$,

$$(\sigma_1 a) \cdot \alpha - \alpha \cdot a = \sum a_\sigma(\sigma_1 a - \sigma a)e_\sigma \in \mathfrak{A}.$$

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 3.10.

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.*

THEOREM 3.13. *For any 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 3.13) 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 2.14) 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 3.14. *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 (see Blanchard, 1972, p94–95, or Farb and Dennis, 1993, p126–128 for the details).

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

$$\ell a \otimes_L b = a \otimes_L \ell b$$

holds for all $a \in A$, $b \in B$, $\ell \in L$.

The k-vector space V has a unique right $A \otimes_k B$-module structure such that

$$(a' \otimes_L b')(a \otimes_k b) = a'a \otimes_L b'b, \text{ all } a', a \in A,\ b', b \in B,$$

and a unique left C-module structure such that

$$(\ell e''_\sigma)(a \otimes_L b) = \ell e_\sigma a \otimes_L e'_\sigma b, \text{ all } \ell \in L, \sigma \in G, a \in A, b \in B.$$

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 noted in (1.16), 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

$$A \otimes_k B \to M_n(C).$$

□

COROLLARY 3.15. *For any separable algebraic closure k^{al} of k, there is a canonical isomorphism* $\mathrm{Br}(k) \to H^2(k^{\mathrm{al}}/k)$.

PROOF. For any 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 $[A(\varphi)]$. Now use that

$$\mathrm{Br}(k) = \cup \mathrm{Br}(L/k) \text{ (see 3.9)},$$

and

$$H^2(k^{\mathrm{al}}/k) = \cup H^2(L/k)$$

where both unions run over the finite Galois extensions L of k contained in k^{al}. □

COROLLARY 3.16. *For any field k,* $\mathrm{Br}(k)$ *is torsion, and for any 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 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 Chapter III (see III.2.3) that, for any 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 any maximal subfield L, $D^\times = \cup \alpha L^\times \alpha^{-1}$, but a finite group can not equal the union of the conjugates of a proper subgroup (the union of the conjugates has too few elements), and so $D = L$. □

The real numbers. Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. Then

$$H^2(\mathbb{C}/\mathbb{R}) \approx H^0_T(G, \mathbb{C}^\times) = \mathbb{R}^\times / \mathrm{Nm}_G(\mathbb{C}^\times) = \{\pm\}$$

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 H be the usual quaternion algebra over $\mathbb{R}$. Then the $\mathbb{C}$-linear map $A(\varphi) \to H$ 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 H.

A nonarchimedean local field. Let K be a nonarchimedean local field.

Let K be a local field, and let D be a central division algebra over K. Let $n^2 = [D : K]$.

For any subfield L of D containing K, the valuation $|\cdot|$ has a unique extension to L. Since any element α of D is contained in such a subfield of D, for example, in $K[\alpha]$, the valuation $|\cdot|$ has a unique extension to D. It is possible to verify that $|\cdot|$ is a nonarchimedean valuation 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 any 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 $d =_{df} \mathcal{O}_D/\mathfrak{P}$ is again a division algebra, and hence a field. 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

$$\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

An element of $\mathrm{Br}(K)$ 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 $G \overset{\mathrm{df}}{=} \mathrm{Gal}(L/K) = \{\sigma^i \mid 0 \le i \le n-1\}$. 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.2.9). The crossed-product algebra $A(\varphi)$ equals $\oplus_{0 \le i \le n-1} L e_i$ 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

$$\mathrm{inv}_K(A(\varphi)) = \mathrm{ord}(e_1) = \frac{1}{n}\mathrm{ord}(e_1^n) = \frac{1}{n}\mathrm{ord}(\pi) = \frac{1}{n},$$

as expected.

PROPOSITION 4.3. *The map* $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ *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 $\ell \to k$, $\ell^\times \to k^\times$ are surjective, and U_L has a filtration whose quotients are $\ell^\times$ or ℓ one finds that the norm map $U_L \to U_K$ is surjective (see III.2.2). 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.2.9). Therefore, $\mathrm{Br}(L/K)$ is cyclic of order n, and it is generated by $[A(\varphi)]$. It now follows that $\mathrm{inv}_K : \mathrm{Br}(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$ 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.

(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 division algebra. If not, then $A(\varphi^i) \sim M_r(D)$ for a 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 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 division algebra D, the order of $[D]$ in $\mathrm{Br}(K)$ is $\sqrt{[D:K]}$.

(c) Let D be a division algebra of degree n^2 over K. Because the map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ multiplies the invariant by $[L:K]$ (Theorem III.1.1), D is split by every extension L of K of degree n. Therefore (3.7), every such L can be embedded into D. Hence *every* irreducible polynomial in $K[X]$ of degree n has a root in D.

5. Complements

Semisimple algebras. A k-algebra A is said to be *semisimple* if every A-module is semisimple. Theorem 1.15 proves that a simple k-algebra is semisimple, and (yet another) theorem of Wedderburn shows that every semisimple k-algebra is a product of simple k-algebras. For any finite group G, the group algebra $k[G]$ is semisimple provided $(G:1)$ is not divisible by the characteristic of k. For more on semisimple k-algebras, see the references below.

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 of degree n over k (e.g., A a division algebra). 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

$$\begin{aligned} \{ab,c\} &= \{a,c\} + \{b,c\} \\ \{a,bc\} &= \{a,b\} + \{a,c\} \\ \{u,1-u\} &= 0. \end{aligned}$$

It is known that these relations imply that

$$\begin{aligned} \{u,v\} &= \{v,u\}^{-1} \\ \{u,-u\} &= 1 \end{aligned}$$

(see J. Rosenberg, Algebraic K-Theory and Its Applications, Springer, 1994, p214).

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. This theorem is discussed in the book (Kersten, I., Brauergruppen von Körpern, Vieweg, 1990).

EXERCISE 5.1. Let F be a field of characteristic $\neq 2$, and define the quaternion algebra $H(a,b)$ as in (1.7). Thus $H(a,b)$ has basis $1,i,j,k$ and $i^2 = a$, $j^2 = b$, $ij = -ji$. 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 $w^2 - a^2x^2 - b^2y^2 + abz^2$ has a nontrivial zero in K. (Hint: for $\alpha = w + xi + yj + zk$, let $\bar{\alpha} = w - xi - yj - zk$, and note that $\alpha\bar{\alpha} = w^2 - a^2x^2 - \cdots$)
(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 defined by $a, b \in L^\times$.
(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 $H(a,b) \approx H(a,b)^{\mathrm{opp}}$.
(j) Show that $H(a,b) \approx M_2(k)$ 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.

Notes. Brauer groups were introduced and studied by R. Brauer, E. Noether, A. Albert, H. 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, A., Les Corps Non Commutatifs, PUP, 1972.

This gives a concise elementary treatment of material in the chapter.

Herstein, I., Noncommutative Rings, Carus, 1968.

Farb, B., and Dennis, R.K., Noncommutative Algebra, Springer, 1993.

These books include the Brauer group, but also cover much more (but no number theory). The second has lots of exercises.

Much of this chapter is based on:

Serre, J-P., Applications algébriques de la cohomologie des groupes, I, II, Séminaire Henri Cartan, 1950/51.

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, p2.

In this chapter, we state and explain the theorems of global class field theory. The main theorems will be proved Chapter VII.

Throughout this chapter, K will be 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 valuations 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 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 $\mathfrak{a}$ 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

$$K^S = \{a \in K^\times \mid (a) \in I^S\} = \{a \in K^\times \mid \mathrm{ord}_\mathfrak{p}(a) = 0 \text{ all finite } \mathfrak{p} \in S\}.$$

There is a natural map $i : K^S \to I^S$ sending an element a of K^S to the ideal $a\mathcal{O}_K$. For example, if $K = \mathbb{Q}$ and S is the set of prime numbers dividing n, then I^S can be

identified with

$$\{r/s \mid r, s \in \mathbb{Z},\ r, s > 0,\ \gcd(r, n) = 1 = \gcd(s, n)\}$$

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 any 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. We first show that every ideal class $\mathcal{C}$ is represented by an ideal in I^S. Let $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals. For any nonzero $c \in \mathfrak{c}$, $\mathfrak{c}|(c)$, and so $\mathfrak{a}(c) = \mathfrak{b}(c)\mathfrak{c}^{-1}$ is an integral ideal. Therefore, $\mathcal{C}$ will be represented by an integral ideal $\mathfrak{a}$. 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 $\pi_\mathfrak{p} \in \mathfrak{p} \setminus \mathfrak{p}^2$, 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

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} \mod \mathfrak{p}^{n(\mathfrak{p})+1}$$

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.

We have shown that $I^S \to C$ is surjective. 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. □

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

$$m : \{\text{primes of } K\} \to \mathbb{Z}$$

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

$$\operatorname{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}) \iff \pi^{m(\mathfrak{p})} | (a_{\mathfrak{p}} - 1) \iff a \mapsto 1 \text{ in } (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{m(\mathfrak{p})})^\times = (\widehat{\mathcal{O}}_{\mathfrak{p}}/\widehat{\mathfrak{p}}^{m(\mathfrak{p})})^\times$$

where π is a prime element in the completion $K_{\mathfrak{p}}$ 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 $i(a) \stackrel{\text{df}}{=} (a)$ lies in $I^{S(\mathfrak{m})}$. 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.

THEOREM 1.5. *For any 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

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p}|\mathfrak{m}}} \{\pm\} \times \prod_{\substack{\mathfrak{p} \text{ finite} \\ \mathfrak{p}|\mathfrak{m}}} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \cong \prod_{\substack{\mathfrak{p} \text{ real} \\ \mathfrak{p}|\mathfrak{m}}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times,$$

where

$$\begin{aligned} K_{\mathfrak{m}} &= K^{S(\mathfrak{m})} = \{\alpha \in K^\times \mid ord_{\mathfrak{p}}(\alpha) = 0 \text{ for all } \mathfrak{p}|\mathfrak{m}_0\} \\ U &= \mathcal{O}_K^\times, \text{ the group of units in } K, \\ U_{\mathfrak{m},1} &= U \cap K_{\mathfrak{m},1}. \end{aligned}$$

Therefore, $C_{\mathfrak{m}}$ *is a finite group of order*

$$h_{\mathfrak{m}} = h \cdot (U : U_{\mathfrak{m},1})^{-1} \cdot 2^{r_0} \cdot \mathbb{N}(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 - \frac{1}{\mathbb{N}\mathfrak{p}})$$

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.4.2) 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.

LEMMA 1.6. *Let S be a finite set of prime ideals of K. Then any 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 $a, b \in \mathcal{O}_K \cap K^S$. □

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 (6.3) 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

$$\mathcal{O}_K/\mathfrak{m}_0 \cong \prod_{\mathfrak{p}|\mathfrak{m}} \mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})},$$

and hence an isomorphism of groups

$$(\mathcal{O}_K/\mathfrak{m}_0)^\times \cong \prod(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times.$$

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

$$k^\times, k, \dots, k, \quad k \stackrel{\text{df}}{=} \mathcal{O}_K/\mathfrak{p},$$

and so $(\mathcal{O}_K/\mathfrak{p}^m)^\times$ has order $(q-1)q^{m-1}$, $q = (\mathcal{O}_K : \mathfrak{p}) \stackrel{\text{df}}{=} \mathbb{N}\mathfrak{p}$. 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 1.7. (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, $K^\times/K_+ \cong \prod_{\mathfrak{p}\text{ real}}\{\pm\}$, 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 complex conjugate of ε. Then $h_\mathfrak{m} = h$ or $2h$ 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. 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 by continuity to an automorphism of 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:

$$\begin{array}{cccccccc} & \mathfrak{P} & L & - & L_{\mathfrak{P}} & - & l & \\ f & & | & & | & & | & D(\mathfrak{P}) \\ & \mathfrak{P}_D & L^{D(\mathfrak{P})} & - & K_{\mathfrak{p}} & - & k & \\ g & & | & \diagup & & & & \\ & \mathfrak{p} & K & & & & & \end{array}$$

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 $(\mathfrak{P}, L/K)$.

1.8. *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

$$\tau\sigma\tau^{-1}(\alpha) = \tau((\tau^{-1}\alpha)^q + a), \text{ some } a \in \mathfrak{P}, \text{ and}$$

$$\tau((\tau^{-1}\alpha)^q + a) = \alpha^q + \tau a \equiv \alpha^q \bmod \tau\mathfrak{P}.$$

□

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).

1.9. *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 $f(\mathfrak{P}/\mathfrak{p}) \stackrel{\text{df}}{=} [k(\mathfrak{P}) : k(\mathfrak{p})]$, and the Frobenius element in $\text{Gal}(k(\mathfrak{Q})/k(\mathfrak{P}))$ is the $f(\mathfrak{P}/\mathfrak{p})^{th}$ power of the Frobenius element in $\text{Gal}(k(\mathfrak{Q})/k(\mathfrak{p}))$. The rest is straightforward. □

1.10. *In (*1.9*), 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

$$\sigma \mapsto (\sigma|L_1, \sigma|L_2)\colon \text{Gal}(M/K) \to \text{Gal}(L_1/K)) \times \text{Gal}(L_2/K).$$

1.11. *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 (1.10). □

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 (1.11), $\mathfrak{p}$ splits completely in M if and only if it splits completely in L_1 and L_2.

2. Dirichlet 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, J.-P. Serre, Cours d'Arithmétique, PUP, 1970, Chapter VI).

Let m be an integer. A *Dirichlet character modulo m* is a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. 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 $n \mod m$. Often one extends χ to a function on all the integers by setting $\chi(n) = 0$ when $\gcd(m, n) \neq 1$. The Dirichlet character modulo m that takes 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, ibid. Propositions 10, 12, Théoòreme 1. □

On applying log to the equality in (a), one finds 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 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, ibid., Lemme 9) shows that, for any a prime to m,

$$\sum_{p \equiv a \mod m} 1/p^s = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s),$$

where $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$ and the sum is over all Dirichlet characters modulo m.

THEOREM 2.2. *For any 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

$$\sum_{p \equiv a \mod m} 1/p^s \sim \frac{1}{\varphi(m)} \chi_0(a)^{-1} f_{\chi_0}(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{1-s} \text{ as } s \downarrow 1.$$

□

COROLLARY 2.3. *For any 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 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, a Dirichlet 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 Dirichlet character* modulo $\mathfrak{m}$ is the function $\chi_0 : C_\mathfrak{m} \to \mathbb{C}^\times$ taking only the value 1.

To a Dirichlet 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 ideals in $\mathcal{O}_K$ 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*

$$\zeta_K(s) \stackrel{\text{df}}{=} \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s}} = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \chi(\mathfrak{a})/\mathbb{N}\mathfrak{a}^s.$$

THEOREM 2.4. *(a) The zeta function $\zeta_K(s)$ extends to a meromorphic function on the half-plane $\Re(s) > 0$, and*

$$\zeta_K(s) \sim \frac{2^{r_1}(2\pi)^{r_2}\text{Reg}(K)}{w_K|\Delta_{K/\mathbb{Q}}|^{1/2}} h_K \frac{1}{s-1} \text{ as } s \downarrow 1$$

where r_1 and r_2 are the numbers of real and complex primes of K respectively, $\text{Reg}(K)$ is the regulator of K (see Math 676), 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

$$\sum_{\mathfrak{p}} 1/\mathbb{N}\mathfrak{p}^s \sim \log \frac{1}{1-s} \text{ as } s \downarrow 1,$$

and one says that a set T of prime ideals in T has *Dirichlet density* δ if

$$\sum_{\mathfrak{p} \in T} 1/\mathbb{N}\mathfrak{p}^s \sim \delta \log \frac{1}{1-s} \text{ as } s \downarrow 1.$$

A similar argument to that in the previous case proves:

THEOREM 2.5. *For any 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 an 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 any 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 any finite set S of primes of K containing all primes that ramify in L, we have a homomorphism

$$\psi_{L/K} : I^S \to \text{Gal}(L/K), \quad \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} \mapsto \prod(\mathfrak{p}_i, L/K)^{n_i}$$

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 $m \equiv 1 \mod 4$ 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

$$p \mapsto (\frac{m}{p}) : I^S \to \mathrm{Gal}(K/\mathbb{Q})$$

where $(\frac{m}{p})$ is the quadratic residue symbol.

EXAMPLE 3.2. Let $L = \mathbb{Q}[\zeta_n]$ where n is a primitive n^{th} root of 1. Assume that n is odd or divisible by 4 (so that the primes ramifying in L are precisely the primes dividing n). The map sending an integer m prime to n to the automorphism $\zeta \mapsto \zeta^m$ of L is an isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\approx} (\mathbb{Z}/n\mathbb{Z})^\times$. For p not dividing n, $(p, L/K) = [p]$ (see 0.8). If r and s are positive integers prime to n, then r/s defines a class $[r/s] = [r][s]^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$, and the Artin map is the composite of

$$I^S \xrightarrow{(r/s)\mapsto[r/s]} (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{[m]\mapsto(\zeta\mapsto\zeta^m)} \mathrm{Gal}(L/\mathbb{Q}).$$

Recall (Math 676, p63) that for any finite extension of number fields L/K, the norm map $\mathrm{Nm}_{L/K}$: $I_L \to I_K$ 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 any intermediate field: $L \supset K' \supset K$. Then the following diagram commutes:*

$$\begin{array}{ccc} I^S_{K'} & \xrightarrow{\phi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow \mathrm{Nm} & & \downarrow \textit{inclusion} \\ I^S_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

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 $\mathrm{Nm}_{L/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$, 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 any prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$. But this was proved in (1.9). □

COROLLARY 3.4. *For any abelian extension L of K,*

$$\mathrm{Nm}_{L/K}(I^S_L) \subset \mathrm{Ker}(\psi_{L/K} : I^S \to \mathrm{Gal}(L/K)).$$

PROOF. Take $K' = L$ in the above diagram. □

Thus the Artin map induces a homomorphism

$$\psi_{L/K} : I^S_K / \mathrm{Nm}(I^S_L) \to \mathrm{Gal}(L/K)$$

whenever L/K is an abelian extension. Note that $I^S / \mathrm{Nm}(I^S_L)$ is still an infinite group, 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 $\psi : I^S \to G$ *admits a modulus* if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \subset S$ 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 $S(\mathfrak{m}) \subset S$.

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 $\psi : I^S \to \mathrm{Gal}(L/K)$ 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 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. 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 any congruence subgroup H modulo $\mathfrak{m}$, there exists an abelian extension L/K 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,*

$$\begin{aligned} L_1 \subset L_2 &\iff \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \supset \mathrm{Nm}(C_{L_2,\mathfrak{m}}); \\ \mathrm{Nm}(C_{L_1 \cdot L_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cap \mathrm{Nm}(C_{L_2,\mathfrak{m}}); \\ \mathrm{Nm}(C_{L_1 \cap L_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{L_1,\mathfrak{m}}) \cdot \mathrm{Nm}(C_{L_2,\mathfrak{m}}). \end{aligned}$$

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

$$(I^{S(\mathfrak{m})} : i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S(\mathfrak{m})}) = [L : K].$$

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.

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 $\psi_{L/K} : I^{S(\mathfrak{m})} \to G$ takes the value 1 on $i(K_{\mathfrak{m},1})$. Consider the map in Theorem 1.5

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \hookrightarrow K_\mathfrak{m}/K_{\mathfrak{m},1} \xrightarrow{i} C_\mathfrak{m} \xrightarrow{\psi_{L/K}} G.$$

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* of L/K.[1] 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 $\mathfrak{f}|\mathfrak{m}$. Every abelian extension of K is contained in $L_\mathfrak{m}$ for some $\mathfrak{m}$.

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 (i.e., such that each finite prime is unramified in the usual sense, and each real prime remains 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 $\mathbb{Q}[\zeta_m]$. 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 $K = \mathbb{Q}[\sqrt{d}]$ by finding the smallest integer m such that $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_m]$.

First, consider an odd prime p. Then $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ 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 $\mathbb{Q}[\zeta_{4n}]$

[1] Führer in German—in Germany in the 1930s, conversations in public on class field theory could be hazardous.

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 $K/\mathbb{Q}$.

EXERCISE 3.12. 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 0.1).

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 3.13. 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 minimum 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.)

EXERCISE 3.14. 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) $\mathfrak{m}(\mathfrak{p}) = 0 \implies \mathfrak{p}$ 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 $I^{S \cup S(\mathfrak{m})}/H \cong \mathrm{Gal}(L/K)$; moreover, every field L satisfying (a) is the S-class field for some H.

Hint: Show $I^{S \cup S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \cong I^{S(\mathfrak{m})}/ <S> \cdot i(K_{\mathfrak{m},1})$, where $<S>$ 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 3.15 (NORM LIMITATION THEOREM). *Let L be a Galois extension of K, and let L'/K be the maximal abelian subextension of L/K. For any defining modulus $\mathfrak{m}$ for L'/K,*

$$i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) = i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L'/K}(I_{L'}^{S(\mathfrak{m})}).$$

This indicates that, for a nonabelian extension L/K, $\mathrm{Spl}(L/K)$ is not described by congruence conditions.

The principal ideal theorem. The following theorem was conjectured by Hilbert about 1900.

THEOREM 3.16. *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.

Suppose we have fields

$$L \supset K' \supset K$$

with L Galois over K (not necessarily abelian). For any 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:

$$\begin{array}{ccc} I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ \Big\downarrow{\scriptstyle \text{can.}} & & \Big\downarrow{\scriptstyle ?} \\ I_{K'}^S & \xrightarrow{\psi_{L/K'}} & \mathrm{Gal}(L/K')^{\mathrm{ab}}. \end{array}$$

What is the map "?" making the diagram commute?

Before describing it, we 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 3.17. *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, M. Hall, The Theory of Groups, Macmillan, 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.

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

$$V : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/K')^{\mathrm{ab}}.$$

Emil Artin showed that this is the map making the above diagram commute (cf. II.2.9b).

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 maximal 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 diagram becomes

$$\begin{array}{ccc} C_K & \xrightarrow{\approx} & \mathrm{Gal}(K'/K) \\ \downarrow{\scriptstyle \text{can.}} & & \downarrow{\scriptstyle V} \\ C_{K'} & \xrightarrow{\approx} & \mathrm{Gal}(K''/K'), \end{array}$$

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 3.18. *Let G be a finite group, and let H be its commutator subgroup; then*

$$V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$$

is zero.

PROOF. This is a theorem in group theory. It was proved by Furtwängler in 1930. For a simple proof, see: Witt, Proc. International Congress of Mathematicians, Amsterdam, 1954, Vol 2, pp71–73. □

REMARK 3.19. 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 3.20. 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 $K^{(n)}$. Note that the same argument that proved K'' is Galois over K shows that $K^{(n)}$ 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's article in Cassels and Fröhlich 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 any prime ideal $\mathfrak{p}$ of K unramified in L,

$$(\mathfrak{p}, L/K) \stackrel{\text{df}}{=} \{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}$$

is a conjugacy class in G.

THEOREM 3.21 (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 $(G : 1)$.*

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 $C_{\mathfrak{m}} \to \text{Gal}(L/K)$ 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 3.22. *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 $\text{Spl}_S(L/K)$ be the set of primes of K not in S that split in L.

THEOREM 3.23. *If L and M are Galois extensions of K, then*

$$L \subset M \iff \text{Spl}_S(L/K) \supset \text{Spl}_S(M/K).$$

Hence

$$L = M \iff \text{Spl}_S(L/K) = \text{Spl}_S(M/K).$$

PROOF. As a consequence of (1.11),

$$\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K).$$

Hence

$$\mathrm{Spl}_S(L/K) \supset \mathrm{Spl}_S(M/K) \implies \mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(M/K),$$

which, by the Chebotarev density theorem, implies

$$[LM : K] = [M : K],$$

and so $L \subset M$. The reverse implication is obvious. □

REMARK 3.24. (a) Theorem 3.23 is not true without the Galois assumption (see Cassels and Fröhlich 1967, p363).

(b) In the statement of Theorem 3.23, 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 (ibid. p363, 6.2).

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 $K_{\mathfrak{m},1}$ 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 3.25 (FÜHRERDISKRIMINANTENPRODUKTFORMEL). *For any finite abelian extension L/K of number fields with Galois group G,*

$$\mathrm{disc}(L/K) = \prod_{\chi \in G^\vee} \mathfrak{f}_0(\chi \circ \psi_{L/K}), \quad G^\vee \stackrel{\mathrm{df}}{=} \mathrm{Hom}(G, \mathbb{C}^\times);$$

$$\mathfrak{f}(L/K) = \mathrm{lcm}\mathfrak{f}(\chi \circ \psi_{L/K}).$$

Clearly $\cap \mathrm{Ker}(\chi : G \to \mathbb{C}^\times) = 0$, from which the second statement follows. We omit the proof of the first—it is really a statement about local fields.

REMARK 3.26. 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 3.27. Let $L = \mathbb{Q}[\sqrt{d}]$. Then $G \approx \mathbb{Z}/2\mathbb{Z}$, and there are only two characters $G \to \mathbb{C}^\times$, one χ_0 trivial and the other χ_1 injective. 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 3.28. Let $L = \mathbb{Q}[\zeta_p]$, p an odd prime. Then $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$, 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 3.29. Verify the conductor-discriminant formula for the extension $\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q}$.

REMARK 3.30. 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 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 $L \overset{\text{df}}{=} K[\sqrt[n]{a}]$ 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

$$\left(\frac{a}{\mathfrak{p}}\right)_n = 1 \iff a \text{ is an } n^{th} \text{ power modulo } \mathfrak{p},$$

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, and let S be a nonempty finite set of prime ideals of K. Does there exist for every prime number p not divisible by any prime in S a sequence of fields $\dots, L_n, L_{n+1}, \dots$ 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 $S = \{\ell\}$.

More explicitly (and slightly harder), fix a prime ℓ in $\mathbb{Q}$. Does there exist for every prime $p \neq \ell$ a sequence of monic irreducible polynomials $f_n(X) \in \mathbb{Z}[X]$ such that

(a) $\mathrm{disc}(f_n(X))$ is not divisible by any prime other than ℓ;
(b) $p^n | \deg f_n(X)$.

See (Milne, Arithmetic Duality Theorems, Academic Press, 1986, p60/61) to find where this problem turned up. It is certainly very difficult.

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 a quadratic imaginary 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 [2] 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 a quadratic imaginary field [3], Proc. Symp. Pure Math. XXVIII, Part 1, AMS, 1976. 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 a quadratic imaginary 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 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

[2] For a careful account of Kronecker's idea and work on it, see Schappacher, N., On the history of Hilbert's twelfth problem, I, Paris 1900—Zürich 1932: The comedy of errors (preprint).

[3] See pp18-20 of *Mathematical Developments arising from Hilbert's Problems*

of K. Then $G \overset{\text{df}}{=} \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/K)$ is a subgroup of index 2 in $G' \overset{\text{df}}{=} \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/F)$, and the corresponding Verlagerung is a homomorphism $V : G'^{\mathrm{ab}} \to G^{\mathrm{ab}}$. In this case, V has a very simple description.

THEOREM 3.31. *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*

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

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 Wafa Wei's thesis (Michigan 1993). □

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.) 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 philosophy, which is a vast interlocking series of conjectures, and some progress has been made, especially in the local case and the function field case (Drin'feld). 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 W. Raskind, Abelian class field theory of arithmetic schemes, Proc. Symp. Pure Math, AMS, Vol 58.1 (1995), 85–187).

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.

Topological groups. A group G with a topology is called a *topological group* if the maps

$$g, g' \mapsto gg' \colon G \times G \to G, \quad g \mapsto g^{-1} \colon G \to G$$

are continuous. The translation map

$$g \mapsto ag \colon G \to G$$

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:

$$\begin{aligned}
|\cdot|_v &= \text{the normalized valuation for } v \text{ (for which the product formula holds)},\\
K_v &= \text{the completion of } K \text{ at } v,\\
\mathfrak{p}_v &= \text{the corresponding prime ideal in } \mathcal{O}_K, \text{ (when } v \text{ is finite)},\\
\mathcal{O}_v &= \text{the ring of integers in } K_v,\\
U_v &= \mathcal{O}_v^\times\\
\widehat{\mathfrak{p}}_v &= \text{the completion of } \mathfrak{p}_v = \text{maximal ideal in } \mathcal{O}_v.
\end{aligned}$$

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

$$1 + \widehat{\mathfrak{p}}_v \supset 1 + \widehat{\mathfrak{p}}_v^2 \supset 1 + \widehat{\mathfrak{p}}^3 \supset \cdots$$

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

$$\mathbb{I}_K = \{(a_v) \in \prod K_v^\times \mid a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\}.$$

For any 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 $\mathbb{I}_K$ 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

$$\prod_v U_v = \begin{cases} U_v & \text{open in } K_v^\times \text{ for all } v; \\ U_v & = \mathcal{O}_v^\times \text{ for almost all } v. \end{cases}$$

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 an enlargement of the ideals: it includes factors for the infinite primes, and it includes the units at the finite primes. Note that $\mathbb{I}_K/\mathbb{I}_{S_\infty} \approx \mathbb{Z}^{(\mathbb{N})}$ (direct sum of countably many copies of $\mathbb{Z}$ with the discrete topology), but that $\prod K_v^\times/\mathbb{I}_{S_\infty} \approx \mathbb{Z}^{\mathbb{N}}$ (*product* of countably many copies of $\mathbb{Z}$, which is itself uncountable).

4.2. There is a canonical injective (diagonal) homomorphism

$$a \mapsto (a, a, a, \dots) \colon K^\times \to \mathbb{I}_K.$$

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 any $a \in K^\times \cap U$,

$$\begin{cases} |a-1|_v < \varepsilon & \text{for all } v \in S \\ |a|_v = 1 & \text{for all } v \notin S. \end{cases}$$

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 $a = 1$.

The quotient $\mathbf{C} = \mathbb{I}/K^\times$ 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

$$a \mapsto (1, \dots, 1, a, 1, \dots 1) \colon K_v^\times \to \mathbb{I}$$

(a in the v^{th} 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: $U_K \overset{\text{df}}{=} \mathcal{O}_K^\times$ is open, and a fundamental system of neighbourhoods of 1 is formed by the subgroups of U_K of finite index (nontrivial theorem). 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.

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

$$W_\mathfrak{m}(\mathfrak{p}) = \begin{cases} \mathbb{R}_{>0} & \mathfrak{p} \text{ real} \\ 1 + \widehat{\mathfrak{p}}^{m(\mathfrak{p})} & \mathfrak{p} \text{ finite.} \end{cases}$$

Thus, in each case, $W_\mathfrak{m}(\mathfrak{p})$ is a neighbourhood of 1 in $K_\mathfrak{p}^\times$, and

$$K_{\mathfrak{m},1} = K^\times \cap \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}).$$

Define

$$\begin{aligned} \mathbb{I}_{\mathfrak{m}} &= \left(\prod_{\mathfrak{p}\nmid\mathfrak{m}} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p})\right) \bigcap \mathbb{I} \\ W_{\mathfrak{m}} &= \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p}\text{ infinite}}} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p}\text{ finite}}} U_{\mathfrak{p}}. \end{aligned}$$

Thus

$$(a_{\mathfrak{p}}) \in \mathbb{I}_{\mathfrak{m}} \iff a_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p}) \text{ for all } \mathfrak{p}|\mathfrak{m},$$

$$(a_{\mathfrak{p}}) \in W_{\mathfrak{m}} \iff (a_{\mathfrak{p}}) \in \mathbb{I}_{\mathfrak{m}} \text{ and } a_{\mathfrak{p}} \text{ is a unit for all finite } \mathfrak{p}\nmid\mathfrak{m}.$$

Note that $\mathbb{I}_{\mathfrak{m}} \cap K^{\times} = K_{\mathfrak{m},1}$ (intersection inside $\mathbb{I}$).

PROPOSITION 4.6. *Let $\mathfrak{m}$ be a modulus of K.*

(a) *The map $id : \mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})}$ defines an isomorphism*

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cdot W_{\mathfrak{m}} \xrightarrow{\approx} C_{\mathfrak{m}}.$$

(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

$$K_{\mathfrak{m},1} \to \mathbb{I}_{\mathfrak{m}} \xrightarrow{id} I^{S(\mathfrak{m})}.$$

The first map is injective, and the second is surjective with kernel $W_{\mathfrak{m}}$, and so the kernel-cokernel sequence (II.4.2) 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 (Theorem 6.3 below). 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 any abelian extension L/K, 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) *$\phi(\mathbf{a}) = \psi(id(\mathbf{a}))$, all $\mathbf{a} \in \mathbb{I}^S \stackrel{\text{df}}{=} \{\mathbf{a} \mid a_v = 1 \text{ all } v \in S\}$.*

Moreover, every continuous homomorphism $\phi : \mathbb{I} \to G$ satisfying (b) arises from a ψ.

PROOF. Because ψ is admits a modulus $\mathfrak{m}$, it factors through $I^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) = C_{\mathfrak{m}}$. Hence we have the diagram:

$$\begin{array}{ccccc} I^{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} & \xrightarrow{\psi} & G \\ & & \uparrow\approx & & \\ \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} & \longrightarrow & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} & & \\ \downarrow\approx & & & & \\ \mathbb{I} \longrightarrow \mathbb{I}/K^\times. & & & & \end{array}$$

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

$$\phi(\mathbf{a}) = \psi(id(\mathbf{a})) \text{ for all } \mathbf{a} \in \mathbb{I}_{\mathfrak{m}},$$

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 (Theorem 6.3): 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's article in Cassels and Fröhlich 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 $\psi(\mathbf{a}) = 1$. In fact, (a) and (b) say that we can multiply $\mathbf{a}$ with idèles of certain types without changing the value $\psi(\mathbf{a})$. 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 $\ell \neq p$, the map sends (ℓ) to the Frobenius automorphism at ℓ, $\zeta \mapsto \zeta^\ell$. 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 $\mathbf{a} = (a_\infty, a_2, \dots, a_p, \dots, a_\ell, \dots)$ be an idèle of $\mathbb{Q}$. If $a_\infty = 1 = a_p$, then $\phi(\mathbf{a}) = \phi(id(\mathbf{a}))$. Thus $\phi(\mathbf{a}) = \zeta_p^m$ where $m = \prod \ell^{\mathrm{ord}_\ell(a_\ell)}$.

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 $(p, p, \dots)$.

Now 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 $c = a_0 + \cdots + a_s p^s \in \mathbb{Z}$. Then $uc \in 1 + p^{s+1}\mathbb{Z}_p$, i.e., for large s it is "close to 1". Write

$$\mathbf{a}c = (c, c, \dots, c, \overset{\ell|c}{1}, c, \dots, \overset{p}{u}\, c, c, \dots)(1, \dots, 1, \overset{\ell|c}{c}, 1, \dots).$$

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, ϕ(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 ϕ(second factor) maps ζ to ζ^c. In conclusion,

$$\phi(\mathbf{a})(\zeta) = \zeta^c = \zeta^{u^{-1}}.$$

Because ϕ is a homomorphism, this completes the explicit description of it.

REMARK 4.11. The map $\pi_\mathfrak{m} : \mathbb{I} \to C_\mathfrak{m}$ is the unique continuous homomorphism such that

(a) $\pi_\mathfrak{m}(K^\times) = 1$;
(b) $\pi_\mathfrak{m}(\mathbf{a}) = id(\mathbf{a})$ for all $\mathbf{a} \in \mathbb{I}^{S(\mathfrak{m})}$.

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 $\pi : \mathbb{I} \to \varprojlim C_\mathfrak{m}$. We wish to determine the kernel and image of this map.

Because each map $\pi_\mathfrak{m} : \mathbb{I} \to C_\mathfrak{m}$ 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.

Norms of idèles. Let L be a finite extension of the number field K, let v be a prime of K. Recall from (Math 676, 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:

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{\text{id}} & I_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\text{id}} & I_K. \end{array}$$

Thus we get a commutative diagram:

$$\begin{array}{ccc} \mathbf{C}_L & \longrightarrow & C_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ \mathbf{C}_K & \longrightarrow & C_K \end{array}$$

($\mathbf{C}_K$ = 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.1.9), and for (c), see III.2.2. □

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 Theorms 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 $D(w) \cong \mathrm{Gal}(L_w/K_v)$. Local class field theory provides us with a homomorphism (the local Artin map)

$$\phi_v : K_v \to D(w) \subset G.$$

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*

$$\begin{array}{ccc} K_v & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\mathbf{a}\mapsto\phi_K(\mathbf{a})|L} & \mathrm{Gal}(L/K) \end{array}$$

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,

$$\begin{array}{ccc} \mathbb{I}_{K'}^S & \xrightarrow{\phi_{L/K'}} & \mathrm{Gal}(L/K') \\ \big\downarrow{\scriptstyle \mathrm{Nm}} & & \big\downarrow{\scriptstyle \text{inclusion}} \\ \mathbb{I}_K^S & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

commutes. On taking $K' = L$, we find that $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$ is contained in the kernel of $\phi_{L/K}$. In particular, the kernel of $\phi_{L/K}$ contains an open subgroup of $\mathbb{I}_L$ (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*

$$\phi_{L/K} : \mathbb{I}_K/(K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K).$$

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

$$\phi_{L/K} : \mathbf{C}_K/\mathrm{Nm}(\mathbf{C}_L) \to \mathrm{Gal}(L/K).$$

EXAMPLE 5.4. Statement (a) of the theorem says that, for any $b \in K^\times$, $\prod \phi_v(b) = 1$. 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.4.3).

THEOREM 5.5 (EXISTENCE THEOREM). *Fix an algebraic closure K^{al} of K; for every open subgroup $N \subset \mathbf{C}_K$ of finite index, there exists a unique abelian extension L of K contained in K^{al} such that $\mathrm{Nm}_{L/K}\, \mathbf{C}_L = N$.*

The subgroups N open and of finite index in $\mathbf{C}_K$ are called the *norm groups,* and the abelian extension L of K such that $\mathrm{Nm}(\mathbf{C}_L) = N$, 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. In the number field case, all subgroups of finite index in $\mathbf{C}_K$ are open.

COROLLARY 5.6. *The map $L \mapsto \mathrm{Nm}(\mathbf{C}_L)$ is a bijection from the set of finite abelian extensions of K to the set of open subgroups of finite index in $\mathbf{C}_K$. Moreover,*

$$\begin{array}{rcl} L_1 \subset L_2 & \iff & \mathrm{Nm}(\mathbf{C}_{L_1}) \supset \mathrm{Nm}(\mathbf{C}_{L_2}); \\ \mathrm{Nm}(\mathbf{C}_{L_1 \cdot L_2}) & = & \mathrm{Nm}(\mathbf{C}_{L_1}) \cap \mathrm{Nm}(\mathbf{C}_{L_2}); \\ \mathrm{Nm}(\mathbf{C}_{L_1 \cap L_2}) & = & \mathrm{Nm}(\mathbf{C}_{L_1}) \cdot \mathrm{Nm}(\mathbf{C}_{L_2}). \end{array}$$

REMARK 5.7. (a) In the number field case, the map

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

is surjective. For an infinite prime v of K, write K_v^+ for the connected component of $K_v^\times$ containing 1; thus $K_v^+ \approx \mathbb{C}^\times$ 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 $\mathbf{C}_K$ is the connected component of $\mathbf{C}_K$ containing 1.

(b) In the function field case, the Artin map $\phi_K : \mathbb{I}_K/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is injective, but it is not surjective (its image is dense).

REMARK 5.8. Assume that the global Artin map $\phi : \mathbb{I} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ contains $K^\times$ in its kernel. Then, for every finite abelian extension L/K, $\phi_{L/K} : \mathbb{I} \to \mathrm{Gal}(L/K)$ arises (as in Proposition 4.7) from a homomorphism $\psi : I^S \to \mathrm{Gal}(L/K)$ 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.

Example.

LEMMA 5.9. *The map*

$$(r, t, (u_p)) \mapsto (rt, ru_2, ru_3, ru_5, \dots) : \mathbb{Q}^\times \times \mathbb{R}_{>0} \times \prod \mathbb{Z}_p^\times \to \mathbb{I}_\mathbb{Q}$$

is an isomorphism of topological groups ($\mathbb{Q}^\times$ with the discrete topology).

PROOF. Any idèle $\mathbf{a} = (a_\infty, a_2, \dots, a_p, \dots)$ can be written

$$\mathbf{a} = a(t, u_2, u_3, u_5, \dots), \quad a \in \mathbb{Q}^\times, \quad t \in \mathbb{R}_{>0}, \quad u_p \in \mathbb{Z}_p^\times;$$

—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

$$\mathbf{C}_\mathbb{Q} \to \mathbb{R}_{>0} \times \prod_{p \text{ finite}} \mathbb{Z}_p^\times = \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times.$$

Let

$$\mathbb{Q}^{\mathrm{cyc}} = \bigcup \mathbb{Q}[\zeta_n].$$

In this case, the global reciprocity map is

$$\phi : \mathbb{I}_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$$

where $\mathbb{I}_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times$ is the above projection map, and $\widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$ is the canonical isomorphism (see I.5.5c).

EXERCISE 5.10. Show that every subgroup of finite index in $\mathbf{C}_K$ is open (K a number field).

Hint: Use that every subgroup of $K_v^\times$ of finite index is open.

6. Appendix: Review of some Algebraic Number Theory

The weak approximation theorem. The theorem in this subsection should have been proved in Math 676. Recall that a valuation on a field K is homomorphism $a \mapsto |a| : K^\times \to \mathbb{R}_{>0}$ such that $|a+b| \le |a| + |b|$ for all $a, b \in K^\times$. We extend it to K by setting $|0| = 0$. A valuation is *trivial* if $|a| = 1$ for all $a \neq 0$. Two nontrivial valuations $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if $|a|_1 < 1$ implies $|a|_2 < 1$, in which case $|\cdot|_2 = |\cdot|_1^r$ for some $r \in \mathbb{R}_{>0}$ (Math 676, 7.8). The statements in this section continue to hold if we replace "valuation" with "positive power of a valuation" (which, in the archimedean case, may fail to satisfy the triangle rule).

LEMMA 6.1. *If $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ are nontrivial inequivalent valuations of K, then there is an element $a \in K$ such that*

$$\begin{cases} |a|_1 > 1 \\ |a|_i < 1, \quad i \neq 1. \end{cases}$$

PROOF. First let $n = 2$. Because $|\ |_1$ and $|\ |_2$ are inequivalent, there are elements b and c such that

$$\begin{cases} |b|_1 < 1, & |b|_2 \ge 1 \\ |c|_1 \ge 1, & |c|_2 < 1. \end{cases}$$

Now $a = \frac{c}{b}$ has the required properties.

We proceed by induction assuming that the lemma is true for $n-1$ valuations. There exist elements b, c such that

$$\begin{cases} |b|_1 > 1, & |b|_i < 1, \quad i = 2, 3, \dots, n-1 \\ |c|_1 < 1, & |c|_n > 1 \end{cases}$$

If $|b|_n \le 1$, then $a = cb^r$ works for sufficiently large r. If $|b|_n > 1$, then $a_r = \frac{cb^r}{1+b^r}$ works for sufficiently large r, because $\frac{b^r}{1+b^r}$ converges to 0 or 1 according as $|b| < 1$ or $|b| > 1$. □

LEMMA 6.2. *In the situation of the last lemma, there exists an element of K that is close to 1 for $|\cdot|_1$ and close to 0 for $|\cdot|_i$, $i = 2, \dots n$.*

PROOF. Choose a as in (6.1), and consider $a_r = \frac{a^r}{1+a^r}$. Then

$$|a_r - 1|_1 = \frac{1}{|1+a^r|_1} \le \frac{1}{|a|_1^r - 1} \to 0$$

as $r \to \infty$. For $i \ge 2$,

$$|a_r|_i = \frac{|a|_i^r}{|1+a|_i^r} \le \frac{|a|_i^r}{1-|a|_i^r} \to 0$$

as $r \to 0$. □

THEOREM 6.3. *Let $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ be nontrivial inequivalent valuations of a field K, and let $a_1, \dots, a_n$ be elements of K. For any $\varepsilon > 0$, there is an element $a \in K$ such that $|a - a_i|_i < \varepsilon$ for all i.*

PROOF. Choose b_i, $i = 1, \dots, n$, close to 1 for $|\ |_i$ and close to 0 for $|\ |_j$, $j \neq i$. Then

$$a = a_1 b_1 + \cdots + a_n b_n$$

works. □

Let K_i be the completion of K for $|\cdot|_i$. The statement of the theorem also holds with a_i in K_i (rather than K)—choose $a_i' \in K$ very close to a_i and $a \in K$ very close to each a_i'. Thus K (embedded diagonally) is dense in $\prod K_i$.

The theorem shows that there can be no finite product formula. More precisely:

COROLLARY 6.4. *Let $|\cdot|_1$, $|\cdot|_2$, ... , $|\cdot|_n$ be nontrivial inequivalent valuations on a field K. If*

$$|a|_1^{r_1} \cdots |a|_n^{r_n} = 1, \quad r_i \in \mathbb{R},$$

for all $a \in K^\times$, then $r_i = 0$ for all i.

PROOF. If any $r_i \neq 0$, an a for which $|a|_i$ is sufficiently large and the $|a|_j$, $j \neq i$, are sufficiently small provides a contradiction. □

The reader should compare the Weak Approximation Theorem with what the Chinese Remainder Theorem gives.

EXERCISE 6.5. Let $|\cdot|_1$, ... , $|\cdot|_n$ be the valuations on a number field K corresponding to distinct prime ideals $\mathfrak{p}_i$, and let $a_1, \dots, a_n$ be elements of K. Let d be a common denominator for the a_i (so that $da_i \in \mathcal{O}_K$). Show that, for any $\varepsilon > 0$, there is an element $a \in K$ such that $|a - a_i|_i < \varepsilon$ for $i = 1, \dots, n$ and $|a| \leq 1/|d|$ for all valuations $|\cdot|$ corresponding to prime ideals other than the $\mathfrak{p}_i$.

Hint: Apply the Chinese Remainder Theorem to the da_i.

Notes: The Weak Approximation Theorem first occurs in: Artin, E., and Whaples, G., Axiomatic characterization of fields by the product formula for valuations, Bull. AMS, 51, 1945, pp. 469–492. Our account follows the original.

The decomposition of primes. Recall the following theorems from Math 676.

THEOREM 6.6. *Let A be a Dedekind domain with field of fractions K, and let L be a finite separable extension of K of degree n. Let B be the integral closure of A in K.*

(a) *Let $\mathfrak{p}$ be a prime ideal of A and write*

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^e, \quad f_i \stackrel{\text{df}}{=} [B/\mathfrak{P}_i : A/\mathfrak{p}_i].$$

Then

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

If L is Galois over K, then $\mathrm{Gal}(L/K)$ acts transitively on the $\mathfrak{P}_i$, and the numbers e_i, f_i are independent of i: $n = efg$.

(b) *A prime $\mathfrak{p}$ ramifies in L (i.e., at least one of the e_i is > 1) if and only if $\mathfrak{p} | \operatorname{disc}(B/A)$.*

Note that, for a Galois extension, except for the finitely many primes that ramify, the type of the decomposition of $\mathfrak{p}B$ into prime factors is described by the single number f.

THEOREM 6.7. *Let K and A be as in the preceding theorem, and let $f(X)$ be a monic polynomial in $A[X]$. Let $L = K[\alpha]$ with α a root of $f(X)$, and let B be the integral closure of A in L. The following conditions on $\mathfrak{p}$ 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 $f(X)$ that give a field automorphism form an abelian group; Theorem 6.7 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.

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 any 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 any 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

$$\chi : I^{\mathfrak{m}} \to \mathbb{C}^\times$$

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

$$\psi : \mathbb{I}_K/K^\times \to \mathbb{C}^\times$$

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

$$\rho : G \to \mathrm{GL}(V)$$

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

$$P_\sigma(T) \overset{\text{df}}{=} \det(1-\rho(\sigma)T \mid V) = \prod_{i=1}^{\dim V} (1-a_i(\sigma)T), \qquad a_i \in \mathbb{C},$$

be the characteristic polynomial of $\rho(\sigma)$. Because $P_\sigma(T)$ depends only on the conjugacy class of σ, for any 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 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 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) $S(x) \le Cx$. 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, Algebraic Number Theory, CUP, 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, Cours..., 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

$$(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots) - 2(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \cdots) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots,$$

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.,

$$\zeta(s) = \frac{1}{s-1} + \text{function holomorphic near 1.}$$

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 $s = 1$

$$f(s) = \frac{a_0}{s-1} + \text{holomorphic function}$$

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. It is a standard fact that $\prod_{n=1}^{\infty} 1+b_n$ 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 $\Pi_m =_{df} \prod_1^m 1+b_n$ and $\Sigma_m =_{df} \sum_1^m b_n$ 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,

$$(\sum_{i=1}^{l} a_i)(\sum_{i=1}^{m} b_i)(\sum_{i=1}^{n} c_i)$$

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. 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 any class $\mathfrak{k}$ in $C_\mathfrak{m} \overset{\text{df}}{=} I^\mathfrak{m}/i(K_{\mathfrak{m},1})$, 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 any 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 Math 676 that there is a homomorphism

$$\ell : U \longrightarrow \mathbb{R}^{r+s}, \quad u \mapsto (\log|\sigma_1(u)|, \dots, 2\log|\sigma_{r+s}(u)|)$$

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 $\ell(U_{\mathfrak{m},1})$. Thus $\operatorname{reg}(\mathfrak{m}) = \operatorname{reg}(K)(U : U(\mathfrak{m}))$.

PROPOSITION 2.8. *For all $x \ge 1$,*

$$|S(x,\mathfrak{k}) - g_\mathfrak{m} x| \le Cx^{1-\frac{1}{d}}, \quad g_\mathfrak{m} = \frac{2^r(2\pi)^s\operatorname{reg}(\mathfrak{m})}{w_\mathfrak{m}\mathbb{N}(\mathfrak{m})|\Delta_{K/\mathbb{Q}}|^{\frac{1}{2}}}, \quad d = [K:\mathbb{Q}],$$

where

$$\begin{aligned} r &= \text{number of real primes,} \\ s &= \text{number of complex primes,} \\ w_{\mathfrak{m}} &= \text{number of roots of 1 in } K_{\mathfrak{m},1}, \\ \mathbb{N}(\mathfrak{m}) &= \mathbb{N}(\mathfrak{m}_0)2^{r_0}, \\ r_0 &= \text{number of real primes in } \mathfrak{m}, \text{ and} \\ \Delta_{K/\mathbb{Q}} &= \text{discriminant of } K/\mathbb{Q}. \end{aligned}$$

PROOF. First show that there is an integral ideal $\mathfrak{b}_0 \in \mathfrak{k}^{-1}$. Then for any $\mathfrak{a} \in \mathfrak{k}$, $\mathfrak{a}$ 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 $|\operatorname{Nm}(\alpha)| \leq x\mathbb{N}(\mathfrak{b}_0)$. 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 $\chi(b) \neq 1$. But

$$\sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ab) = (\sum_a \chi(a))\chi(b),$$

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 chaaracter, 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 $L(1, \chi) \neq 0$.

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*

$$\frac{2^r(2\pi)^s \mathrm{reg}(K)}{w_K|\Delta|^{\frac{1}{2}}} h_K$$

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

$$\lim_{s \to 1}(s-1)\zeta(s) = \begin{cases} \frac{2\log(u)}{\Delta^{\frac{1}{2}}} h_K, & u > 1 \text{ a fundamental unit }, d > 0 \\ \frac{2\pi}{w_K|\Delta|^{\frac{1}{2}}} h_K, & d < 0. \end{cases}$$

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 a quadratic imaginary 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

$$h = \frac{1}{2-0}(\chi(1) + \chi(3) + \chi(7) + \chi(9)) = \frac{4}{2} = 2,$$

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* $\delta(T) = m/n$.

PROPOSITION 3.1. (a) *The set of all prime ideals of K has polar density* 1.
(b) *The polar density of any 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 $\delta(T) = \delta(T_1) + \delta(T_2)$.*

[2]Following Marcus, Number Fields, Springer 1977, p188.

(d) *If $T \subset T'$, then $\delta(T) \leq \delta(T')$ (when both are defined).*

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 $m_1 n - m n_1$ at 1. Therefore

$$\delta(T_2) = \frac{m_1 n}{m m_1} - \frac{m n_1}{m m_1} = \delta(T) - \delta(T_2).$$

(d) Combine (c) with (b). □

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. Therefore, it suffices to prove the theorem under the assumption that L is Galois over 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, $\zeta_{K,S}(s) = \zeta_{L,T}(s)^{[L:K]}$. 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. *For Galois extensions L and M of a number field K,*

$$L \subset M \iff \mathrm{Spl}(L) \supset \mathrm{Spl}(M).$$

Hence

$$L = M \iff \mathrm{Spl}(L) = \mathrm{Spl}(M),$$

and

$$L \mapsto \mathrm{Spl}(L)$$

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.3.23). □

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 any abelian extension L/K and any finite set $S \supset S_\infty$ of primes of K including those that ramify in L, the Artin map $\psi_{L/K} : I^S \to \mathrm{Gal}(L/K)$ 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, 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, p252. □

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, Cours..., 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. All of the sets whose densities we compute in this course will also have natural densities, but we do not prove that.

(b) By definition, polar densities are rational numbers. Therefore any 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 elementary 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*

$$f(s) \stackrel{\text{df}}{=} \prod_{j=1}^{\infty} \frac{1}{1-u_j^{-s}}$$

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

$$\begin{aligned}
\log f(s) &= \sum_{j=1}^{\infty} \log\frac{1}{1-u_j^{-s}} \\
&= \sum_j \sum_{m=1}^{\infty} \frac{1}{mu_j^{sm}} \\
&= \sum_j \frac{1}{u_j^s} + \sum_j \sum_{m=2}^{\infty} \frac{1}{mu_j^{sm}} \\
&= \sum_j \frac{1}{u_j^s} + g(s),
\end{aligned}$$

where

$$|g(s)| \leq \sum_{j=1}^{\infty}\sum_{m=2}^{\infty}\left|\frac{1}{mu_j^{sm}}\right| = \sum_{j=1}^{\infty}\sum_{m=2}^{\infty}\frac{1}{mu_j^{m\sigma}}, \qquad \sigma = \Re(s).$$

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 $\delta(T'\setminus T)$, and

$$\delta(T')-\delta(T)\overset{(c)}{=}\delta(T'\setminus T)\overset{(a)}{\geq}0.$$

□

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 any 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*

$$\sum_{\chi\in A^\vee}\chi(a)=.$$

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 $a\neq1$, there is a character χ_1 such that $\chi_1(a)\neq1$. 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 $\chi_1(a)\neq1$, 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 any 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 $H = \mathrm{Nm}_{L/K}\, I_L^{\mathfrak{m}} \cdot K^\times$. 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 Reciprocity Law (Theorem V.3.5) 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

In this chapter we prove the main theorems of global class field theory, namely, the Reciprocity Law and the Existence Theorem (Theorems V.5.3, V.5.5), following the method of Tate's article in Cassels and Fröhlich 1967 (see also Artin and Tate 1951/52). Throughout, we work with idèles rather than ideals.

This chapter is independent of Chapter VI, except that Theorem VI.4.9 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.

1. Outline

Let L/K be a finite Galois extension of number fields with Galois group G. The idèle class group $\mathbf{C}_L \overset{\text{df}}{=} \mathbb{I}_L/L^\times$ 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

$$\phi : \mathbf{C}_K/\operatorname{Nm}_{L/K}(\mathbf{C}_L) \to G$$

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,

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

where ϕ_v is the local Artin map of Chapters II and IV.

According to Tate's theorem II.2.18, to obtain such an isomorphism, it suffices to prove that, for every finite Galois extension L/K with Galois group G,

(a) $H^1(G, \mathbf{C}_L) = 0$;
(b) $H^2(G, \mathbf{C}_L)$ 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 $\mathrm{Res}(u_{E/K}) = u_{L/K}$.

The isomorphism $\phi_{L/K}$ is then the inverse of that defined by $u_{L/K}$,

$$H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, \mathbf{C}_L).$$

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 $\mathbf{C}_K \to \mathrm{Gal}(L/K)$ 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 idéles in terms of the cohomology of the local fields,

$$H^0(G, \mathbb{I}_L) = \mathbb{I}_K; \quad H_T^r(G, \mathbb{I}_L) = \oplus_v H_T^r(G^v, L^{v\times})$$

(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, $(\mathbf{C}_K : \mathrm{Nm}_{L/K}\, \mathbf{C}_L) \geq [L : K]$.

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 any Galois extension L/K of number fields,
> (a) $(\mathbf{C}_K : \mathrm{Nm}_{L/K}\, \mathbf{C}_L) \leq [L : K]$ (second inequality);
> (b) $H^1(G, \mathbf{C}_L) = 1$;
> (c) $H^2(G, \mathbf{C}_L)$ has order $\leq [L : K]$.

and we prove it using Theorem VI.4.9. 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 any 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 $\mathbf{C}_K$ 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

$$(L, |\ |_w) \longrightarrow (L, |\ |_{\sigma w}),$$

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 (Math 676, 8.2) that the map

$$a \otimes b \mapsto i_w(a)b : L \otimes_K K_v \to \prod_{w|v} L_w$$

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 any $a \in L$, $\sigma(\dots, i_w(a), \dots) = (\dots, i_w(\sigma a), \dots)$.

These conditions determine the action uniquely.

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 $f_\alpha \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$, and the map*

$$\alpha \mapsto f_\alpha : \prod_{w|v} L_w \to \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$$

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

$$\mathrm{Ind}_{G_{w_0}}^G(L_{w_0}) = \{f : G \to L_{w_0} \mid f(\rho\sigma) = \rho f(\sigma), \text{ all } \rho \in G_{w_0}\}$$

and that $\tau \in G$ acts on $f \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$ 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 $f_\alpha \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$. 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 $\prod_{w|v} L_w \to \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$. Given $f \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$, 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,*

$$H^r(G, \prod_{w|v} L_w^\times) \cong H^r(G_{w_0}, L_{w_0}^\times).$$

In particular,

$$H^0(G, \prod_{w|v} L_w^\times) \cong K_v^\times.$$

Similar statements hold with $L_w^\times$ replaced with U_w.

PROOF. We have

$$H^r(G, \prod_{w|v} L_w^\times) = H^r(G, \mathrm{Ind}_{G_{w_0}}^G L_{w_0}^\times) = H^r(G_{w_0}, L_{w_0}^\times)$$

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 $r \geq 0$, $H_T^r(G, \mathbb{I}_L) = \oplus_v H_T^r(G^v, L^{v\times})$.*

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

$$\mathbb{I}_{L,S} = \prod_{v\in S}(\prod_{w|v} L_w^\times) \times \prod_{v\notin S}(\prod_{w|v} U_w).$$

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.3.3),

$$H^r(G, \mathbb{I}_L) = \varinjlim H^r(G, \mathbb{I}_{L,S}).$$

On applying (II.1.25) and (2.3), we find that

$$\begin{aligned} H^r(G, \mathbb{I}_{L,S}) &= \prod_{v\in S} H^r(G, \prod_{w|v} L_w^\times) \times \prod_{v\notin S} H^r(G, \prod_{w|v} U_w) \\ &= \prod_{v\in S} H^r(G^v, L^{v\times}) \times \prod_{v\notin S} H^r(G^v, U^v). \end{aligned}$$

Because of (III.2.1), the second factor is zero when $r > 0$, and so

$$H^r(G, \mathbb{I}_L) = \varinjlim{}_S H^r(G, \mathbb{I}_{L,S}) = \varinjlim{}_S \oplus_{v\in S} H^r(G^v, L^{v\times}) = \oplus_{\text{all } v} H^r(G^v, L^{v\times}).$$

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) $H^2(G, \mathbb{I}_L) \approx \oplus_v \left(\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}\right)$, *where* $n_v = [L^v : K_v]$.

PROOF. (a) Apply Hilbert's theorem 90.

(b) From Theorem III.1.1 we know that the invariant map gives an isomorphism

$$H^2(G^v, L^{v\times}) \xrightarrow{\approx} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}.$$

□

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

$$\mathbb{I}_{L,T} = \left(\prod_{v\in S}(\prod_{w|v} L_w^\times)\right) \times \left(\prod_{v\notin S}(\prod_{w|v} U_w)\right).$$

The Tate cohomology of the second factor is zero, and so the Herbrand quotient

$$h(G,\mathbb{I}_{L,T}) = \prod_{v\in S} h(G,\prod_{w|v} L_w^\times) = \prod_{v\in S} h(G^v, L^{v\times}) = \prod_{v\in S} \#H^2(G^v, L^{v\times}) = \prod_{v\in S} n_v.$$

□

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 (Math 676, 8.3) that there is a commutative diagram:

$$\begin{array}{ccc} L^\times & \longrightarrow & \prod_{w|v} L_w^\times \\ \big\downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \big\downarrow{\scriptstyle (a_w)\mapsto\prod \mathrm{Nm}_{L_w/K_v} a_w} \\ K^\times & \longrightarrow & K_v^\times. \end{array}$$

For any w, $\mathrm{Nm}\, L_w^\times$ is open in $K_v^\times$ (for example, because it is of finite index), and for any unramified w, the norm map sends U_w onto U_v (see III.2.2). The image of the right hand vertical map in the diagram is just $\mathrm{Nm}\, L_w^\times$ 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:

PROPOSITION 2.8. *For any 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.*

Consider

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathbf{C}_L & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \big\downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \big\downarrow & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathbf{C}_K & \longrightarrow & 0. \end{array}$$

The left hand square commutes, and so the norm map $\mathbb{I}_L \to \mathbb{I}_K$ induces a norm map $\mathbf{C}_L \to \mathbf{C}_K$. From the snake lemma, we find that the quotient map $\mathbb{I}_K \to \mathbf{C}_K$ induces an isomorphism $\mathbb{I}_K/K^\times \cdot \mathrm{Nm}(\mathbb{I}_L) \to \mathbf{C}_K$.

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

$$U(T) \stackrel{\text{df}}{=} \{\alpha \in L \mid \text{ord}_w(\alpha) = 0 \text{ all } w \notin T\}$$

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[1] 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 (see the proof of the Normal Basis Theorem II.1.24), and hence is a $k[G]$-isomorphism $M \to N$. □

REMARK 3.3. (For the experts). It is possible to give an alternative proof of the lemma (at least when k has characteristic zero). The group H of automorphisms of M as a $k[G]$-module is a product of groups of the form $\text{GL}_d(D)$, D a division algebra over k. The functor of isomorphisms $M \to N$ is a principal homogeneous space for H

[1]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 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.

(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.*

PROOF. After (II.2.16), 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.2.16) 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 $N\overset{\text{df}}{=}\operatorname{Hom}(T,\mathbb{Z})$. 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

$$\operatorname{Hom}(T,\mathbb{Z})=\oplus_v\operatorname{Hom}(G/G^v,\mathbb{Z}).$$

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 $a\mapsto(\dots,\log|a|_w,\dots)$, 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. Math 676, 5.7). The vector $e = (1, 1, \dots, 1)$ 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,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathbf{C}_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathbf{C}_L & \longrightarrow & 0, \end{array}$$

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 $\mathbf{C}_K \to \mathbf{C}_L$ induces an isomorphism*

$$\mathbf{C}_K \to \mathbf{C}_L^G = H^0(G, \mathbf{C}_L).$$

PROOF. From the bottom row of the above diagram, we obtain a cohomology sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(G, L^\times) & \longrightarrow & H^0(G, \mathbb{I}_L) & \longrightarrow & H^0(G, \mathbf{C}_L) & \longrightarrow & H^1(G, L^\times) \\ & & \| & & \| & & \| & & \| \\ & & L^{\times G} & & \mathbb{I}_L^{\times G} & & \mathbf{C}_L^G & & 0 \end{array}$$

which can be identified with

$$0 \to K^\times \to \mathbb{I}_K \to \mathbf{C}_K \to 0.$$

□

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 $I^S = I/ <S>$, and so $I^S/i(K^\times) = 0$.

For any finite set $S \supset S_\infty$ of primes of K, the natural map $\mathbb{I} \to I^S$ defines an isomorphism $\mathbb{I}/\mathbb{I}_S \xrightarrow{\approx} I^S$. On dividing out by $K^\times$ on both sides, we find that $\mathbb{I}/K^\times \cdot \mathbb{I}_S \cong I^S/i(K^\times) \cong 0$. □

Recall that we want to prove that for any abelian extension L/K, $\mathbf{C}_K/\operatorname{Nm}_{L/K}\mathbf{C}_L \cong \operatorname{Gal}(L/K)$ and that for any Galois extension $H^1(G, C_L) = 1$. For a cyclic extension, the two statements imply that the Herbrand quotient

$$h(\mathbf{C}_L) \overset{\text{df}}{=} \frac{(\mathbf{C}_K : \operatorname{Nm}\mathbf{C}_L)}{\#H^1(G, \mathbf{C}_L)} = [L : K].$$

As a first step, we verify this equality.

THEOREM 4.3. *For any finite cyclic extension L/K of number fields, $h(\mathbf{C}_L) = [L : K]$.*

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

$$\mathbf{C}_L \overset{\text{df}}{=} \mathbb{I}_L/L^\times = L^\times \cdot \mathbb{I}_{L,T}/L^\times \cong \mathbb{I}_{L,T}/L^\times \cap \mathbb{I}_T.$$

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

$$h(\mathbf{C}_L) = h(\mathbb{I}_{L,T})/h(U(T)).$$

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 $h(\mathbf{C}_L) = n$, 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

$$D \subset \mathrm{Nm}_{L/K}(\mathbb{I}_L) = \mathrm{Nm}_{K'/K}(\mathrm{Nm}_{L/K}\,\mathbb{I}_L)) \subset \mathrm{Nm}_{K'/K}(\mathbb{I}_{K'}).$$

Therefore, $K^\times \cdot \mathrm{Nm}_{K'/K}\,\mathbb{I}_{K'}$ is dense in $\mathbb{I}_K$. Because it is a union of translates of $\mathrm{Nm}_{K'/K}\,\mathbb{I}_{K'}$, it is open (2.8), and because it is a subgroup of $\mathbb{I}_K$, it is also closed. Therefore, $K^\times \cdot \mathrm{Nm}_{K'/K}\,\mathbb{I}_{K'} = \mathbb{I}_K$, 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

$$D = \mathbb{I}^S \stackrel{\text{df}}{=} \{(a_v) \mid a_v = 1 \text{ for all } v \in S\}.$$

For $w|v \notin S$, $L_w = K_v$, and so clearly $D \subset \mathrm{Nm}(\mathbb{I}_L)$. Let $\mathbf{a} = (a_v) \in \mathbb{I}$. By the Weak Approximation Theorem (V.6.3), 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 a in $\mathbb{I}_K$. Hence $K^\times \cdot D$ is dense in $\mathbb{I}_K$. □

PROPOSITION 4.7. *For any finite solvable extension L/K with Galois group G, and any finite set of prime ideals T of L including those that ramify from K, the Frobenius elements $(\mathfrak{P}, L/K)$ for $\mathfrak{P} \notin T$ generate G.*

PROOF. Let H be the subgroup generated by the Frobenius elements at the $\mathfrak{P} \notin T$, and let $E = L^H$. Recall (V.1.10) that

$$(\mathfrak{P}, E/K) = (\mathfrak{P}, L/K)|_E,$$

which is the identity map. Therefore all primes $\mathfrak{p} \notin S$ split in E, which shows that $E = K$. By the main theorem of Galois theory, this implies that $H = G$. □

COROLLARY 4.8. *For any abelian extension L/K and finite set of primes $S \supset S_\infty$ of K including the primes that ramify in L, the map*

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

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 $\mathfrak{P}|\mathfrak{p} \in S$, 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 $H^1(G, \mathbf{C}_L) = 0$;*
(c) *the group $H^2(G, \mathbf{C}_L)$ 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 $(\mathbb{I}_K : K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) = (H^2(G, \mathbf{C}_L) : 1) = [L:K]$).*

PROOF. Without restriction on G,

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L) \cong \mathbf{C}_K/\mathrm{Nm}_{L/K}(\mathbf{C}_L) = H^0_T(G, \mathbf{C}_L).$$

If G is cyclic, its cohomology is periodic, and so $H^0_T(G, \mathbf{C}_L) \approx H^2(G, \mathbf{C}_L)$. This proves that (a) and (c) are equivalent. Theorem 4.3 states that the Herbrand quotient $h(\mathbf{C}_L) = [L:K]$, 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 any 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 $H^1_T(G, \mathbf{C}_L)$ and the power of p dividing the orders $H^0_T(G, \mathbf{C}_L)$ and $H^2_T(G, \mathbf{C}_L)$ 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 Math 594g, 4.15). Consider the exact sequence (II.1.34)

$$0 \to H^1(G/H, \mathbf{C}_{K'}) \xrightarrow{\mathrm{Inf}} H^1(G, \mathbf{C}_L) \xrightarrow{\mathrm{Res}} H^1(H, \mathbf{C}_L)$$

where $K' = L^H$. By assumption $H^1(G/H, \mathbf{C}_{K'}) = 0$ and by induction $H^1(H, \mathbf{C}_L) = 0$. Therefore $H^1(G, \mathbf{C}_L) = 0$—statement (b) is true.

Because $H^1(H, \mathbf{C}_L) = 0$, the sequence

$$0 \to H^2(G/H, \mathbf{C}_{K'}) \to H^2(G, \mathbf{C}_L) \to H^2(H, \mathbf{C}_L)$$

is exact, from which it follows that statement (c) is true.

Finally, note that

$$(\mathbf{C}_K : \mathrm{Nm}_{L/K}(\mathbf{C}_L)) = (\mathbf{C}_K : \mathrm{Nm}_{K'/K}(\mathbf{C}_{K'}))(\mathrm{Nm}_{K'/K}(\mathbf{C}_{K'}) : \mathrm{Nm}_{L/K}(\mathbf{C}_L)),$$

which divides $p[L:K']$ because $\mathrm{Nm}_{K'/K}$ defines a surjection

$$\mathbf{C}_{K'}/\mathrm{Nm}_{L/K'}(\mathbf{C}_L) \to \mathrm{Nm}_{K'/K}(\mathbf{C}_{K'})/\mathrm{Nm}_{L/K}(\mathbf{C}_L).$$

□

It therefore remains to prove that the Second Inequality holds for a cyclic extension of characteristic 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 $\mathbf{C}_K/\operatorname{Nm}(\mathbf{C}_L)$ and $H^2(G,\mathbf{C}_L)$. 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 p^{th} root of 1.*

PROOF. Let ζ be a primitive p^{th} 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:

$$\begin{array}{ccc} L & \overset{m}{\text{—}} & L' \\ |p & & |p \\ K & \overset{m}{\text{—}} & K'. \end{array}$$

The map

$$\operatorname{Gal}(L'/K) \to \operatorname{Gal}(L/K) \times \operatorname{Gal}(K'/K)$$

is an isomorphism. Consider the diagram:

$$\begin{array}{ccccccc} \mathbf{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \mathbf{C}_K & \longrightarrow & \mathbf{C}_K/\operatorname{Nm}\mathbf{C}_L & \longrightarrow & 0 \\ \downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} & & \downarrow & & \\ \mathbf{C}_{L'} & \xrightarrow{\mathrm{Nm}_{L'/K'}} & \mathbf{C}_{K'} & \longrightarrow & \mathbf{C}_{K'}/\operatorname{Nm}\mathbf{C}_{L'} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{Nm}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} & & \downarrow & & \\ \mathbf{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \mathbf{C}_K & \longrightarrow & \mathbf{C}_K/\operatorname{Nm}\mathbf{C}_L & \longrightarrow & 0 \end{array}$$

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

$$x \mapsto \sum \sigma x, \quad \sigma \in \operatorname{Gal}(L/K) = \operatorname{Gal}(L'/K'),$$

and $\mathrm{Nm}_{L'/L}$ and $\mathrm{Nm}_{K'/K}$ are the maps

$$x \mapsto \sum \sigma x, \quad \sigma \in \operatorname{Gal}(L'/L) = \operatorname{Gal}(K'/K).$$

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

$$\mathbf{C}_K/\operatorname{Nm}\mathbf{C}_L \to \mathbf{C}_{K'}/\operatorname{Nm}\mathbf{C}_{L'} \to \mathbf{C}_K/\operatorname{Nm}\mathbf{C}_L$$

is also multiplication by m, and hence is an isomorphism (clearly, p^{th} powers in $\mathbf{C}_K$ are norms, and so $\mathbf{C}_K/\operatorname{Nm}\mathbf{C}_L$ is killed by p). In particular, the second map is surjective, and so

$$(\mathbf{C}_K : \operatorname{Nm}\mathbf{C}_L) \text{ divides } (\mathbf{C}_{K'} : \operatorname{Nm}\mathbf{C}_{L'}),$$

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),

$$L = K(a_1^{\frac{1}{p}}, \dots, a_r^{\frac{1}{p}}).$$

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, by (10.5), (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

$$U(S) \approx \mathbb{Z}^{s-1} \times U(S)_{\text{tors}}, \qquad s = \#S,$$

and $U(S)_{\text{tors}}$ is a finite cyclic group. In our case, the order of $U(S)_{\text{tors}}$ 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

$$U(S) \cdot K^{\times p}/K^{\times p} \approx U(S)/U(S) \cap K^{\times p} = U(S)/U(S)^p \approx (\mathbb{Z}/p\mathbb{Z})^s.$$

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 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 that if $w'|v \notin S$, then $M_{w'}$ is an unramified extension of K_v. Hence $\mathrm{Gal}(M_w/K_v)$ is cyclic, and it has exponent p (because it is a subgroup of $\mathrm{Gal}(M/K)$). Therefore it is either cyclic of order p or trivial. In particular, if $M_{w'} \neq L_w$, then $L_w = K_v$.

According to (4.7), there is a finite set $\{w_1, \dots, w_t\}$ of primes of L, none lying over a prime in S, such that the Frobenius elements $(\mathfrak{p}_{w_i}, M/L)$ form a basis for $\mathrm{Gal}(M/L)$. Let v_i be the prime of K lying under w_i. Then, according to the above observation, $L_{w_i} = K_{v_i}$, and therefore $(\mathfrak{p}_{w_i}, M/L) = (\mathfrak{p}_{v_i}, M/K)$. We can take T to be $\{v_1, \dots, v_t\}$. □

Note that the order of T is t where $p^t = [M : L]$, and that for any $w|v \in T$, $L_w = K_v$.

LEMMA 6.3. *With the above notations,*

$$L^{\times p} \cap U(S) = \{a \in U(S) \mid a \in K_v^{\times p}, \quad \text{all } v \in T\}.$$

PROOF. $\subset$: If $a \in$ LHS, then it is in $U(S)$ and it becomes a p^{th} power in L. Therefore it is a p^{th} power in $L_w^\times$ for all w, but if $w|v \in T$, then $L_w = K_v$, and so it is a p^{th} power in K_v.

$\supset$: If $a \in U(S)$, then $a^{\frac{1}{p}} \in M$. If further a is a p^{th} power in K_v for $v \in T$, then $a^{\frac{1}{p}}$ is fixed by $(\mathfrak{p}_v, M/K)$. Since these Frobenius elements generate $\mathrm{Gal}(M/L)$, $a^{\frac{1}{p}}$ 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

$$K_v^\times / \mathrm{Nm}\, L_w^\times \xrightarrow{\approx} \mathrm{Gal}(L_w/K_v).$$

Because the second group is killed by p, so also must be the first group, which means that $K_v^{\times p} \subset \mathrm{Nm}\, L_w^\times$.

$v \in T$: 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.2.2) □

Now

$$(\mathbf{C}_K : \mathrm{Nm}\, \mathbf{C}_L) = (\mathbb{I}_K : K^\times \cdot \mathrm{Nm}\, \mathbb{I}_L),$$

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 $\mathbb{I}_K = K^\times \cdot \mathbb{I}_S = K^\times \cdot \mathbb{I}_{S \bigcup T}$, 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.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B \cap C & \longrightarrow & B & \longrightarrow & BC/C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A \cap C & \longrightarrow & A & \longrightarrow & AC/C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A \cap C/B \cap C & \longrightarrow & A/B & \longrightarrow & AC/BC & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

□

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 notations:*

$$(\mathbb{I}_{S\cup T} : E) = p^{2s}.$$

LEMMA 6.7. *With the above notations:*

$$(U(S \cup T) : K^\times \cap E) = p^{s+t}.$$

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 p^{th} 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 $\|n\|_v \neq 1$, and so

$$\prod_{v\in S} \|n\|_v = \prod_{\text{all } v} \|n\|_v,$$

which equals 1 by the product formula. □

PROPOSITION 6.8. *Let K be a local field of characteristic zero, and let U be the group of units in K. Then*

$$(U : U^n) = \frac{(\mu_n : 1)}{|n|}, \qquad (K^\times : K^{\times n}) = n\frac{(\mu_n : 1)}{|n|}$$

where μ_n is the group of n^{th} roots of 1 in $K^\times$.

PROOF. 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.3.3), 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

$$h_n(U) = h_n(\mathcal{O}_K) = (\mathcal{O}_K : n\mathcal{O}_K) \stackrel{\text{df}}{=} |n|^{-1}.$$

Hence

$$(U : U^n) = \frac{(U_n : 1)}{|n|}$$

and $U_n = \mu_n$. Since $K^\times \approx U \times \mathbb{Z}$, we have

$$(K^\times : K^{\times n}) = (U : U^n)(\mathbb{Z} : n\mathbb{Z}) = \frac{\#\mu_n}{\|n\|}n.$$

□

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

$$U(S)/H = U(S)/U(S) \cap L^{\times p} \cong U(S) \cdot L^{\times p}/L^{\times p}.$$

This last group corresponds by Kummer theory (see 10.3) 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 n^{th} 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 n^{th} 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 $d = (d_v) \in D$. 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 n^{th} 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 $\mathbb{I}_S/D = \prod_{v\in S} U_v/U_v^n$, and by hypothesis $U(S) \to \prod_{v\in S} U_v/U_v^n$ 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

Readers, especially those who skipped Chapter IV, may interprete the notation $\mathrm{Br}(L/K)$ as shorthand for $H^2(\mathrm{Gal}(L/K), L^\times)$ and $\mathrm{Br}(K)$ as shorthand for $H^2(\mathrm{Gal}(K^{\mathrm{al}}/K), K^{\mathrm{al}\times})$.

THEOREM 7.1. *For any Galois extension L/K of number fields (possibly infinite), the canonical map*

$$\mathrm{Br}(L/K) \to \oplus_v \mathrm{Br}(L^v/K_v)$$

is injective.

PROOF. Assume initially that L/K is a finite Galois extension with Galois group G. Because $H^1(G, \mathbf{C}_L) = 0$, the cohomology sequence of

$$0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$$

is

$$0 \to H^2(G, L^\times) \to H^2(G, \mathbb{I}_L) \to \cdots.$$

But

$$H^2(G, L^\times) = \mathrm{Br}(L/K)$$

and (see 2.5)

$$H^2(G, \mathbb{I}_L) = \oplus H^2(G^v, L^{v\times}) = \oplus \mathrm{Br}(L^v/K_v),$$

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 any $\beta \in \mathrm{Br}(K)$, there exists a cyclic cyclotomic extension L of K such that β maps to zero in* $\mathrm{Br}(L)$.

PROOF. The theorem shows that β is determined by its images in $\mathrm{Br}(K_v)$, and hence by the invariants $\mathrm{inv}_v(\beta_v) \in \mathbb{Q}/\mathbb{Z}$ (see Theorem III.1.1). For any finite extension L of K and prime $w|v$ of L, $\mathrm{inv}_w(\beta|L) = [L_w : K_v] \cdot \mathrm{inv}_v(\beta)$ (ibid.), and so we have to find a cyclic cyclotomic extension L/K such that

$$[L^v : K_v] \cdot \mathrm{inv}_v(\beta_v) = 0 \mod \mathbb{Z}$$

for all v. Note that, because $\mathrm{Br}(L/K)$ maps into the direct *sum* of the local Brauer groups, $\mathrm{inv}_v(\beta_v) = 0$ for almost all v. Hence there exists an integer m such that $m\,\mathrm{inv}_v(\beta_v) = 0$ 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 $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \cong (\mathbb{Z}/\ell^r\mathbb{Z})^\times$, and

$$(\mathbb{Z}/\ell^r\mathbb{Z}) \approx \begin{cases} \Delta \times C(\ell^{r-2}) & \ell \text{ odd} \\ \Delta \times C(2^{r-3}) & \ell = 2 \end{cases}$$

where Δ is of order $\ell - 1$ and 2 in the two cases and $C(t)$ denotes a cyclic group of order t (Serre 1970, Cours..., II.3.2). Therefore $L(\ell^r) \overset{\mathrm{df}}{=} \mathbb{Q}[\zeta]^\Delta$ is a cyclic cyclotomic extension of $\mathbb{Q}$ of degree ℓ^{r-2} or ℓ^{r-3}.

Next consider $\mathbb{Q}_p[\zeta]$. If $p = \ell$, then $\mathbb{Q}[\zeta]$ is totally ramified over p, and so $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] = [\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(\ell^r)$. If $p \neq \ell$, then $\mathbb{Q}[\zeta]$ is totally unramified over p, and $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p]$ is the smallest integer t such that $\ell^r | p^t - 1$. In either case, we see that $[\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] \to \infty$ as $r \to \infty$. Thus, for any p, $[L(\ell^r)^p : \mathbb{Q}_p]$ 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 $\ell_1, \dots, \ell_s$, $L = L(\ell_1^{r_1}) \cdots L(\ell_s^{r_s})$ will be cyclic, and clearly, by choosing $\ell_1^{r_1} \dots \ell_s^{r_s}$ 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 $\alpha \in \mathrm{Br}(L/K)$.*

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[2], 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 $\phi(a)|\mathbb{Q}[\zeta_{\ell^r}] = 1$ for all $\ell|m$. Thus, we may assume that $m = \ell^r$, $m \ne 2$.

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 $p \ne \ell$, 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

$$\phi_\ell(a) = [u^{-1}]$$

(see I.3.13)

[2]Because this is true locally.

It suffices to show that $\phi(a) = 1$ in the three cases: $a = -1$, $a = \ell$, $a =$ a prime $q \neq \ell$. We have:

$$\phi_p(-1) = \begin{cases} [-1] & \text{if} \quad p = \infty \\ [-1] & \text{if} \quad p = \ell \\ [1] & \text{if} \quad p \neq \ell, \infty. \end{cases}$$

$$\phi_p(\ell) = \begin{cases} [1] & \text{if} \quad p = \ell \\ [1] & \text{if} \quad p \neq \ell \end{cases}$$

$$\phi_p(q) = \begin{cases} [q] & \text{if} \quad p = q \\ [q^{-1}] & \text{if} \quad p = \ell \\ [1] & \text{if} \quad p \neq \ell, q. \end{cases}$$

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 (8.1a) holds for L/K, then it holds for any subextension.*
(b) *If (8.1a) holds for L/K, then it holds for $L \cdot K'/K'$ for any 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

$$\begin{array}{ccc} K_w'^\times & \xrightarrow{\phi_w} & \mathrm{Gal}(L'^w/K'_w) \\ \downarrow \mathrm{Nm} & & \downarrow \text{inclusion} \\ K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L^v/K_v). \end{array}$$

On combining them, we get a commutative diagram:

$$\begin{array}{ccc} \mathbb{I}'_K & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \downarrow \mathrm{Nm} & & \downarrow \text{inclusion} \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Because the norm map on idèles carries $K^\times$ into $\mathbb{Q}^\times$, we see that this lemma follows from the previous one. □

From the example and the lemma, we find that (8.1a) holds for all cyclotomic extensions[3] 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).*

[3]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:

$$\begin{array}{ccccc} K^\times & \longrightarrow & I_K & \xrightarrow{\phi_{L/K}} & G \\ \downarrow{\scriptstyle \cup\delta\chi} & & \downarrow{\scriptstyle \cup\delta\chi} & & \downarrow{\scriptstyle \chi} \\ H^2(G, L^\times) & \longrightarrow & H^2(G, I_L) & \longrightarrow & Q/Z. \end{array}$$

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.4.1). 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 (a) implies (b). □

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 $\beta \in \mathrm{Br}(K)$. We are given that, if $\beta \in \mathrm{Br}(L/K)$ for some cyclic cyclotomic extension L/K, then $\sum \mathrm{inv}_v(\beta) = 0$, where β_v is the image of β in $\mathrm{Br}(K_v)$, but Proposition 7.2 says that *every* β in $\mathrm{Br}(K)$ lies in $\mathrm{Br}(L/K)$ for some cyclic cyclotomic extension L/K. □

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 $U = \mathrm{Nm}\,\mathbf{C}_L$. According to the Reciprocity Law, the Artin map defines an isomorphism

$$\phi : \mathbf{C}_K/U \to \mathrm{Gal}(L/K).$$

If M is the fixed field of $\phi(V)$, then ϕ defines an isomorphism

$$\mathbf{C}_K/V \to \mathrm{Gal}(M/K),$$

but, according to the Reciprocity Law, the kernel of $\phi : \mathbf{C}_K \to \mathrm{Gal}(M/K)$ is $\mathrm{Nm}_{M/K}\,\mathbf{C}_M$. □

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. Let $L = K[a^{1/n}]$—because $\zeta_n \in K$, this is an abelian extension of K. For any 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

$$K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_K) \supset K^\times \cdot \mathbb{I}_S = \mathbb{I}_K.$$

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 p^{th} root of 1 (p prime). Then every open subgroup V of $\mathbf{C}_K$ such that $\mathbf{C}_K/V$ 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, $\mathrm{Nm}(L_w^\times) \supset K_v^{\times p}$.

For any prime $v \in S$, 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 (Math 676, 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 $K^\times\cdot E=K^\times\cdot\operatorname{Nm}\mathbb{I}_L$.

Now let V be an open subgroup of $\mathbf{C}_K$ such that $\mathbf{C}_K/V$ 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 p202 of Tate's article in Cassels and Fröhlich, 1967.

LEMMA 9.4. *Let U be an open subgroup of finite index in $\mathbf{C}_K$. If there exists a finite extension K'/K such that $\operatorname{Nm}_{K'/K}^{-1}(U)$ is a norm group, then so also is U.*

PROOF. Write U' for $\operatorname{Nm}_{K'/K}^{-1}(U)$, and let L be the abelian extension of K' with $\operatorname{Nm}\mathbf{C}_L=U'$. If M is the maximum abelian subextension of L/K, then we have

$$\operatorname{Nm}_{M/K}\mathbf{C}_M=\operatorname{Nm}_{L/K}\mathbf{C}_L=\operatorname{Nm}_{K'/K}U'\subset U$$

and we can apply Lemma 9.1. □

THEOREM 9.5. *Every subgroup U of finite index in $\mathbf{C}_K$ 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 $(\mathbf{C}_K:U)$. After (9.4) we may assume that K contains a p^{th} root of 1. Choose a subgroup U_1 of $\mathbf{C}_K$ containing U and of index p in $\mathbf{C}_K$. After (9.3), there exists an abelian extension K' of K such that $\operatorname{Nm}_{K'/K}\mathbb{I}_{K'}=U_1$; moreover K' is cyclic of degree p over K. Put $U'=\operatorname{Nm}_{K'/K}^{-1}U$. The map

$$\operatorname{Nm}_{K'/K}:\mathbf{C}_{K'}\to\mathbf{C}_K/U$$

has image U_1/U and kernel U'. Hence

$$(\mathbf{C}_{K'} : U') = (\mathbf{C}_K : U)/p$$

and so, by induction, U' is a norm group. Now we can apply (9.4) to deduce that U is a norm group. □

10. Appendix: Kummer theory

Throughout this subsection, K is a field containing a primitive n^{th} root of 1, ζ. In particular, K either has characteristic 0 or characteristic p not dividing n. Write μ_n for the group of n^{th} roots of 1 in K. Then μ_n is a cyclic subgroup of $K^\times$ of order n with generator ζ.

Consider a field $L = K[\alpha]$ generated by an element α whose n^{th} power is in K. Then α is a root of $X^n - a$, and the remaining roots are the elements $\zeta^i\alpha$, $1 \le i \le n-1$. Since these are all in L, L is a Galois extension of K, with Galois group G say. For any $\sigma \in G$, $\sigma\alpha$ is also a root of $X^n - a$, and so $\sigma\alpha = \zeta^i\alpha$ for some i. Hence $\sigma\alpha/\alpha \in \mu_n$. The map

$$\sigma \mapsto \sigma\alpha/\alpha : G \to \mu_n$$

doesn't change when α is replaced by a conjugate, and it follows that the map is a homomorphism: $\frac{\sigma\tau\alpha}{\alpha} = \frac{\sigma(\tau\alpha)}{\tau\alpha}\frac{\tau\alpha}{\alpha}$. Because α generates L/K, the map is injective. If it is not surjective, then G maps into a subgroup μ_d of μ_n, some $d|n$, $d < n$. In this case, $(\sigma\alpha/\alpha)^d = 1$, i.e., $\sigma\alpha^d = \alpha^d$, for all $\sigma \in G$, and so $\alpha^d \in K$. Thus the map is surjective if n is the smallest positive integer such that $\alpha^n \in K$. We have proved the first part of the following statement.

PROPOSITION 10.1. *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. It remains to prove the second statement. Let σ generate G and let ζ generate μ_n. It suffices to find an element $\alpha \in L^\times$ such that $\sigma\alpha = \zeta^{-1}\alpha$, for then $\alpha^n \in K$, and α^n is the smallest power of α that lies in K. According to the Normal Basis Theorem (II.1.24), there exists an element $\gamma \in L$ such that $\{\gamma, \sigma\gamma, \dots, \sigma^{n-1}\gamma\}$ is a basis for L/K as a K-vector space. Form the sum

$$\alpha = \sum \zeta^i\sigma^i\gamma.$$

Then $\alpha \neq 0$ because the $\sigma^i\gamma$ are linearly independent and the $\zeta^i \in K$, and $\sigma\alpha = \zeta^{-1}\alpha$. □

PROPOSITION 10.2. *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. Only the "only if" part requires proof. We are given that $K[\alpha] = K[\beta]$ with $\alpha^n = a$ and $\beta^n = b$. Let σ be the generator of the Galois group with $\sigma\alpha = \zeta\alpha$, and let $\sigma\beta = \zeta^i\beta$, $(i, n) = 1$. We can write

$$\beta = \sum_{j=0}^{n-1} c_j\alpha^j, \quad c_j \in K,$$

and then

$$\sigma\beta = \sum_{j=0}^{n-1} c_j \zeta^j \alpha^j.$$

On comparing this with $\sigma\beta = \zeta^i\beta$, we find that $\zeta^i c_j = \zeta^j c_j$ for all j. Hence $c_j = 0$ for $j \neq i$, and therefore $\beta = c_i\alpha^i$. □

The last two results give us a complete classification of the cyclic extensions of K of degree n (recall that we are assuming K contains a primitive n^{th} root of 1). It is not difficult to extend this to a classification of all abelian extensions of exponent n. (We say that a group G has *exponent* n if $\sigma^n = 1$ for all $\sigma \in G$. A finite abelian group of exponent n is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^r$ for some r.)

Let L/K be a finite Galois extension with Galois group G. From the exact sequence

$$1 \to \mu_n \to L^\times \xrightarrow{x\mapsto x^n} L^{\times n} \to 1$$

we obtain a cohomology sequence

$$1 \to \mu_n \to K^\times \xrightarrow{x\mapsto x^n} K^\times \cap L^{\times n} \to H^1(G, \mu_n) \to 1.$$

The 1 at the right is because of Hilbert's Theorem 90. Thus we obtain an isomorphism

$$K^\times \cap L^{\times n}/K^{\times n} \to \operatorname{Hom}(G, \mu_n).$$

This map can be described as follows: let a be an element of $K^\times$ that becomes an n^{th} power in L, say $a = \alpha^n$; then a maps to the homomorphism $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$. If G is abelian of exponent n, then

$$\#\operatorname{Hom}(G, \mu_n) = (G : 1).$$

THEOREM 10.3. *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 n^{th} root of each element of B. If $L \leftrightarrow B$, then $[L : K] = (B : K^{\times n})$.

PROOF. For any finite Galois extension L of K, define $B(L) = K^\times \cap L^{\times n}$. Then $L \supset K[B(L)^{\frac{1}{n}}]$, and for any group B containing $K^{\times n}$ as a subgroup of finite index, $B(K[B^{\frac{1}{n}}]) \supset B$. Therefore,

$$[L : K] \geq [K[B(L)^{\frac{1}{n}}] : K] = (B(K[B(L)^{\frac{1}{n}}]) : K^{\times n}) \geq (B(L) : K^{\times n}).$$

If L/K is abelian of exponent n, then $[L : K] = (B(L) : K^{\times n})$, and so equalities hold throughout: $L = K[B(L)^{\frac{1}{n}}]$.

Next consider a group B containing $K^{\times n}$ as a subgroup of finite index, and let $L = K[B^{\frac{1}{n}}]$. Then L is a composite of the extensions $K[a^{\frac{1}{n}}]$ for a running through a set of generators for $B/K^{\times n}$, and so it is a finite abelian extension of exponent n. Therefore

$$a \mapsto (\sigma \mapsto \frac{\sigma a^{\frac{1}{n}}}{a}) : B(L)/K^{\times n} \to \operatorname{Hom}(G, \mu_n), \quad G = \operatorname{Gal}(L/K),$$

is an isomorphism. This map sends $B/K^{\times n}$ isomorphically onto the subgroup $\mathrm{Hom}(G/H, \mu_n)$ of $\mathrm{Hom}(G, \mu_n)$ where H consists of the $\sigma \in G$ such that $\sigma a^{\frac{1}{n}}/a = 1$ for all $a \in B$. But such a σ fixes all $a^{\frac{1}{n}}$ for $a \in B$, and therefore is the identity automorphism on $L = K[B^{\frac{1}{n}}]$. This shows that $B(L) = B$, and hence $L \mapsto B(L)$ and $B \mapsto K[B^{\frac{1}{n}}]$ are inverse bijections. □

EXAMPLE 10.4. (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 excursion into algebra, we return to some number theory.

PROPOSITION 10.5. *Let K be a number field (containing a primitive n^{th} root of 1, as always in this subsection), and let $L = K[a_1^{\frac{1}{n}}, \cdots, a_n^{\frac{1}{n}}]$. 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 10.1) we can assume to have degree n. Let $\alpha = a^{\frac{1}{n}}$ and $f = X^n - a$. Then

$$\mathrm{disc}\, f = \pm \mathrm{Nm}_{L/K}\, f'(\alpha) = \pm \mathrm{Nm}_{L/K}\, n\alpha^{n-1} = \pm n^n a^{n-1}.$$

Thus if $\mathfrak{p}_v$ does not divide na, it does not divide $\mathrm{disc}\, f$, and, *a fortiori,* it does not divide $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$. (See Math 676, 2.33, 2.22.) □

REMARK 10.6. 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 $X^p \equiv a \bmod p\pi\mathfrak{p}$ 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 $X^p \equiv a \bmod p\pi$ 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 L. Washington, Introduction to Cyclotomic Fields, Springer, 1982/1997, Exercise 9.3, and Cassels and Fröhlich 1967, Exercise 2.12, p353. In the case $K = \mathbb{Q}[\zeta]$, see also J. Cassels, Local Fields, Cambridge, 1986, pp 139–140, and A. Fröhlich and M. Taylor, Algebraic Number Theory, Cambridge, 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 all results proved in Serre, Cours..., 1970, Chapters I–IV, VI to arbitrary number fields.

1. The Local-Global Principle

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 three cases where class field theory allows us to prove that the principle holds.

nth Powers.

THEOREM 1.1. *Let K be a number field containing a primitive nth root of 1, and let S be a finite set of primes of K. An element a of $K^\times$ is an nth power in K if and only if it is an nth power in K_v for all primes v.*

PROOF. Only the sufficiency needs to be proved. Consider $L = K[a^{\frac{1}{n}}]$. This is an abelian extension of K, and a prime v splits in L if and only if a is an nth power in K_v. Therefore, every prime not in S splits in L, and Proposition VII.4.6 implies that $L = K$. □

REMARK 1.2. (a) If we use (VI.3.4) rather than (VII.4.6), we obtain the stronger result: under the hypothesis of the theorem, a is an nth power in K if it an nth power in K_v for all v in a set of density $> 1/2$.

(b) In 1933, Grünwald proved Theorem 1.1 without the assumption that K contain a primitive nth root of 1 (Grünwald's theorem). In 1942, Whaples gave another proof of Grünwald's theorem. Then in 1948, Wang gave a counterexample to Grünwald's theorem (see the exercise below), and later gave a proof of a corrected theorem (Grünwald-Wang theorem). The correct theorem states:

> Let K be a number field, and let n be a positive integer. Let $a \in K^\times$, and suppose that $a \in K_v^{\times n}$ for all but finitely many primes v. Then at least one of the following is true:
> (a) $a \in K^{\times n}$;
> (b) $n = 2^t n'$ for some odd n', $\mathrm{Gal}(K[\zeta_{2^t}]/K)$ is not cyclic, and $a^2 \in K^{\times n}$.

See Cassels, Local Fields, 1968, Exercise on p248, and Artin and Tate 1951/52, p96.

EXAMPLE 1.3. 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 at all odd p, and deduce that, for p odd, $\mathbb{Q}_p$ contains at least one of $1 + i$, $\sqrt{2}$, or $\sqrt{-2}$.)

Norms.

THEOREM 1.4. *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, $H^1(G, \mathbf{C}_L) = 0$. Because of the periodicity of the cohomology of cyclic groups, this implies that $H_T^{-1}(G, \mathbf{C}_L) = 0$. Therefore, from the cohomology sequence of

$$1 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$$

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

$$K^\times / \operatorname{Nm}(L^\times) \to \oplus_v K_v^\times / \operatorname{Nm}(L^{v\times}).$$

□

REMARK 1.5. The proof fails for noncyclic extension, and, in fact, the statement is not true for noncyclic extensions. For example, 2 is a local norm from $\mathbb{Q}[\sqrt{13}, \sqrt{17}]$ at all primes but is not a global norm.

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) $B(v, w) \stackrel{\text{df}}{=} Q(v + w) - Q(v) - Q(w)$ is a bilinear form on V.

The quadratic form Q is said to be *nondegenerate* if its associated bilinear form B is nondegenerate. 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 1.6. *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

$$q(X_1, \dots, X_n) = a_1X_1^2 + \cdots + a_nX_n^2,$$

and keep in mind that an invertible change of variables will change none of our statements.

LEMMA 1.7. *A nondegenerate quadratic form $q(X_1, \dots, X_n)$ represents a if and only if $r \stackrel{\text{df}}{=} q - aY^2$ represents 0.*

PROOF. If $q(x_1, \dots, x_n) = a$, the $r(x_1, \dots, x_n, 1) = 0$. 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 1.8. *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.

COROLLARY 1.9. *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 1.10. *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 1.7, $X^2 - aY^2$ represents 0 if and only if X^2 represents a.

(c) According to 1.7, $X^2 - aY^2 - bZ^2$ 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,

$$q(x, y, z, t) = 0 \iff c = \frac{\text{Nm}_{k[\sqrt{b}]/k}(x + \sqrt{b}y)}{\text{Nm}_{k[\sqrt{a}]/k}(z + \sqrt{a}t)}.$$

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 1.11. *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, (∗) $\implies$ (∗∗). 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.1.22), 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 (a) of the Theorem. 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 (1.8a) 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 (1.10) and Theorem 1.4. □

Proof of (b) of the Theorem 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 (1.10) and Theorem 1.1.

When $n = 3, 4$ the statement follows in a similar fashion from (1.10c,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 (Math 676, 7.23) 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 1.4b 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, 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

$$c \stackrel{\text{df}}{=} ax_1^2 + bx_2^2$$

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 1.12. *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 $a = b \times (\text{square})$ (see VII.10.1). 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.5.1). For

$$\alpha = x + yi + zj + tk$$

we define

$$\bar{\alpha} = x - yi - zj - tk$$

so that

$$\mathrm{Nm}(\alpha) \stackrel{\mathrm{df}}{=} \alpha\bar{\alpha} = x^2 - by^2 - cz^2 + bct^2.$$

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 any $\alpha \in H(b,c)$,

$$P_\alpha(X) \stackrel{\mathrm{df}}{=} (X-\alpha)(X-\bar{\alpha}) = X^2 - (\alpha+\bar{\alpha})X + \mathrm{Nm}(\alpha) \in K[X].$$

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 1.13. *Every nondegenerate quadratic form q in ≥ 5 variables over a finite extension of $\mathbb{Q}_p$ represents* 0.

PROOF. We can write $q = r(X_1, \dots, X_4) - aX_5^2 + q'(X_6, \dots)$, where r is a nondegenerate quadratic form in 4 variables and $a \neq 0$. Then r represents a and so q represents 0. □

COROLLARY 1.14. *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 (1.13) with (1.8). □

REMARK 1.15. The proof of Proposition 1.12 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.

2. 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

$$H^2(L/K) = H^2(\mathrm{Gal}(L/K), \mathbf{C}_L).$$

Because $H^1(G, L^\times) = 0$ (see II.1.21) and $H^1(G, \mathbf{C}_L) = 0$ (see VII.5.1), for any 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:

$$\begin{array}{ccccccc} & & & & & \nearrow & H^2(L/K) \\ 0 & \to & \mathrm{Br}(L/K) & \to & \oplus \mathrm{Br}(L^v/K_v) & & \\ & & & & & \searrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

The top row is part of the cohomology sequence of

$$0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0.$$

The zero at left comes from the fact that $H^1(G, \mathbf{C}_L) = 0$. The top row is exact, but the map $\oplus_v \mathrm{Br}(L^v/K_v) \to H^2(L/K)$ will not in general be surjective—we denote its image by $H^2(L/K)'$.

Recall (III.1.1), 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

$$\Sigma : \oplus \mathrm{Br}(L^v/K_v) \to \mathbb{Q}/\mathbb{Z}, \quad (\beta_v) \mapsto \sum \mathrm{inv}_v(\beta_v).$$

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 2.5 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 $(H^2(L/K)' : 1) \leq (H^2(L/K) : 1) \leq n$.)
(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 2.1. *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 $n_0 \stackrel{\mathrm{df}}{=} \mathrm{lcm}(n_v)$. According to , 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.5.5d) (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

$$0 \to \mathrm{Br}(\Omega_n/K) \to \oplus\, \mathrm{Br}(\Omega_n^v/K_v) \xrightarrow{\Sigma} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact. On passing to the direct limit (actually, directed union) over all n, we obtain an exact sequence

$$0 \to \mathrm{Br}(\Omega/K) \to \oplus_v \mathrm{Br}(\Omega^v/K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

THEOREM 2.2. *For any number field K, the sequence*

$$0 \to \mathrm{Br}(K) \to \oplus_v \mathrm{Br}(K_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0$$

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 2.3. *For any finite extension L/K, the sequence*

$$0 \to \mathrm{Br}(L/K) \to \oplus_v \mathrm{Br}(L^v/K_v) \xrightarrow{\Sigma} \frac{1}{n_0}\mathbb{Z}/\mathbb{Z} \to 0, \quad n_0 = \mathrm{lcm}(n_v),$$

is exact.

PROOF. Apply the snake lemma to the diagram obtained by mapping the fundamental exact sequence for K to that for L. □

EXAMPLE 2.4. (a) For a finite cyclic extension of number fields L/K, the fundamental exact sequence becomes identified with

$$0 \to K^\times/\operatorname{Nm}(L^\times) \to \oplus K_v^\times/\operatorname{Nm}(L^{v\times}) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0, \quad n = [L:K].$$

(b) Let D be a division algebra over a number field K, and let $i_v = \operatorname{inv}_v(D \otimes_K K_v)$. 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 $\sum i_v \equiv 0 \mod v$. 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 $\operatorname{Br}(K)$ 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 2.5. 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 $\operatorname{Gal}(L/\mathbb{Q})$, 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

$$\operatorname{inv}_K : H^2(\Omega/K) \to \mathbb{Q}/\mathbb{Z}$$

uniquely characterized by having the property that the composite

$$\oplus_v \operatorname{Br}(K_v) \to H^2(\Omega/K) \xrightarrow{\operatorname{inv}_K} \mathbb{Q}/\mathbb{Z}$$

is $(\beta_v) \mapsto \sum \operatorname{inv}_v(\beta_v)$.

LEMMA 2.6. *For any finite extension L/K of number fields and $\gamma \in H^2(\Omega/K)$, $\operatorname{inv}_L(\gamma) = n \operatorname{inv}_K(\gamma)$, $n = [L:K]$.*

PROOF. Use that the sum of the local degrees is the global degree. □

Therefore, for any L/K finite and Galois, we obtain an isomorphism

$$\operatorname{inv}_{L/K} : H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

On passing to the direct limit over all $L \subset K^{\mathrm{al}}$, we obtain an isomorphism

$$\operatorname{inv}_K : H^2(K^{\mathrm{al}}/K) \to \mathbb{Q}/\mathbb{Z}.$$

THEOREM 2.7. *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 $\operatorname{inv}_{L/K}(u_{L/K}) = \frac{1}{n} \mod \mathbb{Z}$. □

The generator $u_{L/K}$ of $H^2(L/K)$ is called the *fundamental class.* One shows as in the local case (see III.1.2) that for any tower $E \supset L \supset K$ of finite Galois extensions,

$$\begin{aligned} \mathrm{Res}(u_{E/K}) &= u_{E/L} \\ \mathrm{Inf}(u_{L/K}) &= [E:L]u_{E/K}. \end{aligned}$$

Therefore, one may apply Tate's theorem (II.2.18) to obtain an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathbf{C}_K/\,\mathrm{Nm}(\mathbf{C}_L).$$

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 2.8. *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*

$$\mathrm{Nm}_{E/K}\,\mathbf{C}_E = \mathrm{Nm}_{M/K}\,\mathbf{C}_M.$$

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

$$\begin{array}{ccc} H_T^{-2}(H,\mathbb{Z}) & \xrightarrow{\approx} & H_T^0(H,\mathbf{C}_L) \\ \big\downarrow{\scriptstyle \mathrm{Cor}} & & \big\downarrow{\scriptstyle \mathrm{Cor}} \\ H_T^{-2}(G,\mathbb{Z}) & \xrightarrow{\approx} & H_T^0(G,\mathbf{C}_L) \end{array}$$

in which the horizontal arrows are cup-product with the fundamental classes. This can be identified with the commutative diagram:

$$\begin{array}{ccc} H^{\mathrm{ab}} & \xrightarrow{\approx} & \mathbf{C}_E/\,\mathrm{Nm}_{L/E}\,\mathbf{C}_L \\ \big\downarrow & & \big\downarrow{\scriptstyle \mathrm{Nm}_{E/K}} \\ G^{\mathrm{ab}} & \xrightarrow{\approx} & \mathbf{C}_K/\,\mathrm{Nm}_{L/K}\,\mathbf{C}_L \end{array}$$

Hence the cokernel of $H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ is isomorphic to $\mathbf{C}_K/\,\mathrm{Nm}_{E/K}(\mathbf{C}_E)$. But the cokernel is equal to $\mathrm{Gal}(M/K)$, which is isomorphic to $\mathbf{C}_K/\,\mathrm{Nm}_{M/K}(\mathbf{C}_M)$. Since $\mathrm{Nm}(\mathbf{C}_M) \supset \mathrm{Nm}(\mathbf{C}_E)$, the two groups must be equal. □

3. Higher Reciprocity Laws

For an odd prime p and integer a not divisible by p, one defines (*Legendre symbol, quadratic residue symbol)*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

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 any finite set $a, b, \dots$ of elements of K, we define $S(a, b, \dots)$ to be the set of prime ideals of K such that $\mathrm{ord}_\mathfrak{p}(n) \neq 0$, or $\mathrm{ord}_\mathfrak{p}(a) \neq 0$, or $\mathrm{ord}_\mathfrak{p}(b) \neq 0$,... . 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 $q = \mathbb{N}\mathfrak{p} \stackrel{\mathrm{df}}{=} (\mathcal{O}_K : \mathfrak{p})$. Then $\mathbb{F}_q^\times$ is cyclic of order $q-1$, and so $n | q-1$ and $u^{\frac{q-1}{n}} \in \mu_n \subset \mathbb{F}_q^\times$.

For $a \in K^\times$ and $\mathfrak{p} \in S(a)$, define $\left(\frac{a}{\mathfrak{p}}\right)$ to be the unique nth root of 1 such that

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{\mathbb{N}\mathfrak{p}-1}{n}} \mod \mathfrak{p}.$$

3.1. *For any $a, b \in K^\times$ and $\mathfrak{p} \in S(a, b)$,*

$$\left(\frac{ab}{\mathfrak{p}}\right) = \left(\frac{a}{\mathfrak{p}}\right)\left(\frac{b}{\mathfrak{p}}\right).$$

This is obvious from the definition.

3.2. *For $a \in K^\times$ and $\mathfrak{p} \in S(a)$, 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

$$1 \to \mathbb{F}_q^{\times n} \to \mathbb{F}_q^\times \xrightarrow{x \mapsto x^{q-1/n}} \mu_n \to 1, \qquad q = \mathbb{N}\mathfrak{p}.$$

If $X^n - a$ has a solution modulo $\mathfrak{p}$, then Hensel's lemma (Math 676, 7.24) 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).

3.3. *For any $a \in K^\times$ 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

$$\zeta(\mathfrak{p}) \cdot a^{\frac{1}{n}} \equiv x^{\frac{\mathbb{N}\mathfrak{p}}{n}} \mod \mathfrak{p},$$

from which it follows that $\zeta(\mathfrak{p}) = \left(\frac{a}{\mathfrak{p}}\right)$.

3.4. *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 any 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 $\mathfrak{b}$.

3.5. *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.10.5, $S(a)$ 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 $C_{\mathfrak{m}}$.

The Hilbert symbol. Let K_v be a local field containing a primitive nth root of 1. The *Hilbert symbol* is a pairing

$$a, b \mapsto (a,b)_v : K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$$

where μ_n is the group of nth roots of 1 in K_v. Probably the most natural way of defining this 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 3.6. 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.5.1; Proposition 1.10d; Proposition 1.10c. The last condition shows that our definition of the Hilbert symbol agrees with that, for example, in Serre, Cours..., 1970, III.

3.7. *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 $A(a,b;\zeta)^{\mathrm{opp}} \to A(a,b;\zeta^{-1})$.

3.8. *Let $a, b \in K^\times$. For any $v \in S(a)$, $(a,b)_v = \left(\frac{a}{\mathfrak{p}_v}\right)^{ord_v(b)}$.*

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 $\mathrm{inv}_v([D]) = \mathrm{ord}_v(\alpha)$.

We apply this with $L = K_v[i] = K_v[a^{\frac{1}{n}}]$. Note that, because $v \in S(a)$, 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 $\mathrm{ord}_v(\beta) = -\frac{r}{n}\mathrm{ord}_v(b)$. Hence

$$(a,b)_v \overset{\mathrm{df}}{=} \zeta^{-n\,\mathrm{inv}_v(A(a,b;\zeta))} = \zeta^{r\cdot\mathrm{ord}_v(b)} = \left(\frac{a}{\mathfrak{p}_v}\right)^{\mathrm{ord}_v(b)}.$$

Remark 3.9. In fact,

$$(a,b)_v = \frac{\phi_v(b)(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}$$

for all a, b, v. See III.4.3.

3.10. *For $a, b \in K^\times$,*

$$\prod_v (a,b)_v = 1.$$

In the course of proving the Reciprocity Law, we showed that, for any $\beta \in \mathrm{Br}(K)$, $\sum \mathrm{inv}_v(\beta) = 0$. In particular, $\sum \mathrm{inv}_v(A(a,b;\zeta)) = 0$, and this implies the formula.

For $a, b \in K^\times$, define

$$\left(\frac{a}{b}\right) = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{\mathrm{ord}_v(b)} = \left(\frac{a}{(b)^{S(a)}}\right)$$

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 3.11 (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

$$\left(\frac{c}{b}\right) = \prod_{v\in S}(c,b)_v.$$

PROOF. Let $S'(a) = S(a) \setminus S$ and $S'(b) = S(b) \setminus S$. Our assumption is that $S'(a)$ and $S'(b)$ are disjoint. Then

$$\left(\frac{a}{b}\right) = \prod_{v\in S'(b)}\left(\frac{a}{\mathfrak{p}_v}\right)^{\mathrm{ord}_v(b)} = \prod_{v\in S'(b)}(a,b)_v$$

and

$$\left(\frac{b}{a}\right) = \prod_{v\in S'(a)}\left(\frac{b}{\mathfrak{p}_v}\right)^{\mathrm{ord}_v(a)} = \prod_{v\in S'(a)}(b,a)_v.$$

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 3.8 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, Cours..., 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.10.6a). 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 3.12. *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, p354.

EXAMPLE 3.13. (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.

EXERCISE 3.14. 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 $x^2 + 27y^2$, $x, y \in \mathbb{Z}$.

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 (Math 676, 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 $\left(\frac{\alpha}{\beta}\right) = 1$ for all $\beta \in \mathbb{Z}[\zeta]$ relatively prime to α.

THEOREM 3.15. *Let x, y, z be relative prime positive integers such that $p \nmid xyz$ and $x^p + y^p = z^p$. For any 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

$$\mathrm{Tr}\,\frac{\alpha-1}{\pi} = \mathrm{Tr} - \frac{y\pi}{x+y} = -\frac{y}{x+y}(p-1),$$

which is not divisible by p. Therefore $\frac{q^{p-1}-1}{p}$ is divisible by p. □

COROLLARY 3.16 (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 $2^{p-1} \equiv 1 \mod p^2$.*

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: $3^{p-1} \not\equiv 1 \mod p^2$.

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 $p < 3 \times 10^9$.

Notes: Theorem 3.15 was proved by Furtwängler (see Hasse 1970, II, 22); see also Koch 1992, II.6.3, and Herbrand 1936, p47. 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.

4. 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, 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 any 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 4.1. *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 e, 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 any $y \in V$ 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 4.2. *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

$$q(X_1, \dots, X_n) = \sum a_{ij} X_i X_j, \qquad a_{ij} = B(e_i, e_j).$$

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 4.2 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 4.1 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, $q = a_1 X_1^2 + \cdots + a_r X_r^2$, 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 4.3 (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 1.8, 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 (4.2) 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 4.4. Let (V, Q) be a quadratic space over a field k, and let O be its group of isometries. Theorem 4.3 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 -1s 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 4.5. *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 4.6. Serre, Cours..., 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 4.7. *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

$$q \sim a_1X_1^2 + \cdots + a_iX_i^2 + a_{i+1}X_{i+1}^2 + \cdots \sim a'_1X_1^2 + \cdots + a'_iX_i^2 + a'_{i+1}X_{i+1}^2 + \cdots$$

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

$$(a_i, d_{i-1})(a_{i+1}, d_i) = (a_i, d_{i-1})(a_{i+1}, d_{i-1})(a_{i+1}, a_i) = (a_ia_{i+1}, d_{i-1})(a_i, a_{i+1})$$

and a_ia_{i+1} differs from $a'_ia'_{i+1}$ by a square, and so it remains to show that $(a_i, a_{i+1}) = (a'_i, a'_{i+1})$. According to Proposition 4.2, $a_iX_i^2 + a_{i+1}X_{i+1}^2 \sim a'_iX_i^2 + a'_{i+1}X_{i+1}^2$, 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 4.8. *Let B and B' be orthogonal bases for a nondegenerate quadratic space (V, Q). Then there exists a chain of orthogonal bases $B_1, B_2, \ldots, B_m$ 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. O'Meara, Introduction to Quadratic Forms, Springer, 1963, Lemma 58.1. □

PROPOSITION 4.9. *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 $q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$. Then q represents a if and only if there exists an $e \in K^\times$ for which the equations

$$a_1X_1^2 + a_2X_2^2 = e = a_3X_3^2 - aX_4^2$$

have solutions. According to (b), this will be so if and only if

$$(e, -a_1a_2) = (a_1, a_2), \quad (e, a_3a) = (a_3, -a). \qquad (*)$$

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 $f(x) = \varepsilon_1$, $f(x) = \varepsilon_2$ 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 $(\cdot, -a_1a_2), (\cdot, a_3a) : K^\times/K^{\times 2} \to \{\pm 1\}$, we find that there will exist an e satisfying $(*)$ unless $-a_1a_2 = a_3a$ (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 1.13). □

THEOREM 4.10. *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 4.7 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 4.9, 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 4.11. *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

$$d = -1 \implies S(q) = (-1, a)(-1, b) = (-1, d) = (-1, -1).$$

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 $q \stackrel{\text{df}}{=} aX^2 + adY^2$ 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 4.12. *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 4.11 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, $0 \le t_v \le n$, $d_v = (-1)^{t_v}$ (modulo squares), and $s_v = (-1)^{t_v(t_v+1)/2}$.

PROOF. 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 4.13. *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,

$$G \cong \mathbf{C}_K/2\mathbf{C}_K \cong \mathbb{I}/K^\times \cdot \mathbb{I}^2.$$

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

$$S_v(q) \stackrel{\text{df}}{=} (a, a)_v(ad_0, d_0)_v = S(q(v))$$

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 $i_v(a)d_v = -1 \implies (a, d_v)_v \cdot s_v = 1$. Let $T = \{v \mid s_v \neq 1\}$—by hypothesis, it is a finite set. By the weak approximation theorem, 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 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 4.14 (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, Cours..., 1970, Chap. IV. □

5. Density Theorems

Throughout this section, K is a number field.

THEOREM 5.1. *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 5.2. *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 5.1 with Theorem VI.4.8. □

COROLLARY 5.3. *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 5.4 (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*

$$x \in C, \quad \tau \in G \implies \tau x \tau^{-1} \in C.$$

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 notations

$$\mathfrak{P}|\mathfrak{q}|\mathfrak{p}$$

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 (5.3 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

$$\mathfrak{P} \mapsto \mathfrak{q} =_{df} \mathfrak{P} \cap \mathcal{O}_M \colon T_{L,\sigma} \to T_{M,\sigma}.$$

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 $<\sigma>$, which has order f, and $C_G(\sigma)$ has order $\frac{d}{c}$ because there is a bijection

$$\tau \mapsto \tau\sigma\tau^{-1} \colon G/C_G(\sigma) \to C.$$

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 5.5. 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

$$\pi_C(x) = \#\{\mathfrak{p} | (\mathfrak{p}, L/K) = C, \quad \mathbb{N}\mathfrak{p} \leq x\}.$$

Then

$$\pi_C(x) = \frac{c}{d}\frac{x}{\log x} + \text{specific error term.}$$

6. Function Fields

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 1951/52) or (better) one can base the proofs on Tsen's theorem (see J. Milne, Arithmetic Duality Theorems, Academic Press, 1986, Appendix to Chapter I).

7. 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., J. Milne, ibid., Chapter I).

8. 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 W. Narkiewicz, Elementary and Analytic Theory of Numbers, PWN, 1974.

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[1]

$$\rho \approx \chi_1 \oplus \cdots \oplus \chi_m,$$

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 $\{(a_v) \mid a_v = 1 \text{ for } v \in S,\ a_v = \text{unit for all } v\}$

EXAMPLE 8.1. 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 $\psi(p) = \frac{\pi}{\sqrt{p}}\left(\frac{D}{\bar{\pi}}\right)$.

[1]By this we mean that, relative to suitable basis for V,

$$\rho(g) = \begin{pmatrix} \chi_1(g) & 0 & \cdots & 0 \\ 0 & \chi_2(g) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \chi_m(g) \end{pmatrix}, \quad g \in G.$$

For such a character, we define

$$L(s,\psi) = \prod_{v\notin S} \frac{1}{1-\psi(\pi_v)\mathbb{N}\mathfrak{p}_v^{-s}}$$

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).

Weil groups and Artin-Hecke L-series. For this topic, see J. Tate, Number theoretic background, pp 3–26, in: Automorphic Forms, Representations, and L-Functions, AMS, 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 J. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer, 1992, IV.2.

Gauss's theorem implies that the Weil conjecture 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, p213.

Index