Notes on class field theory

Notes on class field theory

Kiran S. Kedlaya
University of California San Diego

Preface

Last modified: May 12, 2024.

This text is a lightly edited version of the lecture notes of a course on class field theory (Math 254B) that I gave at UC Berkeley in the spring of 2002. To describe the scope of the course, I can do no better than to quote from the original syllabus:

> Class field theory, the study of abelian extensions of number fields, was a crowning achievement of number theory in the first half of the 20th century. It brings together, in a unified fashion, the quadratic and higher reciprocity laws of Gauss, Legendre et al, and vastly generalizes them. Some of its consequences (e.g., the Chebotaryov density theorem) apply even to nonabelian extensions.
>
> Our approach in this course will be to begin with the formulations of the statements of class field theory, omitting the proofs (except for the Kronecker-Weber theorem, which we prove first). We then proceed to study the cohomology of groups, an important technical tool both for class field theory and for many other applications in number theory. From there, we set up a local form of class field theory, then proceed to the main results.

The assumed background for the course was a one-semester graduate course in algebraic number theory, including the following topics: number fields and rings of integers; structure of the class and unit groups; splitting, ramification, and inertia of prime ideals under finite extensions; different and discriminant; basic properties of local fields. In fact, most of the students in Math 254B had attended such a course that I gave the previous semester (Math 254A) based on chapters I, II, and III of Neukirch's book [37]; for that reason, it was natural to use that book as a primary reference. However, no special features of that presentation are assumed, so just about any graduate-level text on algebraic number theory (e.g., Fröhlich-Taylor [11], Janusz [25], Jarvis [26], Lang [33]) should provide suitable background.

After the course ended, I kept the lecture notes posted on my web site in their originally written, totally uncorrected state. Despite their roughness, I heard back from many people over the years who had found them useful; in response to this, I decided to prepare a corrected version of the notes. This project gained some steam when I had the opportunity to teach another class[1] on class field theory in winter 2021. This occasioned some more significant revisions than I had previously dared, including a small degree of rearrangement of the material; however, I have tried to retain most of the original structure, on the grounds that the informality of the original notes contributed to their

[1] `kskedlaya.org/math204b-win21/`

readibility. In other words, this document is not intended as a standalone replacement for a good book on class field theory!

I maintain very few claims of originality concerning the presentation of the material. Besides [37], the main source of inspiration was Milne's lecture notes on class field theory [36] (and by extension the original development by Artin and Tate [1]). The basic approach may be summarized as follows: I follow Milne's treatment of local class field theory using group cohomology, then follow Neukirch to recast local class field theory in the style of Artin-Tate's class formations, then reuse the same framework to obtain global class field theory. Since the original draft of these notes was written, several treatments have appeared in a similar vein: [38], [17]. (See also [13] for a modern exposition of a more classical approach.)

My winter 2021 class, having taken place during the COVID-19 pandemic, was given online with recorded lectures. The recordings continue to be available from the course web site[2].Thanks to Zonglin Jiang, Justin Lacini, and Zongze Liu for their feedback on previous drafts, and to the participants in Math 204B (winter 2021) for "test-driving" the HTML version and generating much additional feedback. Thanks also to Rob Beezer and David Farmer for their assistance with the conversion from LaTeX to PreTeXt[3], which made it feasible to produce an HTML version[4] in sync with the PDF version[5].

[2] kskedlaya.org/math204b-win21/
[3] pretextbook.org/
[4] kskedlaya.org/cft
[5] kskedlaya.org/papers/cft-ptx.pdf

Contents

Chapter 1

Trailer: Abelian extensions of the rationals

Though class field theory has its origins in the law of quadratic reciprocity discovered by Gauss, its proper beginning is indicated by the Kronecker-Weber theorem, first stated by Kronecker in 1853 and proved by Weber in 1886. Although one could skip this theorem and deduce it as a consequence of more general results later on, I prefer to work through it explicitly. It will serve as a trailer for the rest of the course, giving us a preview of a number of key elements:

- reciprocity laws;
- passage between local and global fields, using Galois theory;
- group cohomology, and applications to classifying field extensions;
- computations in local fields.

1.1 The Kronecker-Weber theorem

Reference. Our approach follows [56], Chapter 14. A variety of other methods can be found in other texts.

Abelian extensions of $\mathbb{Q}$

Definition 1.1.1 An **abelian extension** of a field is a Galois extension with abelian Galois group. An example of an abelian extension of $\mathbb{Q}$ is the cyclotomic field $\mathbb{Q}(\zeta_n)$ (where n is a positive integer and ζ_n is a primitive n-th root of unity), whose Galois group is $(\mathbb{Z}/n\mathbb{Z})^*$, or any subfield thereof. Amazingly, Theorem 1.1.2 implies that there are no other examples! ◊

Theorem 1.1.2 Kronecker-Weber. *If $K/\mathbb{Q}$ is a finite abelian extension, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some positive integer n.*

Proof. See Lemma 1.1.10. ■

Example 1.1.3 A fundamental example of Theorem 1.1.2 is that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic field. This was known to Gauss via what we now call **Gauss sums**, and forms the basis of one of his proofs of quadratic reciprocity. It is this proof in particular that generalizes to

Artin reciprocity (Theorem 2.2.6). See also Exercise 2 and Exercise 3. □

Definition 1.1.4 The smallest n such that $K \subseteq \mathbb{Q}(\zeta_n)$ is called the **conductor** of $K/\mathbb{Q}$. It plays an important role in the splitting behavior of primes of $\mathbb{Q}$ in K, as we will see a bit later. ◊

We will prove Theorem 1.1.2 in the next few lectures. Our approach will be to deduce it from a local analogue (see Theorem 1.3.4).

Theorem 1.1.5 Local Kronecker-Weber. *If $K/\mathbb{Q}_p$ is a finite abelian extension, then $K \subseteq \mathbb{Q}_p(\zeta_n)$ for some n, where ζ_n is a primitive n-th root of unity.*

Proof. See Theorem 1.3.4. ■

Before proceeding, it is worth noting explicitly a nice property of abelian extensions that we will exploit below.

Remark 1.1.6 Let L/K be a Galois extension with Galois group G, let $\mathfrak{p}$ be a prime of K, let $\mathfrak{q}$ be a prime of L over $\mathfrak{p}$, and let $G_\mathfrak{q}$ and $I_\mathfrak{q}$ be the decomposition and inertia groups of $\mathfrak{q}$, respectively. Then any other prime $\mathfrak{q}'$ over $\mathfrak{p}$ can be written as $\mathfrak{q}^g$ for some $g \in G$, and the decomposition and inertia groups of $\mathfrak{q}'$ are the conjugates $g^{-1}G_\mathfrak{q}g$ and $g^{-1}I_\mathfrak{q}g$, respectively. (Note: my Galois actions will always be *right* actions, denoted by superscripts.)

If L/K is *abelian*, though, these conjugations have no effect. So it makes sense to talk about *the* decomposition and inertia groups of $\mathfrak{p}$ itself!

A reciprocity law

Assuming the Kronecker-Weber theorem, we can deduce strong results about the way primes of $\mathbb{Q}$ split in an abelian extension.

Definition 1.1.7 Suppose $K/\mathbb{Q}$ is abelian, with conductor m. Then we get a surjective homomorphism

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}).$$

On the other hand, suppose p is a prime not dividing m, so that $K/\mathbb{Q}$ is unramified above p. As noted above, there is a well-defined decomposition group $G_p \subseteq \mathrm{Gal}(K/\mathbb{Q})$. Since there is no ramification above p, the corresponding inertia group is trivial, so G_p is generated by a Frobenius element F_p, which modulo any prime above p, acts as $x \mapsto x^p$. We can formally extend the map $p \mapsto F_p$ to a homomorphism from S_m, the subgroup of $\mathbb{Q}$ generated by all primes not dividing m, to $\mathrm{Gal}(K/\mathbb{Q})$. This is called the **Artin map** of $K/\mathbb{Q}$.

The punchline is that the Artin map factors through the map $(\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(K/\mathbb{Q})$ we wrote down above! Namely, note that the image of r under the latter map takes ζ_m to ζ_m^r. For this image to be equal to F_p, we must have $\zeta_m^r \equiv \zeta_m^p \pmod{\mathfrak{p}}$ for some prime $\mathfrak{p}$ of K above p. But $\zeta_m^r(1 - \zeta_m^{r-p})$ is only divisible by primes above m (see Exercise 4) unless $r - p \equiv 0 \pmod{m}$. Thus F_p must be equal to the image of p under the map $(\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(K/\mathbb{Q})$. ◊

Remark 1.1.8 The **Artin reciprocity law** states that a similar phenomenon arises for any abelian extension of any number field; that is, the Frobenius elements corresponding to various primes are governed by the way the primes "reduce" modulo some other quantity. There are several complicating factors in the general case, though.

- Prime ideals in a general number field are not always principal, so we can't always take a generator and reduce it modulo something.

- There can be lots of units in a general number field, so even when a prime ideal is principal, it is unclear which generator to choose.
- It is not known in general how to explicitly construct generators for all of the abelian extensions of a general number field.

Thus our approach will have to be a bit more indirect. See Chapter 2 for the beginning of the story.

Reduction to the local case

Our reduction of Kronecker-Weber to local Kronecker-Weber relies on a key result typically seen in a first course on algebraic number theory.

Theorem 1.1.9 Minkowski. *There are no nontrivial extensions of $\mathbb{Q}$ which are unramified everywhere.*

Proof. See for instance [37] III.2. ■

Using Minkowski's theorem, let us deduce the Kronecker-Weber theorem from the local Kronecker-Weber theorem.

Lemma 1.1.10 *The local Kronecker-Weber theorem (Theorem 1.1.5) implies the Kronecker-Weber theorem (Theorem 1.1.2).*

Proof. For each prime p over which K ramifies, pick a prime $\mathfrak{p}$ of K over p; by local Kronecker-Weber (Theorem 1.1.5), $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{n_p})$ for some positive integer n_p. Let p^{e_p} be the largest power of p dividing n_p, and put $n = \prod_p p^{e_p}$. (This is a finite product since only finitely many primes ramify in K.)
Write $L = K(\zeta_n)$; we will prove that $K \subseteq \mathbb{Q}(\zeta_n)$ by proving that $L = \mathbb{Q}(\zeta_n)$. Form the completion $L_{\mathfrak{q}}$ for some prime $\mathfrak{q}$ over p; it is contained in $\mathbb{Q}_p(\zeta_{\mathrm{lcm}(n,n_p)})$. Let I_p be the inertia group of p in L; the fixed fixed U of I_p on $L_{\mathfrak{q}}$ is the maximal unramified subextension of $L_{\mathfrak{q}}$. Since $\mathbb{Q}_p(\zeta_e)$ is unramified over $\mathbb{Q}_p$ for any positive integer e coprime to p, we have $L_{\mathfrak{q}} = U(\zeta_{p^{e_p}})$ and so $I_p \cong \mathrm{Gal}(L_{\mathfrak{q}}/U) \subseteq (\mathbb{Z}/p^{e_p}\mathbb{Z})^*$. Let I be the group generated by all of the I_p; then

$$|I| \leq \prod |I_p| \leq \prod \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

On the other hand, the fixed field of I is an everywhere unramified extension of $\mathbb{Q}$, which can only be $\mathbb{Q}$ itself by Minkowski's theorem. That is, $I = \mathrm{Gal}(L/\mathbb{Q})$. But then

$$[L : \mathbb{Q}] = |I| \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}],$$

and $\mathbb{Q}(\zeta_n) \subseteq L$, so we must have $\mathbb{Q}(\zeta_n) = L$ and $K \subseteq \mathbb{Q}(\zeta_n)$, as desired. ■

Exercises

1. Prove that the ring of integers in $\mathbb{Q}(\zeta_n)$ equals $\mathbb{Z}[\zeta_n]$.

Hint. For n a power of a prime p, the minimal polynomial of ζ_n is the cyclotomic polynomial $\Phi_n(x) = x^{(p-1)n/p} + \cdots + x^{n/p} + 1$; use the polynomial $\Phi_n(x-1)$ to show that $1 - \zeta_n$ generates a prime ideal. For the general case, show that if K and L are linearly disjoint extensions of $\mathbb{Q}$ with coprime discriminants, then $\mathfrak{o}_{KL} = \mathfrak{o}_K \mathfrak{o}_L$.

2. For $m \in \mathbb{Z}$ not a perfect square, determine the conductor of $\mathbb{Q}(\sqrt{m})$.

Hint. First show that for p prime, $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ has conductor p.

3. Using the previous exercise, recover the law of quadratic reciprocity from the Artin reciprocity law.

4. Prove that if m, n are coprime integers in $\mathbb{Z}$, then $1-\zeta_m$ and n are coprime in $\mathbb{Z}[\zeta_m]$.

Hint. Look at the polynomial $(1-x)^m - 1$ modulo a prime divisor of n.

5. Prove that if m is not a prime power, then $1-\zeta_m$ is a unit in $\mathbb{Z}[\zeta_m]$.

6. Let p be an odd prime. Prove that $\mathbb{Z}[\zeta_p]^*$ is generated by ζ_p and $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*$.

Hint. By Dirichlet's units theorem, the index $[\mathbb{Z}[\zeta_p]^* : \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^*]$ is finite. For $\alpha \in \mathbb{Z}[\zeta_p]^*$, the ratio $\alpha/\overline{\alpha}$ is an algebraic integer having absolute value 1 under each complex embedding, and hence is a root of unity by Kronecker's theorem.

1.2 Kummer theory

Reference. [46] Chapter X; [37] section IV.3; or just about any advanced algebra text (e.g., [32]). The last lemma is from [56], Chapter 14.

Before attempting to classify all abelian extensions of $\mathbb{Q}_p$, we recall an older classification result. This result will continue to be useful as we proceed to class field theory in general, and the technique in its proof prefigures the role to be played by group cohomology down the line. So watch carefully!

Remark 1.2.1 A historical note (due to Franz Lemmermeyer): while the idea of studying field extensions generated by radicals was used extensively by Kummer in his work on Fermat's Last Theorem, the name **Kummer theory** for the body of results described here was first applied somewhat later by Hilbert in his *Zahlbericht* [21], a summary of algebraic number theory as of the end of the 19th century.

Theorem 90

We start with a fundamental result from field theory, which will crop up time and again in our work. To state it, let me introduce some terminology which marks the tip of the iceberg of group cohomology, which we will treat in a more comprehensive way Chapter 3.

Definition 1.2.2 If G is a group and M is an abelian group on which G acts (written multiplicatively), one defines the group $H^1(G, M)$ as the set of functions $f : G \to M$ such that $f(gh) = f(g)^h f(h)$, modulo the set of such functions of the form $f(g) = x(x^g)^{-1}$ for some $x \in M$. ◊

Lemma 1.2.3 "Theorem 90". *Let L/K be a finite Galois extension of fields with Galois group G. Then $H^1(G, L^*) = 0$.*

Proof. Let f be a function of the form described above. By the linear independence of automorphisms (see Exercise 1), there exists $x \in L$ such that $t = \sum_{g \in G} x^g f(g)$ is nonzero. But now

$$t^h = \sum_{g \in G} x^{gh} f(g)^h = \sum_{g \in G} x^{gh} f(gh) f(h)^{-1} = f(h)^{-1} t.$$

Thus f is zero in $H^1(G, L^*)$. ■

Remark 1.2.4 Lemma 1.2.3 derives its unusual name from the fact that in the special case where G is cyclic, this statement occurs as Theorem (Satz) 90 in [21]. The general case first appears in Emmy Noether's 1933 paper [40] on the principal ideal theorem (Theorem 2.3.1), where Noether attributes it to

Andreas Speiser.

Kummer extensions

Definition 1.2.5 Jargon watch. If G is a group, a **G-extension** of a field K is a Galois extension of K with Galois group G. ◊

Theorem 1.2.6 *If $\zeta_n \in K$, then every $\mathbb{Z}/n\mathbb{Z}$-extension of K is of the form $K(\alpha^{1/n})$ for some $\alpha \in K^*$ with the property that $\alpha^{1/d} \notin K$ for any proper divisor d of n, and vice versa.*

Proof. On one hand, suppose that $\alpha \in K^*$ is such that $\alpha^{1/d} \notin K$ for any proper divisor d of n. Then every automorphism of $K(\alpha^{1/n})$ over K must have the form $\alpha \mapsto \alpha\zeta_n^r$ for some $r \in \mathbb{Z}/n\mathbb{Z}$; this defines a homomorphism $\mathrm{Gal}(K(\alpha^{1/n})/K) \cong \mathbb{Z}/n\mathbb{Z}$ which is injective because any automorphism of $K(\alpha^{1/n})$ over K is uniquely determined by its effect on $\alpha^{1/n}$. We claim that this map is also surjective. If n is prime, we can see this from the fact that by hypothesis $K(\alpha^{1/p}) \neq K$, so the map $\mathrm{Gal}(K(\alpha^{1/n})/K) \cong \mathbb{Z}/n\mathbb{Z}$ is an injective map from a nonzero group into a prime cyclic group and hence must be surjective. In the general case, note that the definition of the map $\mathrm{Gal}(K(\alpha^{1/n})/K) \cong \mathbb{Z}/n\mathbb{Z}$ is compatible with replacing n with one of its prime factors p, and this logic tells us that the image of $\mathrm{Gal}(K(\alpha^{1/n})/K)$ in $\mathbb{Z}/n\mathbb{Z}$ cannot be contained in $p\mathbb{Z}/n\mathbb{Z}$ for any prime divisor p of n. So again we conclude that $\mathrm{Gal}(K(\alpha^{1/n})/K) \cong \mathbb{Z}/n\mathbb{Z}$. (As a corollary, we deduce that the polynomial $x^n - \alpha$ is irreducible over K; see Exercise 4 and Exercise 5 for discussion of what happens when $\zeta_n \notin K$.)
On the other hand, let L be an arbitrary $\mathbb{Z}/n\mathbb{Z}$-extension of K. Choose a generator $g \in \mathrm{Gal}(L/K)$, and let $f : \mathrm{Gal}(L/K) \to L^*$ be the map that sends rg to ζ_n^r for $r \in \mathbb{Z}$. Then $f \in H^1(\mathrm{Gal}(L/K), L^*)$, so there exists $t \in L$ such that $t^{rg}/t = f(rg) = \zeta_n^r$ for $r \in \mathbb{Z}$. In particular, t^n is invariant under $\mathrm{Gal}(L/K)$, so $t^n = \alpha$ for some $\alpha \in K$ and $L = K(t) = K(\alpha^{1/n})$, as desired. ■

Remark 1.2.7 Another way to state Theorem 1.2.6 is as a bijection

$$(\mathbb{Z}/n\mathbb{Z})^r\text{-extensions of } K \longleftrightarrow (\mathbb{Z}/n\mathbb{Z})^r\text{-subgroups of } K^*/(K^*)^n,$$

where $(K^*)^n$ is the group of n-th powers in K^*. (What we proved above was the case $r = 1$, but the general case follows at once.) Another way is in terms of the absolute Galois group of K, as in Theorem 1.2.9 below.

The Kummer pairing

Definition 1.2.8 Define the **Kummer pairing**

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\overline{K}/K) \times K^* \to \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$$

as follows: given $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $z \in K^*$, choose $y \in \overline{K}^*$ such that $y^n = z$, and put $\langle \sigma, z \rangle = y^\sigma / y$. Note that this does not depend on the choice of y: the other possibilities are $y\zeta_n^k$ for $k = 0, \ldots, n-1$, and $\zeta_n^\sigma = \zeta_n$ by the assumption on K, so it drops out. ◊

Theorem 1.2.9 Kummer reformulated. *The Kummer pairing induces an isomorphism*

$$K^*/(K^*)^n \to \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z})$$

where the subscript cts *indicates continuous homomorphisms for the profinite topology on* $\mathrm{Gal}(\overline{K}/K)$ *and the discrete topology on* $\mathbb{Z}/n\mathbb{Z}$. *Concretely, this*

means we consider homomorphisms that factor through a quotient of the form $\mathrm{Gal}(L/K)$ *for some finite extension* L *of* K*.*

Proof. The map comes from the pairing; we have to check that it is injective and surjective. If $y \in K^* \setminus (K^*)^n$, then $K(y^{1/n})$ is a nontrivial Galois extension of K, so there exists some element of $\mathrm{Gal}(K(y^{1/n})/K)$ that doesn't preserve $y^{1/n}$. Any lift of that element to $\mathrm{Gal}(\overline{K}/K)$ pairs with y to give something other than 1; that is, y induces a nonzero homomorphism of $\mathrm{Gal}(\overline{K}/K)$ to $\mathbb{Z}/n\mathbb{Z}$. Thus injectivity follows.
On the other hand, suppose $f : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/n\mathbb{Z}$ is a homomorphism whose image is the cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. Let H be the kernel of f; then the fixed field L of H is a $\mathbb{Z}/d\mathbb{Z}$-extension of K with Galois group $\mathrm{Gal}(\overline{K}/K)/H$. By Kummer theory, $L = K(y^{1/d})$ for some y. But now the homomorphisms induced by $y^{mn/d}$, as m runs over all integers coprime to d, give all possible surjective homomorphisms of $\mathrm{Gal}(\overline{K}/K)/H$ to $\mathbb{Z}/d\mathbb{Z}$, so one of them must equal f. Thus surjectivity follows. ∎

Cyclic extensions without roots of unity

Remark 1.2.10 If K is of characteristic coprime to n but $\zeta_n \notin K$, then an extension of the form $K(a^{1/n})$ is in general not Galois. For some analysis of such extensions, see Exercise 4 and Exercise 5.

By the same token, $\mathbb{Z}/n\mathbb{Z}$-extensions of a field that does not contains ζ_n are harder to describe than Kummer extensions, and indeed describing such extensions of $\mathbb{Q}$ is the heart of this course. One statement that ties this together with the previous point is that if L/K is a $\mathbb{Z}/n\mathbb{Z}$-extension, then $L(\zeta_n)/K(\zeta_n)$ is a $\mathbb{Z}/d\mathbb{Z}$-extension for some divisor d of n, and the latter is a Kummer extension.

We will use the following elaboration of Remark 1.2.10 in the proof of the Kronecker-Weber theorem (Theorem 1.3.4).

Lemma 1.2.11 *Let* n *be a prime (or an odd prime power), let* K *be a field of characteristic coprime to* n*, let* $L = K(\zeta_n)$*, and let* $M = L(a^{1/n})$ *for some* $a \in L^*$*. Define the homomorphism* $\omega : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^*$ *by the relation* $\zeta_n^{\omega(g)} = \zeta_n^g$*. Then* M/K *is Galois and abelian if and only if*

$$a^g/a^{\omega(g)} \in (L^*)^n \qquad \forall g \in \mathrm{Gal}(L/K). \tag{1.2.1}$$

(Note that $\omega(g)$ *is only defined up to adding a multiple of* n*, but this is enough to interpret* $a^{\omega(g)}$ *modulo* $(L^*)^n$*.)*

Proof. If $a^g/a^{\omega(g)} \in (L^*)^n$ for all $g \in \mathrm{Gal}(L/K)$, then a, $a^{\omega(g)}$ and a^g all generate the same subgroup of $(L^*)/(L^*)^n$. Thus $L(a^{1/n}) = L((a^g)^{1/n})$ for all $g \in \mathrm{Gal}(L/K)$, so M/K is Galois. Thus it suffices to assume M/K is Galois, then prove that M/K is abelian if and only if (1.2.1) holds. In this case, we must have $a^g/a^{\rho(g)} \in (M^*)^n$ for some map $\rho : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^*$, whose codomain is cyclic by our assumption on n.
Note that $\mathrm{Gal}(M/K)$ admits a homomorphism ω to a cyclic group whose kernel $\mathrm{Gal}(M/L) \subseteq \mathbb{Z}/n\mathbb{Z}$ is also abelian. Thus $\mathrm{Gal}(M/K)$ is abelian if and only if g and h commute for any $g \in \mathrm{Gal}(M/K)$ and $h \in \mathrm{Gal}(M/L)$, i.e., if $h = g^{-1}hg$. (Since g commutes with powers of itself, g then commutes with everything.)
Let $A \subseteq L^*/(L^*)^n$ be the subgroup generated by a. Then the Kummer pairing gives rise to a pairing

$$\mathrm{Gal}(M/L) \times A \to \{1, \zeta_n, \dots, \zeta_n^{n-1}\}$$

which is bilinear and nondegenerate, so $h = g^{-1}hg$ if and only if $\langle h, s^g \rangle =$

$\langle ghg^{-1}, s^g \rangle$ for all $s \in A$. But the Kummer pairing is **equivariant** with respect to $\mathrm{Gal}(L/K)$ as follows:

$$\langle h, s \rangle^g = \langle g^{-1}hg, s^g \rangle,$$

because

$$\left(\frac{(s^{1/n})^h}{s^{1/n}} \right)^g = \frac{((s^g)^{1/n})^{g^{-1}hg}}{(s^g)^{1/n}}.$$

(Here by $s^{1/n}$ I mean an arbitrary n-th root of s in M, and by $(s^g)^{1/n}$ I mean $(s^{1/n})^g$. Remember that the value of the Kummer pairing doesn't depend on which n-th root you choose.) Thus $h = ghg^{-1}$ if and only if $\langle h, s^g \rangle = \langle h, s \rangle^g$ for all $s \in A$, or equivalently, just for $s = a$. But

$$\langle h, a \rangle^g = \langle h, a \rangle^{\omega(g)} = \langle h, a^{\omega(g)} \rangle.$$

Thus g and h commute if and only if $\langle h, a^g \rangle = \langle h, a^{\omega(g)} \rangle$, if and only if (by nondegeneracy) $a^g / a^{\omega(g)} \in (L^*)^n$, as desired. ■

Remark 1.2.12 In what follows, we will only need one implication of Lemma 1.2.11: if M/K is Galois and abelian, then (1.2.1) holds. However, we chose to include both implications for completeness.

Exercises

1. Prove **Dedekind's lemma** on the linear independence of automorphisms: if $g_1, \dots, g_n$ are distinct automorphisms of L over K, then there do not exist $x_1, \dots, x_n \in L$ such that $x_1 y^{g_1} + \cdots + x_n y^{g_n} = 0$ for all $y \in L$. (This is a key step in the proof of **Artin's lemma** in Galois theory.)

Hint. Suppose the contrary, choose a counterexample with n as small as possible, then make an even smaller counterexample.

2. Prove the additive analogue of Lemma 1.2.3: if L/K is a finite Galois extension with Galois group G, then $H^1(G, L) = 0$, where the abelian group is now the additive group of L.

Hint. By the normal basis theorem (see for example [32]), there exists $\alpha \in L$ whose conjugates form a basis of L as a K-vector space.

3. Prove the following extension of Lemma 1.2.3 (also due to Speiser). Let L/K be a finite Galois extension with Galois group G. Despite the fact that $H^1(G, \mathrm{GL}(n, L))$ does not make sense as a group (because $\mathrm{GL}(n, L)$ is not abelian), show nonetheless that "$H^1(G, \mathrm{GL}(n, L))$ is trivial" in the sense that every function $f : G \to \mathrm{GL}(n, L)$ for which $f(gh) = f(g)^h f(h)$ for all $g, h \in G$ can be written as $x(x^g)^{-1}$ for some $x \in \mathrm{GL}(n, L)$.

Hint. To imitate the proof in the case $n = 1$, one must find an $n \times n$ matrix x over L such that $t = \sum_{g \in G} x^g f(g)$ is not only nonzero but *invertible*. To establish this, note that the set of possible values of t on one hand is an L-vector space, and on the other hand satisfies no nontrivial L-linear relation. (See Lemma 7.1.15 for a similar idea.)

4. Let n be a positive integer, let K be a field of characteristic coprime to n, choose $a \in K^*$, and put $L = K(a^{1/n})$. Prove that $[L : K]$ divides n.

Hint. Reduce to the case where n is prime. Since $[K(\zeta_n) : K]$ is coprime to n, by taking norms we see that $a \in (K^*)^n$ if and only if $a \in (K(\zeta_n)^*)^n$; we may thus reduce to the case $\zeta_n \in K$, to which Kummer theory applies.

5. With notation as Exercise 4, prove that $[L : K] = n$ if and only if $a \notin (K^*)^p$ for any prime divisor p of n.

Hint. We may proceed by induction on n once we check that for any prime divisor q of n, if $a \notin (K^*)^p$ for any prime divisor p of n, then $a^{1/q} \notin ((K(a^{1/q})^*)^p$ for any prime divisor p of n. To prove this, assume the contrary; since $[K(a^{1/q}) : K] = q$, taking norms yields $a \in (K^*)^p$, a contradiction.

1.3 The local Kronecker-Weber theorem

Reference. [56], Chapter 14.

We now prove the local Kronecker-Weber theorem (Theorem 1.1.5), modulo some steps which will be left as exercises. As shown previously, this will imply the original Kronecker-Weber theorem.

Extensions of local fields

We first recall the following facts from the theory of local fields (e.g., see [37] II.7).

Definition 1.3.1 Let L/K be an extension of finite extensions of $\mathbb{Q}_p$. Let $\mathfrak{o}_K, \mathfrak{o}_L$ be the integral closures of $\mathbb{Z}_p$ in K, L. We say that L/K is **unramified** if the maximal ideal of $\mathfrak{o}_K$ generates the maximal ideal of $\mathfrak{o}_L$. In other words, any element π of K which generates the maximal ideal of $\mathfrak{o}_K$ (i.e., any **uniformizer** of K) is also a uniformizer of L. In still other words, the condition is that the **ramification index** $e(L/K)$ is equal to 1.

In general, there is a maximal subextension of L/K which is unramified. If this is K itself, we say that L/K is **totally ramified**.

Let U be the maximal unramified subextension of L/K. We say that L/K is **tamely ramified** if the degree $[L : U]$ is not divisible by p. In other words, the condition is that $e(L/K)$ is not divisible by p. ◊

Lemma 1.3.2 *Let L/K be an unramified extension of finite extensions of $\mathbb{Q}_p$. Then $L = K(\zeta_{q-1})$, where q is the cardinality of the residue field of L.*

Proof. Choose $u \in \mathfrak{o}_L$ generating the residue field of L over the residue field of K, and let $P(x)$ be the minimal polynomial of u over K. Then over the residue field of K, $P(x)$ divides the $(q-1)$-st cyclotomic polynomial, so by Hensel's lemma it splits over $K(\zeta_{q-1})$. Hence $L \subseteq K(\zeta_{q-1})$, and equality follows by comparing degrees. ■

Lemma 1.3.3 *Let L/K be a totally and tamely ramified extension of finite extensions of $\mathbb{Q}_p$ of degree e. Then there exists a uniformizer π of K such that $L = K(\pi^{1/e})$.*

Proof. Let π_L be a uniformizer of L. Then π_L^e can be written as a product of a uniformizer π of K times an element u of $\mathfrak{o}_L$ congruent to 1 modulo π_L. By Hensel's lemma, u has an e-th root in L, as then does π. ■

Proof of local Kronecker-Weber

We now proceed to the proof of Theorem 1.3.4, modulo some lemmas which we fill in later.

Theorem 1.3.4 Local Kronecker-Weber. *If $K/\mathbb{Q}_p$ is a finite abelian extension, then $K \subseteq \mathbb{Q}_p(\zeta_n)$ for some positive integer n.*

Proof. Since $\mathrm{Gal}(K/\mathbb{Q}_p)$ decomposes into a product of cyclic groups of prime-power order, by the structure theorem for finite abelian groups we may write K as the compositum of extensions of $\mathbb{Q}_p$ whose Galois groups are cyclic of prime-power order. In other words, it suffices to prove local Kronecker-Weber under the assumption that $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r\mathbb{Z}$ for some prime q and some positive integer r. We split this discussion into three cases; see Lemma 1.3.5, Lemma 1.3.6, and Lemma 1.3.7. ■

Lemma 1.3.5 *The statement of Theorem 1.3.4 holds when* $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r\mathbb{Z}$ *for some prime* $q \neq p$.

Proof. To begin, note that $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally tamely ramified of degree $p-1$, so by Lemma 1.3.3 it has the form $\mathbb{Q}_p(c^{1/(p-1)})$ for some $c \in p\mathbb{Z}_p^*$. (The value of c won't be critical here, but see Lemma 1.3.8 for later reference.)
Let L be the maximal unramified subextension of K. By Lemma 1.3.2, $L = \mathbb{Q}_p(\zeta_n)$ for some n. Let $e = [K : L]$. Since e is a power of q, e is not divisible by p, so K is totally and tamely ramified over L. Thus by Lemma 1.3.3, there exists $\pi \in L$ generating the maximal ideal of $\mathfrak{o}_L$ such that $K = L(\pi^{1/e})$. Since $L/\mathbb{Q}_p$ is unramified, p also generates the maximal ideal of $\mathfrak{o}_L$, so we can write $\pi = cu$ for some unit $u \in \mathfrak{o}_L^*$. Now $L(u^{1/e})/L$ is unramified since e is prime to p and u is a unit. In particular, $L(u^{1/e})/\mathbb{Q}_p$ is unramified, hence abelian. Then $K(u^{1/e})/\mathbb{Q}_p$ is the compositum of the two abelian extensions $K/\mathbb{Q}_p$ and $L(u^{1/e})/\mathbb{Q}_p$, so it's also abelian. Hence any subextension is abelian, in particular $\mathbb{Q}_p(c^{1/e})/\mathbb{Q}_p$.
For $\mathbb{Q}_p(c^{1/e})/\mathbb{Q}_p$ to be Galois, it must contain the e-th roots of unity (since it must contain all of the e-th roots of $-p$, and we can divide one by another to get an e-th root of unity). But $\mathbb{Q}_p(c^{1/e})/\mathbb{Q}_p$ is totally ramified, whereas $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is unramified. This is a contradiction unless $\mathbb{Q}_p(\zeta_e)$ is actually equal to $\mathbb{Q}_p$, which only happens if $e|(p-1)$ (since the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p$ contains only $(p-1)$-st roots of unity).
Now $K \subseteq L(c^{1/e}, u^{1/e})$ as noted above. But on one hand, $L(u^{1/e})$ is unramified over L, so $L(u^{1/e}) = L(\zeta_m)$ for some m; on the other hand, because $e|(p-1)$, we have $\mathbb{Q}_p(c^{1/e}) \subseteq \mathbb{Q}_p(c^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$. Putting it all together,

$$K \subseteq L(c^{1/e}, u^{1/e}) \subseteq \mathbb{Q}_p(\zeta_n, \zeta_p, \zeta_m) \subseteq \mathbb{Q}_p(\zeta_{mnp}).$$

■

Lemma 1.3.6 *The statement of Theorem 1.3.4 holds when* $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r\mathbb{Z}$ *for* $q = p \neq 2$.

Proof. Suppose $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z}$. We can use roots of unity to construct two other extensions of $\mathbb{Q}_p$ with this Galois group. Namely, $\mathbb{Q}_p(\zeta_{p^{p^r}-1})/\mathbb{Q}_p$ is unramified of degree p^r, and automatically has cyclic Galois group; meanwhile, the index $p-1$ subfield of $\mathbb{Q}_p(\zeta_{p^{r+1}})$ is totally ramified with Galois group $\mathbb{Z}/p^r\mathbb{Z}$. By assumption, K is not contained in the compositum of these two fields, so for some $s > 0$,

$$\mathrm{Gal}(K(\zeta_{p^{p^r}-1}, \zeta_{p^{r+1}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

This group admits $(\mathbb{Z}/p\mathbb{Z})^3$ as a quotient, so we have an extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$. We rule this out using Lemma 1.3.9. ■

Lemma 1.3.7 *The statement of Theorem 1.3.4 holds when* $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r\mathbb{Z}$ *for* $q = p = 2$.

Proof. This is similar to Lemma 1.3.6, but a bit messier because $\mathbb{Q}_2$ *does* admit an extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. We defer this case to the exercises; see Exercise 4, Exercise 5, and Exercise 6. ■

Filling in the details

We now return to the lemmas that we skipped over in the proof of Theorem 1.3.4. At this point, we make heavy use of Kummer theory.

Lemma 1.3.8 *The fields $\mathbb{Q}_p((-p)^{1/(p-1)})$ and $\mathbb{Q}_p(\zeta_p)$ are equal.*

Proof. See Exercise 1. ■

Lemma 1.3.9 *For $p \neq 2$, there is no extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$.*

Proof. For convenience, put $\pi = \zeta_p - 1$. Then π is a uniformizer of $\mathbb{Q}_p(\zeta_p)$.
If $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^3$, then $\mathrm{Gal}(K(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^3$ as well, and $K(\zeta_p)$ is abelian over $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^3$. Applying Kummer theory to $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ produces a subgroup $B \subseteq \mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$ such that $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, B^{1/p})$.
Let $\omega : \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^*$ be the canonical map; since $\mathbb{Q}_p(\zeta_p, b^{1/p}) \subseteq K(\zeta_p)$ is also abelian over $\mathbb{Q}_p$, by Lemma 1.2.11,

$$b^g/b^{\omega(g)} \in (\mathbb{Q}_p(\zeta_p)^*)^p \qquad (\forall b \in B, g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)).$$

Recall the structure of $\mathbb{Q}_p(\zeta_p)^*$: the maximal ideal of $\mathbb{Z}_p[\zeta_p]$ is generated by π, while each unit of $\mathbb{Z}_p[\zeta_p]$ is congruent to a $(p-1)$-st root of unity modulo π, and so

$$\mathbb{Q}_p(\zeta_p)^* = \pi^{\mathbb{Z}} \times (\zeta_{p-1})^{\mathbb{Z}} \times U_1,$$

where U_1 denotes the set of units of $\mathbb{Z}_p[\zeta_p]$ congruent to 1 modulo π. Correspondingly,

$$(\mathbb{Q}_p(\zeta_p)^*)^p = \pi^{p\mathbb{Z}} \times (\zeta_{p-1})^{p\mathbb{Z}} \times U_1^p.$$

Now choose a representative $a \in L^*$ of some nonzero element of B; without loss of generality, we may assume $a = \pi^m u$ for some $m \in \mathbb{Z}$ and $u \in U_1$. Then

$$\frac{a^g}{a^{\omega(g)}} = \frac{(\zeta_p^{\omega(g)} - 1)^m}{\pi^{m\omega(g)}} \frac{u^g}{u^{\omega(g)}};$$

but $v_\pi(\pi) = v_\pi(\zeta_p^{\omega(g)} - 1) = 1$. Thus the valuation of the right hand side is $m(1 - \omega(g))$, which can only be a multiple of p for all g if $m \equiv 0 \pmod{p}$. (Notice we just used that p is odd!) That is, we could have taken $m = 0$ and $a = u \in U_1$.
As for $u^g/u^{\omega(g)}$, note that U_1^p is precisely the set of units congruent to 1 modulo π^{p+1} (see Exercise 2). Since $\zeta_p = 1 + \pi + O(\pi^2)$, we can write $u = \zeta_p^b(1 + c\pi^d + O(\pi^{d+1}))$, with $c \in \mathbb{Z}$ and $d \geq 2$. Since $\pi^g/\pi \equiv \omega(g) \pmod{\pi}$, we get

$$u^g = \zeta_p^{b\omega(g)}(1 + c\omega(g)^d\pi^d + O(\pi^{d+1})),$$
$$u^{\omega(g)} = \zeta_p^{b\omega(g)}(1 + c\omega(g)\pi^d + O(\pi^{d+1})).$$

But these two have to be congruent modulo π^{p+1}. Thus either $d \geq p+1$ or $d \equiv 1 \pmod{p-1}$, the latter only occurring for $d = p$.
What this means is that the set of possible u is generated by ζ_p and by $1 + \pi^p$. But these only generate a subgroup of U_1/U_1^p isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, whereas $B \cong (\mathbb{Z}/p\mathbb{Z})^3$. Contradiction. ■

Exercises

1. Prove Lemma 1.3.8.

Hint. Prove that $(\zeta_p - 1)^{p-1}/p - 1$ belongs to the maximal ideal of $\mathbb{Z}_p[\zeta_p]$.

2. Prove that (in the notation of Lemma 1.3.9) U_1^p is the set of units congruent to 1 modulo π^{p+1}.

Hint. In one direction, write $u \in U_1$ as a power of ζ_p times a unit congruent to 1 modulo π^2. In the other direction, use the binomial series for $(1+x)^{1/p}$. (See Exercise 1 for a generalization of this result.)

3. Prove that for any $r > 0$, there is an extension of $\mathbb{Q}_2$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2$ contained in $\mathbb{Q}_2(\zeta_n)$ for some $n > 0$.

Hint. Consider $L = \mathbb{Q}_2(\zeta_{2^{r+1}}, \zeta_{2^r-1})$.

4. Suppose that $K/\mathbb{Q}_2$ is a $\mathbb{Z}/2^r\mathbb{Z}$-extension not contained in $\mathbb{Q}_2(\zeta_n)$ for any $n > 0$. Prove that there exists an extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$.

Hint. Compare K with its compositum with some field L as in Exercise 3. Use the structure of finite abelian groups to show that if $LK \neq L$, then $\mathrm{Gal}(LK/\mathbb{Q}_2)$ is forced to have a quotient of the specified form.

5. Prove that there is no extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$.

Hint. Use Kummer theory to show that every quadratic extension of $\mathbb{Q}_2$ is contained in $\mathbb{Q}_2(\zeta_{24})$.

6. Prove that there is no extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/4\mathbb{Z})^3$.

Hint. Reduce to showing that there exists no extension of $\mathbb{Q}_2$ containing $\mathbb{Q}_2(\sqrt{-1})$ with Galois group $\mathbb{Z}/4\mathbb{Z}$. Prove this by following the argument of Lemma 1.3.9.

Chapter 2

The statements of class field theory

We next give the statements of the principal results of class field theory, with almost no proofs. Our goal at this point is to clarify what the statements say and how they can be applied. We will have to discuss plenty of other material before returning to the proofs, but the reader who wishes to peek ahead for a glimpse of the strategy is directed to Section 5.4.

Definition 2.0.1 Jargon watch. By a **place** of a number field K, we mean either an archimedean completion $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$ (an **infinite place**), or a $\mathfrak{p}$-adic completion $K \hookrightarrow K_{\mathfrak{p}}$ for some nonzero prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$ (a **finite place**). (Note: there is only one place for each pair of complex embeddings of K.)

Each place corresponds to an equivalence class of absolute values on K; if v is a place, we write K_v for the corresponding completion, which is either $\mathbb{R}$, $\mathbb{C}$, or $K_{\mathfrak{p}}$ for some prime $\mathfrak{p}$.

This form of parity between finite and infinite places will be a recurring theme throughtout this book. ◊

2.1 The Hilbert class field

Reference. [36], Introduction; [37], VI.6.

An example of an unramified extension

Recall that the field $\mathbb{Q}$ has no extensions which are everywhere unramified (Theorem 1.1.9). This is quite definitely not true of other number fields; we begin with an example illustrating this.

Example 2.1.1 An unramified extension of a number field. In the number field $K = \mathbb{Q}(\sqrt{-5})$, the ring of integers is $\mathbb{Z}[\sqrt{-5}]$ and the ideal (2) factors as $\mathfrak{p}^2$, where the ideal $\mathfrak{p} = (2, 1 + \sqrt{-5})$ is not principal.

Now let's see what happens when we adjoin a square root of -1, obtaining $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. The extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ only ramifies over 2, so L/K can only be ramified over $\mathfrak{p}$. On the other hand, if we write $L = K(\alpha)$ where $\alpha = (1+\sqrt{5})/2$, then modulo $\mathfrak{p}$ the minimal polynomial $x^2 - x - 1$ of α remains irreducible, so $\mathfrak{p}$ is unramified (and not split) in L. □

Hilbert class fields

We've now seen that $\mathbb{Q}(\sqrt{-5})$ admits both a nonprincipal ideal and an unramified abelian extension. It turns out these are not unrelated events.

Definition 2.1.2 Jargon watch. In class field theory, the phrase "L/K is unramified" is conventionally interpreted to mean that L/K is unramified over all finite places in the usual sense, *and* that every real embedding of K extends to a real embedding of L. ◊

Theorem 2.1.3 *Let L be the maximal unramified abelian extension of a number field K. Then L/K is finite, and its Galois group is isomorphic to the ideal class group $\mathrm{Cl}(K)$ of K. The field L is called the* ***Hilbert class field*** *of K.*

Proof. A canonical isomorphism will be given by the Artin reciprocity law (Theorem 2.2.6). ■

Remark 2.1.4 While Theorem 2.1.3 implies that an abelian unramified extension must be finite, there can be infinite unramified *nonabelian* extensions. See Remark 2.3.12.

Remark 2.1.5 At this point, it should now be apparent that **class field theory** is "class field" theory, i.e., the theory of **class fields** such as the Hilbert class fields (and other examples described in Definition 2.2.7) rather than a special type of "field theory". Whether this affects your pronunciation of the entire phrase is up to you!

Exercises

1. Let K be an imaginary quadratic extension of $\mathbb{Q}$ in which t finite primes ramify. Assuming Theorem 2.1.3, prove that $\#(\mathrm{Cl}(K)/2\,\mathrm{Cl}(K)) = 2^{t-1}$; this recovers a theorem of Gauss originally proved using binary quadratic forms.

Hint. If an odd prime p ramifies in K, show that $K(\sqrt{p^*})/K$ is unramified for $p^* = (-1)^{(p-1)/2}p$; if 2 ramifies in K, show that $K(p^*)/K$ is unramified for one of $p^* = -1, 2, -2$.

2. Give an example, using a real quadratic field, to illustrate that:

(a) Theorem 2.1.3 fails if we don't require the extensions to be unramified above the real place;

(b) the previous exercise fails for real quadratic fields.

3. Prove that Exercise 1 extends to real quadratic fields if one replaces the class group by the **narrow class group**, in which you only mod out by principal ideals having a totally positive generator. This gives an example of a **ray class group**; more on those in Section 2.2.

4. The field $\mathbb{Q}(\sqrt{-23})$ admits an ideal of order 3 in the class group and an unramified abelian extension of degree 3. Find both.

Hint. The extension contains a cubic field of discriminant -23.

5. Let L/K be an extension of number fields admitting no nontrivial abelian subextension M/K which is everywhere unramified (including at archimedean places). Assuming Theorem 2.1.3, prove that the class number of K divides the class number of L.

6. A number field K is called a **CM field** if it is a totally complex quadratic extension of a totally real number field K_+. Using Exercise 5, show that the class number of K_+ divides the class number of K. The ratio is called

the **relative class number**.

7. Let K be a number field of degree n with Galois group S_n whose discriminant D is squarefree. Prove that the Galois closure of K is unramified over all finite places of $\mathbb{Q}(\sqrt{D})$. This gives an ample supply of everywhere unramified extensions (of various fields) which are nonabelian for $n > 3$.

Hint. Let M be the Galois closure of K. For any odd prime p dividing the discriminant, use the restriction on D to show that there is exactly one prime of K above p which is ramified and that its ramification index is 2. Then deduce that the inertia group of a prime of M above p has order 2, and finally argue that said prime is unramified over its restriction to $\mathbb{Q}(\sqrt{D})$.

2.2 Generalized ideal class groups and the Artin reciprocity law

Reference. [36] V.1; [37] VI.6.

An example (continued)

Before proceeding to generalized ideal class groups, we continue a bit with Example 2.1.1 to illustrate what is about to happen.

Proposition 2.2.1 *For $K = \mathbb{Q}(\sqrt{-5}), L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$, let $\mathfrak{p}$ be a prime of $\mathfrak{o}_K$. Then $\mathfrak{p}$ splits in L if and only if $\mathfrak{p}$ is principal.*

Proof. First suppose $\mathfrak{p} = (p)$, where $p \neq 2, 5$ is a rational prime that remains inert (i.e., does not split and is not ramified) in K. This happens if and only if -5 is not a square mod p. In this case, one of -1 and 5 is a square in $\mathbb{F}_p$, so $\mathfrak{o}_K/\mathfrak{p}$ contains a square root of one of them, hence of both (since -5 already has a square root there). Thus the residue field does not grow when we pass to L, that is, $\mathfrak{p}$ is split.

Next suppose $p \neq 2, 5$ is a rational prime that splits as $\mathfrak{p}\overline{\mathfrak{p}}$. If $\mathfrak{p} = (\beta)$ is principal, then the equation $x^2 + 5y^2 = p$ has a solution in $\mathbb{Z}$ (namely, for $x + y\sqrt{-5} = \beta$), but this is only possible if $p \equiv 1 \pmod 4$. Then p splits in $\mathbb{Q}(\sqrt{-1})$ as well, so p is totally split in L, so $\mathfrak{p}$ splits in L.

Conversely, suppose $\mathfrak{p}$ is not principal. Since there are only two ideal classes in $\mathbb{Q}(\sqrt{-5})$, we have $\mathfrak{p} = \alpha(2, 1 + \sqrt{-5})$ for some $\alpha \in K$. Thus $\mathrm{Norm}(\mathfrak{p}) = |\mathrm{Norm}(\alpha)|\,\mathrm{Norm}(2, 1 + \sqrt{-5})$. If $\alpha = x + y\sqrt{-5}$ for $x, y \in \mathbb{Q}$, we then have $p = 2(x^2 + 5y^2)$. Considering things mod 4, we see that $2x$ and $2y$ must be ratios of two odd integers, and $p \equiv 3 \pmod 4$. Thus p does not split in L, so $\mathfrak{p}$ cannot split in L.

The only cases left are $\mathfrak{p} = (2, 1 + \sqrt{-5})$, which does not split (see above), and $\mathfrak{p} = (\sqrt{-5})$, which does split (since -1 has a square root mod 5). ∎

Remark 2.2.2 As a bonus, note that in Proposition 2.2.1, for any ideal $\mathfrak{a}$ of $\mathfrak{o}_K$, $\mathfrak{a}\mathfrak{o}_L$ is principal. (To check this, it suffices to verify that $(2, 1 + \sqrt{-5})\mathfrak{o}_L = (1 + \sqrt{-1})\mathfrak{o}_L$.) This is a special case of the principal ideal theorem (Theorem 2.3.1).

Generalized ideal class groups

In this section, we formulate (without proof) the Artin reciprocity law for an arbitrary abelian extension L/K of number fields. This map will generalize the canonical isomorphism, in the case $K = \mathbb{Q}$, of $\mathrm{Gal}(L/\mathbb{Q})$ with a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ for some m, as well as the splitting behavior we saw in the previous

example. Before proceeding, we need to define the appropriate generalization of $(\mathbb{Z}/m\mathbb{Z})^*$ to number fields.

Definition 2.2.3 Recall that the ideal class group $\mathrm{Cl}(K)$ of K is defined as the group J_K of fractional ideals modulo the subgroup P_K of principal fractional ideals. Let $\mathfrak{m}$ be a formal product of places of K; you may regard such a beast as an ordinary integral ideal together with a nonnegative coefficient for each infinite place.

Let $J_K^{\mathfrak{m}}$ be the group of fractional ideals of K which are coprime to each finite place of K occurring in $\mathfrak{m}$. Let $P_K^{\mathfrak{m}} \subseteq J_K^{\mathfrak{m}}$ be the group of principal fractional ideals generated by elements $\alpha \in K$ such that:

- for $\mathfrak{p}^e | \mathfrak{m}$ finite, $\alpha \equiv 1 \pmod{\mathfrak{p}^e}$;
- for every real place τ in $\mathfrak{m}$, $\tau(\alpha) > 0$.

(There is no condition for complex places.) Then the **ray class group** $\mathrm{Cl}^{\mathfrak{m}}(K)$ is defined as the quotient $J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. A quotient of a ray class group is called a **generalized ideal class group**. ◊

The Artin reciprocity law

We imitate the "reciprocity law" construction we made for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ (Definition 1.1.7) with a general abelian extension of number fields, but this time with no *a priori* reason to expect it to give anything useful.

Definition 2.2.4 Let L/K be a (finite) abelian extension of number fields. For each prime $\mathfrak{p}$ of K that does not ramify in L, let $\mathfrak{q}$ be a prime of L above K, and put $\kappa = \mathfrak{o}_K/\mathfrak{p}$ and $\lambda = \mathfrak{o}_L/\mathfrak{q}$. Then the residue field extension λ/κ is an extension of finite fields, so it has a canonical generator σ, the Frobenius, which acts by raising to the q-th power. (Here $q = \mathrm{Norm}(\mathfrak{p}) = \#\kappa$ is the absolute norm of $\mathfrak{p}$.) Since $\mathfrak{p}$ does not ramify, the decomposition group $G_{\mathfrak{q}}$ is isomorphic to $\mathrm{Gal}(\lambda/\kappa)$, so we get a canonical element of $G_{\mathfrak{q}}$, called the Frobenius of $\mathfrak{q}$. In general, replacing $\mathfrak{q}$ by $\mathfrak{q}^\tau$ for some $\tau \in \mathrm{Gal}(L/K)$ conjugates both the decomposition group and the Frobenius by τ; since L/K is abelian in our case, that conjugation has no effect. Thus we may speak of "the Frobenius of $\mathfrak{p}$" without ambiguity.

Now for $\mathfrak{m}$ divisible by all primes of K which ramify in L, define a homomorphism (the **Artin map**)

$$J_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K) \qquad \mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}\,.$$

◊

Remark 2.2.5 The fact that we have to avoid the ramified primes will be a bit of a nuisance later. Eventually we'll get around this using the adelic formulation (Section 6.4).

At this point, the following miracle occurs.

Theorem 2.2.6 Artin reciprocity. *There exists a formal product $\mathfrak{m}$ of places of K, including all (finite and infinite) places over which L ramifies, such that $P_K^{\mathfrak{m}}$ belongs to the kernel of the Artin map.*

Proof. We will deduce this much later from a corresponding statement made in the language of adèles and idèles. See Theorem 6.4.1 and Proposition 6.4.7. ■

In particular, we get a map $J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ which turns out to be surjective (see Exercise 5), but now we don't have the Kronecker-Weber theorem to explain this.

Definition 2.2.7 Define the **conductor** of L/K to be the smallest formal product $\mathfrak{m}$ for which the conclusion of Theorem 2.2.6 holds. We say L/K is the **ray class field** corresponding to the product $\mathfrak{m}$ if L/K has conductor dividing $\mathfrak{m}$ and the map $J_K/J_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is an isomorphism. ◊

Theorem 2.2.8 Existence of ray class fields. *Every formal product $\mathfrak{m}$ has a ray class field.*

Proof. Again, we will deduce this later from a statement in the adelic language. See Theorem 6.4.2. ■

Example 2.2.9 The ray class field of $\mathbb{Q}$ of conductor $m\infty$ is $\mathbb{Q}(\zeta_m)$. The ray class field of $\mathbb{Q}$ of conductor m is the maximal real subfield of $\mathbb{Q}(\zeta_m)$. □

Remark 2.2.10 Unfortunately, for number fields other than $\mathbb{Q}$, we do not have an explicit description of the ray class fields as being generated by particular algebraic numbers. A salient exception is the imaginary quadratic fields, for which the theory of elliptic curves with complex multiplication provides such numbers. Also, if we were to work with function fields instead of number fields, the theory of Drinfeld modules would do something similar.

This gap in our knowledge, also referred to as **Hilbert's 12th Problem**, will make establishing class field theory somewhat more complicated than it would be otherwise. In particular, the proof of Theorem 2.2.8 is rather inexplicit; see Section 7.4.

Exercises

1. For $\mathfrak{p}$ a prime ideal of K and L/K an abelian extension in which $\mathfrak{p}$ does not ramify, let $\mathrm{Frob}_{L/K}(\mathfrak{p}) \in \mathrm{Gal}(L/K)$ be the Frobenius of $\mathfrak{p}$. Prove that Frobenius obeys the following compatibilities:

(a) If M/L is another extension with M/K abelian, $\mathfrak{q}$ is a prime of L over $\mathfrak{p}$, and M/L is unramified over $\mathfrak{q}$, then $\mathrm{Frob}_{M/K}(\mathfrak{p})$ restricted to L equals $\mathrm{Frob}_{L/K}(\mathfrak{p})$.

(b) In this notation, $\mathrm{Frob}_{M/L}(\mathfrak{q}) = \mathrm{Frob}_{M/K}(\mathfrak{p})^{f(\mathfrak{q}/\mathfrak{p})}$, where f denotes the residue field degree.

2. Find a formula for the order of $\mathrm{Cl}^{\mathfrak{m}}(K)$ in terms of the order of $\mathrm{Cl}(K)$ and other relevant stuff.

Hint. It's in [36] V.1. Make sure you understand its proof!

3. Use Exercise 2 to give a formula for the order of $\mathrm{Cl}^{\mathfrak{m}}(\mathbb{Q}(\sqrt{D}))$ for D odd and squarefree, in terms of the prime factors of $\mathfrak{m}$ and D and the class number of $\mathbb{Q}(\sqrt{D})$.

4. Find the ray class field of $\mathbb{Q}(i)$ of conductor (3), and verify Artin reciprocity explicitly in this case.

2.3 The principal ideal theorem

Reference. [36], section V.3 (but you won't find the proofs I've omitted there either); [37], section VI.7 (see also IV.5); [33], section XI.5.

Statement of the theorem

For a change, we're going to prove something, although the proof will depend on the Artin reciprocity law which we haven't proved. Or rather, we're going to

sketch a proof that you will get to fill in by doing the exercises. (Why should I have all the fun?)

The following theorem is due to Furtwängler, a student of Hilbert. (It's also called the "capitulation" theorem, because the word "capitulate" was formerly used to mean "to become principal". Etymology left to the reader.)

Theorem 2.3.1 Principal ideal theorem. *Let L be the Hilbert class field of the number field K. Then every ideal of K becomes principal in L.*

Proof. This will follow by combining Theorem 2.3.7 (construction of the transfer homomorphism), Lemma 2.3.9 (implication that vanishing of the transfer homomorphism implies the desired result), and Theorem 2.3.10 (vanishing of the transfer homomorphism). ■

Example 2.3.2 If $K = \mathbb{Q}(\sqrt{-5})$, then $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$, and the nonprincipal ideal class of K is represented by $(2, 1 + \sqrt{-5})$, which is generated by $1 + \sqrt{-1}$ in L. □

First steps of the proof

The idea of the proof is to apply Artin reciprocity to reduce to a problem purely in finite group theory, which we then solve. To this end, let M be the Hilbert class field of L; then an ideal of L is principal if and only if its image under the Artin map $J_L \to \mathrm{Gal}(M/L)$ is trivial. So our first step will be to give a purely group-theoretic description of the map $V : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/L)$ corresponding to the extension homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ (i.e., making the diagram in Figure 2.3.3 commute, in which the horizontal arrows are Artin maps).

$$\begin{array}{ccc} \mathrm{Cl}(K) & \longrightarrow & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow V \\ \mathrm{Cl}(L) & \longrightarrow & \mathrm{Gal}(M/L) \end{array}$$

Figure 2.3.3

In order to proceed further, we must extract more information about the Galois groups in question.

1. The extension M/K is unramified because M/L and L/K are. It is also Galois: its image under any element of $\mathrm{Gal}(\overline{K}/K)$ is still an unramified abelian extension of L and so is contained in M.

2. The maximal subextension of M/K which is abelian over K is equal to L.

Translation into group theory

Definition 2.3.4 Given a finite group G, let G^{ab} denote the maximal abelian quotient of G; that is, G^{ab} is the quotient of G by its commutator subgroup G'. Then the previous discussion implies that $\mathrm{Gal}(M/L)$ is the commutator subgroup of $\mathrm{Gal}(M/K)$ and $\mathrm{Gal}(M/K)^{\mathrm{ab}} = \mathrm{Gal}(L/K)$. We may thus relabel Figure 2.3.3 as in Figure 2.3.5.

$$\begin{array}{ccc} \mathrm{Cl}(K) & \longrightarrow & \mathrm{Gal}(L/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}} \\ \downarrow & & \downarrow V \\ \mathrm{Cl}(L) & \longrightarrow & \mathrm{Gal}(M/L) = \mathrm{Gal}(M/L)^{\mathrm{ab}} \end{array}$$

Figure 2.3.5

◊

We now give the purely group-theoretic interpretation of the map V in Figure 2.3.5.

Definition 2.3.6 Let G be a finite group and H a (not necessarily normal) subgroup. Let $g_1, \ldots, g_n$ be left coset representatives of H in G: that is, $G = g_1 H \cup \cdots \cup g_n H$. For $g \in G$, put $\phi(g) = g_i$ if $g \in g_i H$ (i.e., $g_i^{-1} g \in H$). Put

$$V(g) = \prod_{i=1}^{n} \phi(g g_i)^{-1} (g g_i);$$

then $V(g)$ always lands in H.

Now consider what happens when we compose the map $g \mapsto V(g) : G \to H$ (which is not necessarily a homomorphism) with the projection $H \to H^{\mathrm{ab}}$. It will follow from Theorem 2.3.7 that the resulting map $G \to H^{\mathrm{ab}}$ is a homomorphism which factors through G^{ab}. The induced map $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is called the **transfer map** (in German "Verlagerung", hence the use of the letter V in the notation). ◊

Theorem 2.3.7 *With notation as in Definition 2.3.6, the map $V : G \to H^{\mathrm{ab}}$ is a homomorphism; it does not depend on the choice of the g_i; and induces a homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ (i.e., kills commutators in G).*

Proof. See Exercise 1. ■

Remark 2.3.8 In lieu of establishing Theorem 2.3.7 directly, one can derive it from properties of homology of finite groups. See Exercise 2.

Setting aside the proof of Theorem 2.3.7 for the moment, let's see that this does indeed give the correct map in Figure 2.3.5 when we take $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. This amounts to computing what happens when we apply all of the maps starting with a prime $\mathfrak{p}$ of K at the top left of the diagram.

Choose a prime $\mathfrak{q}$ of L over $\mathfrak{p}$ and a prime $\mathfrak{r}$ of M over $\mathfrak{q}$, let $G_{\mathfrak{r}} \subseteq G$ be the decomposition group of $\mathfrak{r}$ over K (i.e., the stabilizer of $\mathfrak{r}$ under the action of G on the primes above $\mathfrak{p}$), and let $g \in G_{\mathfrak{r}}$ be the Frobenius of $\mathfrak{r}$. Keep in mind that since G is not abelian, g depends on the choice of $\mathfrak{r}$, not just on $\mathfrak{q}$; that is, there's no Artin map into G.

Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the primes of L above $\mathfrak{p}$; then the image of $\mathfrak{p}$ in L is $\prod_i \mathfrak{q}_i$, and the image of that product under the Artin map is $\prod_i \mathrm{Frob}_{M/L}(\mathfrak{q}_i)$. To show that this equals $V(g)$, we make a careful choice of the coset representatives g_i in the definition of V. Namely, decompose G as a union of double cosets $G_{\mathfrak{r}} \tau_i H$. Then the primes of L above $\mathfrak{p}$ correspond to these double cosets, where the double coset $G_{\mathfrak{r}} \tau_i H$ corresponds to $L \cap \mathfrak{r}^{\tau_i}$. Let m be the order of $\mathrm{Frob}_{L/K}(\mathfrak{p})$ and write $G_{\mathfrak{r}} \tau_i H = \tau_i H \cup g \tau_i H \cup \cdots \cup g^{m-1} \tau_i H$ for each i; we then use the elements $g_{ij} = g^j \tau_i$ as the left coset representatives to define ϕ and V. Thus the equality $V(g) = \prod_i \mathrm{Frob}_{M/L}(\mathfrak{q}_i)$ follows from the following lemma.

Lemma 2.3.9 *If $L \cap \mathfrak{r}^{\tau_i} = \mathfrak{q}_i$, then $\mathrm{Frob}_{M/L}(\mathfrak{q}_i) = \prod_{j=0}^{m-1} \phi(g g_{ij})^{-1} g g_{ij}$.*

Proof. See Exercise 2. ■

The final group-theoretic ingredient

With this, Theorem 2.3.1 follows from the following fact.

Theorem 2.3.10 *Let G be a finite group and H its commutator subgroup. Then the transfer map $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is zero.*

Proof. See Exercise 5. ■

Remark 2.3.11 The fact that Theorem 2.3.10 is so general means that we can easily obtain some extensions of Theorem 2.3.1. For example, it was observed by Iyanaga that if L is the ray class field of K of some modulus $\mathfrak{m}$, and $\mathfrak{m}\mathfrak{o}_L$ is the extension of this modulus to L (that is, extend the finite part and take all places of L above the infinite places in $\mathfrak{m}$), then the induced map $\mathrm{Cl}^{\mathfrak{m}}(K) \to \mathrm{Cl}^{\mathfrak{m}}(L)$ again vanishes.

Additional remarks

Remark 2.3.12 One important qualification of Theorem 2.3.1 is that L need not itself have class number 1. In fact, it is an open problem to show that every number field K admits an extension which has class number 1.

One approach to constructing such an extension would be to consider the **class field tower** over K, in which $K_0 = K$ and for each positive integer i, K_i is the Hilbert class field of K_{i-1}. However, Golod and Shafarevich showed that in certain cases this sequence grows without bound; for example, this holds if K is an imaginary quadratic field in which at least six distinct primes of $\mathbb{Q}$ ramify. In particular, in such cases K admits an *infinite* unramified extension. (See [4] for more discussion.)

Remark 2.3.13 Let K be a number field. Let M be the $\mathfrak{o}_K$-submodule of $K[x]$ consisting of **integer-valued** polynomials, meaning those that map $\mathfrak{o}_K$ into itself. The field K is said to be a **Pólya field** if M admits a basis consisting of polynomials of pairwise distinct degrees; such a basis is called a **regular basis**. Any field with trivial class group is a Pólya field, but not conversely. The terminology is due to Zantema [58], who showed among other things that every cyclotomic field is a Pólya field.

Using Theorem 2.3.1, Leriche showed that the Hilbert class field of any number field is a Pólya field (see [35], Corollary 3.2). In particular, every number field can be embedded into a Pólya field via an abelian extension, whereas it is unknown whether every number field can be embedded into a field of class number one (and Remark 2.3.12 shows that solvable extensions are definitely not enough).

Exercises

1. Prove Theorem 2.3.7.

Hint. One approach to proving independence from choices is to change one g_i at a time. Also, notice that $\phi(gg_1), \ldots, \phi(gg_n)$ are a permutation of $g_1, \ldots, g_n$.

2. Prove Lemma 2.3.9.

Hint. See [37], Proposition IV.5.9.

3. Let $H \subseteq G$ be an inclusion of finite groups. Let G' and H' be the commutator subgroups of G and H. Let $\mathbb{Z}[G]$ be the group algebra of G, i.e., the (noncommutative) ring of formal linear combinations $\sum_{g \in G} n_g[g]$ with $n_g \in \mathbb{Z}$, multiplied by putting $[g][h] = [gh]$. Let $I_G \subset \mathbb{Z}[G]$ be the

ideal of sums $\sum n_g[g]$ with $\sum n_g = 0$ (called the **augmentation ideal**; see Section 3.3). Let

$$\delta : H/H' \to (I_H + I_G I_H)/I_G I_H$$

be the homomorphism taking the class of h to the class of $[h] - 1$. Prove that δ is an isomorphism.

Hint. Show that the elements

$$[g]([h] - 1) \qquad \text{for } g \in \{g_1, \dots, g_n\}, h \in H$$

form a basis of $I_H + I_G I_H$ as a $\mathbb{Z}$-module. For more clues, see [37], Lemma VI.7.7.

4. With notation as in Exercise 3, prove that the diagram in Figure 2.3.14 commutes, where S is given by $S(x) = x([g_1] + \cdots + [g_n])$.

$$\begin{array}{ccc} G/G' & \xrightarrow{V} & H/H' \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ I_G/I_G^2 & \xrightarrow{S} & (I_H + I_G I_H)/I_G I_H, \end{array}$$

Figure 2.3.14

5. Prove Theorem 2.3.10.

Hint. Quotient by the commutator subgroup of H to reduce to the case where H is abelian. Apply the classification of finite abelian groups to write G/H as a product of cyclic groups $\mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_m\mathbb{Z}$. Let f_i be an element of G lifting a generator of $\mathbb{Z}/e_i\mathbb{Z}$ and put $h_i = f_i^{-e_i} \in H$; then $0 = \delta(f_i^{e_i} h_i)$, which can be rewritten as $\delta(f_i)\mu_i$ for some $\mu_i \in \mathbb{Z}[G]$ congruent to e_i modulo I_G. Now check that

$$n\mu_1 \cdots \mu_m \equiv [g_1] + \cdots + [g_n] \pmod{I_H \mathbb{Z}[G]}.$$

For more details, see [37], Theorem VI.7.6.

2.4 Zeta functions and the Chebotaryov density theorem

Reference. [33], Chapter VIII for starters; see also [36], Chapter VI and [37], Chapter VII. For advanced reading, see Tate's thesis ([4], Chapter XV), but wait until we introduce the adèles (Section 6.1).

The Dedekind zeta function of a number field

Although this is supposed to be a course on algebraic number theory, the following analytic discussion is so fundamental that we must at least allude to it here.

Definition 2.4.1 Let K be a number field. The **Dedekind zeta function** $\zeta_K(s)$ is a function on the complex plane given, for $\mathrm{Re}(s) > 1$, by the absolutely convergent product and sum

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \mathrm{Norm}(\mathfrak{p})^{-s})^{-1} = \zeta_K(s) = \sum_{\mathfrak{a}} \mathrm{Norm}(\mathfrak{a})^{-s}$$

where $\mathfrak{p}$ runs over the nonzero prime ideals of $\mathfrak{o}_K$ and $\mathfrak{a}$ runs over the nonzero ideals of $\mathfrak{o}_K$.

For exmaple, if $K = \mathbb{Q}$, then ζ_K equals the Riemann zeta function. ◊

A fundamental fact about the zeta function is the following.

Theorem 2.4.2 *The function $\zeta_K(s)$ extends to a meromorphic function on $\mathbb{C}$ whose only pole is a simple pole at $s = 1$.*

Proof. See [37], Corollary VII.5.11. ■

Remark 2.4.3 In Theorem 2.4.2, the residue of the pole at $s = 1$ is computed by the **analytic class number formula**; it is the product of the class number, the unit regulator, and another quantity that depends on the discriminant and signature of K.

There is also a functional equation relating the values of ζ_K at s and $1 - s$, and an extended Riemann hypothesis: aside from "trivial" zeros along the negative real axis, the zeroes of ζ_K all have real part $1/2$.

L-functions of abelian characters

Definition 2.4.4 More generally, let $\mathfrak{m}$ be a formal product of places of K, and let $\chi_{\mathfrak{m}} : \mathrm{Cl}^{\mathfrak{m}}(K) \to \mathbb{C}^*$ be a character of the ray class group of conductor $\mathfrak{m}$. Extend $\chi_{\mathfrak{m}}$ to a function on all ideals of K by declaring its value to be 0 on ideals not coprime to $\mathfrak{m}$. Then we define the **L-function**

$$L(s, \chi_{\mathfrak{m}}) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} (1 - \chi(\mathfrak{p}) \operatorname{Norm}(\mathfrak{p})^{-s})^{-1} = \sum_{(\mathfrak{a}, \mathfrak{m}) = 1} \chi(\mathfrak{a}) \operatorname{Norm}(\mathfrak{a})^{-s};$$

again the product converges absolutely for $\operatorname{Re}(s) > 1$. ◊

Theorem 2.4.5 *If $\chi_{\mathfrak{m}}$ is not trivial, then $L(s, \chi_{\mathfrak{m}})$ extends to an analytic function on $\mathbb{C}$.*

Proof. See [37], Theorem VII.2.8 (or Theorem VII.8.5). ■

Remark 2.4.6 By contrast with Theorem 2.4.5, if $\chi_{\mathfrak{m}}$ is trivial, then $L(s, \chi_{\mathfrak{m}})$ is just the Dedekind zeta function with the Euler factors for primes dividing $\mathfrak{m}$ removed, so it still has a pole at $s = 1$ by Theorem 2.4.2.

Nonvanishing of L-functions and consequences

One more basic fact is the following.

Theorem 2.4.7 *If $\chi_{\mathfrak{m}}$ is not the trivial character, then $L(1, \chi_{\mathfrak{m}}) \neq 0$.*

Proof. See [37], Theorem VII.2.9. ■

For $K = \mathbb{Q}$, Theorem 2.4.7 is already a nontrivial but important result: it implies Dirichlet's famous theorem that there are infinitely many primes in arithmetic progression, as follows.

Definition 2.4.8 A set of primes S in a number field K has **Dirichlet density** d if

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \operatorname{Norm}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} = d.$$

This in particular presumes the existence of the limit; otherwise, we may still define the **lower Dirichlet density** and **upper Dirichlet density** using the limits inferior and superior. ◊

Remark 2.4.9 Theorem 2.4.7 implies that the Dirichlet density of the set of primes congruent to a modulo m is $1/\phi(m)$ if a is coprime to m (and 0 otherwise). The key point is that for any nontrivial $\chi_{\mathfrak{m}}$, $\sum_{\mathfrak{p}} \chi(\mathfrak{p}) \operatorname{Norm}(\mathfrak{p})^{-s}$ remains bounded as $s \to \infty$.

The fact also implies that for any number field K and any formal product of places $\mathfrak{m}$, there are infinitely many primes in each class of the ray class group of conductor $\mathfrak{m}$, the set of such primes having Dirichlet density $1/\# \operatorname{Cl}^{\mathfrak{m}}(K)$. (See Exercise 3.)

The Chebotaryov density theorem

Finally, we point out a result of class field theory that also applies to nonabelian extensions.

Definition 2.4.10 Recall that if L/K is any Galois extension of number fields with Galois group G, $\mathfrak{p}$ is a prime of K which does not ramify in L, and $\mathfrak{q}$ is a prime above $\mathfrak{p}$, then there is a well-defined **Frobenius element** to $\mathfrak{q}$: it's the element g of the decomposition group $G_{\mathfrak{q}}$ such that $x^g \equiv x^{\#(\mathfrak{o}_K/\mathfrak{p})} \pmod{\mathfrak{q}}$. Keep in mind that as a function of $\mathfrak{p}$, this Frobenius is only well-defined up to conjugation in G. (If $\mathfrak{p}$ ramifies in L, then a further ambiguity occurs: the Frobenius element associated to $\mathfrak{q}$ is only well-defined in the quotient of $G_{\mathfrak{q}}$ by the inertia group $I_{\mathfrak{q}}$.) ◊

Theorem 2.4.11 Chebotaryov density theorem. *Let L/K be a Galois extension of number fields with Galois group G. Then for any $g \in G$, there exist infinitely many primes $\mathfrak{p}$ of K such that there is a prime $\mathfrak{q}$ of L above $\mathfrak{p}$ with Frobenius g. In fact, the Dirichlet density of such primes $\mathfrak{p}$ is the order of the conjugacy class of G divided by $\#G$.*

Proof. This follows from everything we have said so far, plus Artin reciprocity, in case L/K is abelian. In the general case, let f be the order of g, and let K' be the fixed field of g; then we know that the set of primes of K' with Frobenius $g \in \operatorname{Gal}(L/K') \subset G$ has Dirichlet density $1/f$. The same is true if we restrict to primes of absolute degree 1 (see Exercise 2).
Let Z be the centralizer of g in G; that is, $Z = \{z \in G : zg = gz\}$. Then for each prime of K of absolute degree 1) with Frobenius in the conjugacy class of g, there are $\#Z/f$ primes of K' above it (also of absolute degree 1) with Frobenius g. (Say $\mathfrak{p}$ is such a prime and $\mathfrak{q}$ is a prime of L above $\mathfrak{p}$ with Frobenius g. Then for $h \in G$, the Frobenius of $\mathfrak{q}^h$ is hgh^{-1}, so the number of primes $\mathfrak{q}$ with Frobenius g is $\#Z$. But each prime of L' below one of these is actually below f of them.) Thus the density of primes of K with Frobenius in the conjugacy class of g is $(1/f)(1/(\#Z/f)) = 1/\#Z$. To conclude, note that the order of the conjugacy class of G is $\#G/\#Z$. ■

We state the following here as a corollary of Theorem 2.4.11; however, we will eventually prove it *before* proving Artin reciprocity (see Corollary 7.1.16).

Corollary 2.4.12 *Let L/K be a nontrivial extension of number fields. Then there exist infinitely many primes of K which do not split completely in L.*

Proof. Let M/K be the Galois closure of L/K, and set $G = \operatorname{Gal}(M/K), H = \operatorname{Gal}(M/L)$. By hypothesis, G is not the trivial group and the conjugates of H in G have trivial intersection.
Let $\mathfrak{p}$ be any prime of K which does not ramify in M and let $\mathfrak{q}$ be a prime of M above K. Then $\mathfrak{p}$ splits completely in M if and only if the Frobenius element of $\mathfrak{q}$ is trivial. Moreover, if $\mathfrak{p}$ splits completely in L, then g lies in every conjugate of H and hence must be trivial, so $\mathfrak{p}$ also splits completely in M. (The converse

is also true.)
Since $G \neq H$, we can choose an element $g \in G \setminus H$. By Theorem 2.4.11, there exist infinitely many primes $\mathfrak{p}$ of K for which there is a prime $\mathfrak{q}$ of L above $\mathfrak{p}$ with Frobenius g. By the previous discussion, any such $\mathfrak{p}$ does not split completely in K. ■

Remark 2.4.13 Theorem 2.4.11 is a special case of a much more general equidistribution conjecture including, among other things, the **Sato-Tate conjecture** on the distribution of Frobenius traces of elliptic curves. See [49] for an introduction to this circle of ideas.

Remark 2.4.14 With somewhat more work, all of the previous density assertions remain true (and are indeed strictly stronger than before) if Dirichlet density is replaced by natural density. The **natural density** of a set S of prime ideals of a number field K is the limit (if it exists)

$$\lim_{X \to \infty} \frac{\#\{\mathfrak{p} : \mathfrak{p} \in S, \mathrm{Norm}(\mathfrak{p}) \leq X\}}{\#\{\mathfrak{p} : \mathrm{Norm}(\mathfrak{p}) \leq X\}}$$

where in both sets $\mathfrak{p}$ runs over all prime ideals of K. (Again, if the limit does not exist, we may still define the **lower natural density** and **upper natural density** using the limits inferior and superior.)

As with the prime number theorem, one can obtain effective power-saving error estimates conditional on the Generalized Riemann Hypothesis for appropriate Artin L-functions. See [31].

Remark 2.4.15 For fun, we mention a lesser-known result of Chebotaryov here: the character table of a finite cyclic group, viewed as a square matrix, has the property that every minor is nonzero.

By contrast, for a group which is abelian but not cyclic there exists a 2×2 submatrix with all entries equal to 1, whereas for a nonabelian group any nonabelian character takes the value 0 somewhere (a result of Burnside; see [23], Theorem 3.15).

Exercises

1. Show that the Dirichlet density of the set of all primes of a number field is 1.

2. Show that in any number field, the Dirichlet density of the set of primes $\mathfrak{p}$ of absolute degree greater than 1 is zero.

3. Let $\mathfrak{m}$ be a formal product of places of the number field K. Using Theorem 2.4.2, Theorem 2.4.5, and Theorem 2.4.7, prove that the set of primes of K lying in any specified class of the generalized ideal class group of conductor $\mathfrak{m}$ has Dirichlet density $1/\# \mathrm{Cl}^{\mathfrak{m}}(K)$.

Hint. Combine the quantities $\sum_{\mathfrak{p}} \chi(\mathfrak{p}) \mathrm{Norm}(\mathfrak{p})^{-s}$ to cancel out all but one class.

4. Let L/K be an extension of number fields. Suppose that for every prime $\mathfrak{p}$ of K which does not ramify in L, all of the primes of L above $\mathfrak{p}$ have isomorphic residue fields. Using Theorem 2.4.11, prove that L/K is Galois.

Hint. Let M be the Galois closure of L/K. Put $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. For $\mathfrak{q}$ a prime of M with decomposition group $G_{\mathfrak{q}}$ lying above the prime $\mathfrak{p}$ of K, relate the orders of the residue fields of the primes of L to the intersections of $G_{\mathfrak{q}}$ with the conjugates of H in G (see Remark 1.1.6). Use the fact that these conjugates have trivial intersection to deduce that $G_{\mathfrak{q}}$ must be trivial, and invoke Theorem 2.4.11 to conclude.

5. Let L/K be an abelian extension of number fields. Using Corollary 2.4.12, show that the homomorphism $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective.

6. Let K be a number field and let $\mathfrak{m}$ be a formal product of places of K. Use Corollary 2.4.12 to show that the ray class field of $\mathfrak{m}$ is unique.

Hint. Show that if L_1, L_2 are both ray class fields of $\mathfrak{m}$, then all but finitely many primes of L_1 split completely in the compositum L_1L_2 (namely, those which do not ramify in the compositum).

7. Here is an example to illustrate the difference between Dirichlet density and natural density, albeit not for primes. Let S be the set of positive integers whose decimal expansion begins with 1.

(a) Prove that S does not have a natural density, in the sense that

$$\lim_{X\to\infty} \frac{1}{X}\#(S \cap \{1, \dots, X\})$$

does not exist.

(b) On the other hand, prove that S has a Dirichlet density in the sense that

$$\lim_{s\to 1^+} \frac{\sum_{n\in S} n^{-s}}{\sum_{n=1}^{\infty} n^{-s}}$$

exists, and compute this value.

Hint. Estimate $\sum_{n=a}^{b} n^{-s}$ using upper and lower Riemann sums for the integral of $x^{-s}\,dx$.

Chapter 3

Cohomology of groups

In this chapter, we introduce the cohomology of finite groups, which plays a key role in the proofs of class field theory. We also discuss homology and Tate groups, and touch briefly on profinite groups.

We begin with the construction of group cohomology in the language of derived functors. Readers not familiar with this material may find it easiest to treat Section 3.1 as a "black box" on first reading.

3.1 Cohomology of finite groups I: abstract nonsense

Reference. [36], II.1. See [48] for a much more general presentation. (We will generalize ourselves from finite to profinite groups a bit later on; see Section 3.5).

For the broader context of homological algebra, the original reference is [14]. See [36], Appendix II.A for a summary.

Caveat. This material may seem a bit dry. If so, don't worry; only a small part of the theory will be relevant for class field theory. However, it doesn't make sense to learn that small part without knowing what it is a part of!

The euphemism "abstract nonsense" in specific reference to category theory and/or homological algebra has been attributed to Norman Steenrod. It was used in a tongue-in-cheek manner without intending a negative connotation, although such a connotation has been imputed by later authors (a notable example being [32]).

Caveat. The Galois cohomology groups used in [37] are not the ones we define here. Rather, they are the Tate groups to be introduced in Section 3.3.

Caveat. Some authors (like Milne, and Neukirch for the most part) put group actions on the left and some (like Neukirch in chapter IV, and myself here) put them on the right. Of course, the theory is the same either way!

G-modules and their invariants

Definition 3.1.1 Let G be a finite group. A **(right) G-module** is an abelian group A equipped with a right G-action. I'll write this action using superscripts, i.e., the image of the action of g on m is m^g. Alternatively, A can be viewed as a right module for the group algebra $\mathbb{Z}[G]$.

A **homomorphism** of G-modules $\phi : M \to N$ is a homomorphism of abelian groups that is compatible with the G-actions, i.e., $\phi(m^g) = \phi(m)^g$. $\Diamond$

Remark 3.1.2 For those keeping score, the category of G-modules is an example of an **abelian category**; that is, it is an **additive category** (meaning that the Hom sets have abelian group structures for which composition distributes over addition) with some extra properties related to kernels and cokernels of morphisms. The following discussion is specialized from the general theory of derived functors on abelian categories.

Definition 3.1.3 Given a G-module M, let M^G be the abelian group of G-invariant elements of M:

$$M^G = \{m \in M : m^g = m \forall g \in G\}.$$

The functor $M \to M^G$ from G-modules to abelian groups is **left exact** but not **right exact**. That is, say we start with an **exact sequence**

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

of G-modules; that is, the kernel of each map is equal to the image of the previous map. Then

$$0 \to (M')^G \to M^G \to (M'')^G$$

is again an exact sequence, but this need not remain true if we add 0 at the end; that is, the map $M^G \to (M'')^G$ may not be surjective.

More generally, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then $0 \to (M')^G \to M^G \to (M'')^G$ is exact, $\Diamond$

Example 3.1.4 Take the sequence $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ of G-modules for $G = \mathbb{Z}/p\mathbb{Z}$, which acts on the middle factor by $a^g = a(1 + pg)$. Then $M^G \to (M'')^G$ is the zero map but $(M'')^G$ is nonzero.) $\square$

Injective objects and resolutions

The topic of **homological algebra** provides a systematic way to quantify the difference between an exact functor and a left exact (or a right exact) functor. This rests on the following key concept.

Definition 3.1.5 A G-module M is **injective** if for every inclusion $A \subset B$ of G-modules and every G-module homomorphism $\phi : A \to M$, there is a homomorphism $\psi : B \to M$ that extends ϕ. $\Diamond$

Lemma 3.1.6 *Every G-module can be embedded into some injective G-module. In other words, the abelian category of G-modules **has enough injectives**.*

Proof. See Exercise 3. $\blacksquare$

Definition 3.1.7 An **injective resolution** of a G-module M is a sequence

$$I^0 \stackrel{d^0}{\to} I^1 \stackrel{d^1}{\to} \dots$$

in which the objects $I^0, I^1, \dots$ are injective G-modules and the **augmented sequence**

$$0 \to M \to I^0 \stackrel{d^0}{\to} I^1 \stackrel{d^1}{\to} \dots$$

is exact.

From Lemma 3.1.6, it follows that injective resolutions always exist. To wit, first embed M into an injective G-module I^0, then embed I^0/M into an

injective G-module I^1, and so on. ◊

Definition 3.1.8 Starting with an injective resolution of M, apply the functor of G-invariants; the result

$$0 \to (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} \dots$$

is still a **complex** in the sense that any two consecutive maps compose to zero, but it is not necessarily exact. (That is, we still have inclusions $\mathrm{im}(d^i) \subseteq \ker(d^{i+1})$, but these need not be equalities.) We turn this failure into success by defining the i-th **cohomology group** as the quotient

$$H^i(G, M) = \ker(d^i)/\,\mathrm{im}(d^{i-1}),$$

with the temporary proviso that this appears to depend not just on M but also on the injective resolution. By convention, we let d^{-1} be the map $0 \to I_0^G$, so $H^0(G, M) = M^G$.

Given a homomorphism $f : M \to N$ and another injective resolution $0 \to N \to J_0 \to J_1 \to \cdots$, Lemma 3.1.6 again implies the existence of a commutative diagram as in Figure 3.1.9 with exact rows. When we apply the functor of G-invariants, we again get a commutative diagram, but the rows are only complexes rather than exact sequences. However, the vertical arrows in the resulting diagram induce maps $H^i(f) : H^i(G, M) \to H^i(G, N)$.

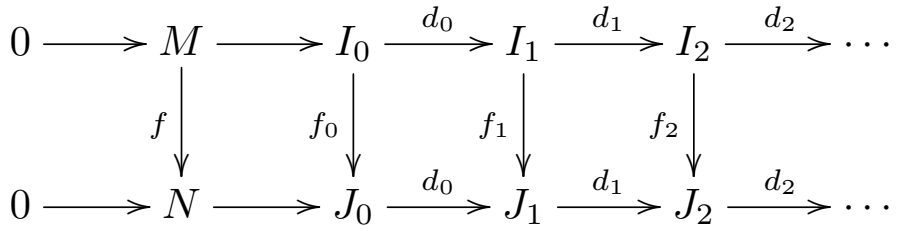

Figure 3.1.9

◊

Right derived functors

Continuing the thread, we observe the following.

Lemma 3.1.10 *For a fixed choice of the injective resolutions of M and N in Definition 3.1.8, the map $H^i(f)$ does not depend on the choice of the f_i.*

Proof. This proof is a standard example of "abstract nonsense". It suffices to check that if $f = 0$, then the $H^i(f)$ are all zero regardless of what the f_i are. In that case, it turns out one can construct maps $g_i : I_{i+1} \to J_i$ (and by convention $g_{-1} = 0$) such that $f_i = g_i \circ d_i + d_{i-1} \circ g_{i-1}$, as illustrated in Figure 3.1.11. (Beware that this figure is not a commutative diagram!) Details left as an exercise (see Exercise 4). ■

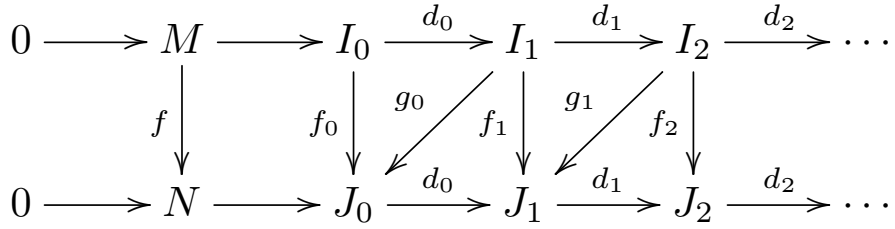

Figure 3.1.11

Remark 3.1.12 The diagonal arrows depicted in Figure 3.1.11 with the property described in the proof of Lemma 3.1.10 (namely, that $f_i = g_i \circ d_i + d_{i-1} \circ g_{i-1}$), are collectively called a **chain homotopy** for the map f.

Definition 3.1.13 We can now close the books on Definition 3.1.8 as follows. If $M = N$ and f is the identity, we get a canonical map between $H^i(G, M)$ and $H^i(G, N)$ for each i. That is, the groups $H^i(G, M)$ are well-defined independent of the choice of the injective resolution. Likewise, the map $H^i(f)$ is also independent of the choice of resolutions, so each H^i defines a functor from G-modules to abelian groups. These are called the **right derived functors** of the functor of G-invariants. ◊

Lemma 3.1.14 *Given a short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules, there is a canonical long exact sequence of abelian groups*

$$0 \to H^0(G, M') \to \cdots \to H^i(G, M'') \xrightarrow{\delta_i} H^{i+1}(G, M') \to H^{i+1}(G, M) \to H^{i+1}(G, M'') \to \cdots$$

*in which the δ_i are certain **connecting homomorphisms**.*

I will not subject you to the proof of this, but rather mention the key step in its proof.

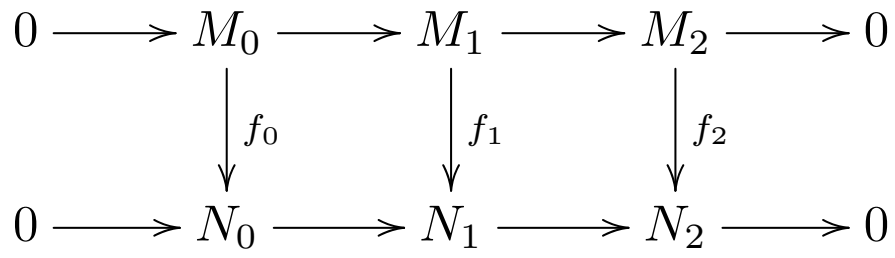

Figure 3.1.15

Lemma 3.1.16 Snake Lemma. *Given a commuting diagram as in Figure 3.1.15 with exact rows, there is a canonical map $\delta : \ker(f_2) \to \operatorname{coker}(f_0)$ such that the sequence*

$$0 \to \ker(f_0) \to \ker(f_1) \to \ker(f_2) \xrightarrow{\delta} \operatorname{coker}(f_0) \to \operatorname{coker}(f_1) \to \operatorname{coker}(f_2) \to 0$$

is exact.

Proof. The key point is to define the map δ, as the rest amounts to "diagram chasing". To wit, given $x \in \ker(f_2) \subseteq M_2$, lift x to M_1, push it into N_1 by f_1, then check that the image has a preimage in N_0. Verification that this is well-defined (and a homomorphism), and that everything is exact, is left to the reader. ■

Remark 3.1.17 The snake lemma is depicted in the movie *It's My Turn*[1], but not in any more detail than we have given here.

Remark 3.1.18 In modern algebra, it is common to define objects (e.g., tensor products of modules) in terms of "universal properties" that they satisfy. This can be done for derived functors via the theory of δ**-functors**, as introduced in [14].

Additional comments

One important consequence of the long exact sequence is that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of G-modules and $H^1(G, M') = 0$, then $0 \to (M')^G \to M^G \to (M'')^G \to 0$ is also exact.

More abstract nonsense:

- If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of G-modules and $H^i(G, M) = 0$ for all $i > 0$, then the connecting homomorphisms in the long exact sequence induce isomorphisms $H^i(G, M'') \to H^{i+1}(G, M')$ for all $i > 0$ (and a surjection for $i = 0$). This sometimes allows one to prove general facts by proving them first for H^0, where they have a direct interpretation, then "dimension shifting"; however, getting from H^0 to H^1 typically requires some extra attention.
- If M is an injective G-module, then $H^i(G, M) = 0$ for all $i > 0$. (Use $0 \to M \to M \to 0 \to \cdots$ as an injective resolution.) This fact has a sort of converse: see next bullet.
- We say M is **acyclic** if $H^i(G, M) = 0$ for all $i > 0$; so in particular, injective G-modules are acyclic. It turns out that we can replace the injective resolution in the definition by an acyclic resolution for the purposes of doing a computation; see Exercise 5.

Of course, the abstract nature of the proofs so far gives us almost no insight into what the objects are that we've just constructed. We'll remedy that next time by giving more concrete descriptions that one can actually compute with.

Exercises

1. Let G be the one-element group. Show that a G-module (i.e., abelian group) is injective if and only if it is divisible, i.e., the map $x \mapsto nx$ is surjective for any nonzero integer n.

Hint. You'll need Zorn's lemma or equivalent in one direction.

2. Let A be an abelian group, regarded as a G-module for G the trivial group. Prove that A can be embedded in an injective G-module.

3. Prove Lemma 3.1.6.

Hint. For M a G-module, the previous exercises show that the underlying abelian group of M embeds into a divisible group N. Now map M into $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], N)$ and check that the latter is an injective G-module.

4. Prove Lemma 3.1.10 following the sketch given.

Hint. Construct g_i given f_{i-1} and g_{i-1}, using that the J's are injective G-modules.

[1] `www.youtube.com/watch?v=etbcKWEKnvg`

5. Prove that if $0 \to M \to M^0 \to M^1 \to \cdots$ is an exact sequence of G-modules and each M_i is acyclic, then the cohomology groups of the complex $0 \to M^{0G} \to M^{1G} \to \cdots$ coincide with $H^i(G, M)$.

Hint. Construct the canonical long exact sequence from the exact sequence

$$0 \to M \to M^0 \to M^0/M \to 0,$$

then do dimension shifting using the fact that

$$0 \to M^0/M \to M^1 \to M^2 \to \cdots$$

is again exact. Don't forget to be careful about H^1!)

3.2 Cohomology of finite groups II: concrete nonsense

Reference. [36], II.1.

In the previous chapter, we associated to a finite group G and a (right) G-module M a sequence of abelian groups $H^i(G, M)$, called the **cohomology groups** of M. (They're also called the **Galois cohomology** groups because in number theory, G will invariably be the Galois group of some extension of number fields, and A will be some object manufactured from this extension.) What we didn't do is make the construction at all usable in practice! This time we will remedy this.

Induced G-modules

In light of Exercise 5, to compute cohomology we are going to need an ample supply of acyclic G-modules. We will get these using a process known as **induction**.

Remark 3.2.1 By way of motivation, we note first that if G is the trivial group, *every* G-module is acyclic: if $0 \to M \to I^0 \to I^1 \cdots$ is an injective resolution, taking G-invariants has no effect, so $0 \to I^0 \to I^1 \to \cdots$ is still exact except at I^0 (where we omitted M).

Definition 3.2.2 If H is a subgroup of G and M is an H-module, we define the **induction** of M from H to G to be $\mathrm{Ind}_H^G M = M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. We may also identify $\mathrm{Ind}_H^G M$ with the set of functions $\phi\colon G \to M$ such that $\phi(gh) = \phi(g)^h$ for $h \in H$, with the G-action on the latter being given by $\phi^g(g') = \phi(gg')$: namely, the element $m \otimes [g] \in M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$ corresponds to the function $\phi_{m,g}$ taking g' to $m^{gg'}$ if $gg' \in H$ and to 0 otherwise. ◊

Lemma 3.2.3 Shapiro's lemma. *If H is a subgroup of G and N is an H-module, then there is a canonical isomorphism $H^i(G, \mathrm{Ind}_H^G N) \to H^i(H, N)$. In particular, N is an acyclic H-module if and only if $\mathrm{Ind}_H^G(N)$ is an acyclic G-module.*

Proof. The key points are:

1. $(\mathrm{Ind}_H^G N)^G = N^H$, so there is an isomorphism for $i = 0$ (this is most visible from the description using functions);
2. the functor Ind_H^G from H-modules to G-modules is exact (that is, $\mathbb{Z}[G]$ is flat over $\mathbb{Z}[H]$; in fact it is free over $\mathbb{Z}[H]$);
3. if I is an injective H-module, then $\mathrm{Ind}_H^G(I)$ is an injective G-module. This

follows from the existence of a canonical isomorphism $\mathrm{Hom}_G(M, \mathrm{Ind}_H^G I) = \mathrm{Hom}_H(M, I)$, for which see Proposition 3.2.6 below.

Now take an injective resolution of N, apply Ind_H^G to it, and the result is an injective resolution of $\mathrm{Ind}_H^G N$. ■

Definition 3.2.4 We say M is an **induced** G-module if it has the form $\mathrm{Ind}_1^G N$ for some abelian group N, i.e., it can be written as $N \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. (The subscript 1 stands for the trivial group, since G-modules for $G = 1$ are just abelian groups.) ◊

Corollary 3.2.5 *If M is an induced G-module, then M is acyclic.*

Proof. Apply Lemma 3.2.3 with $H = \{1\}$. ■

To complete the previous argument, we need an important property of induced modules. This is closely related to the **Frobenius reciprocity law** in the theory of representations of finite groups.

Proposition 3.2.6 *Let H be a subgroup of G, let M be a G-module, and let N be an H-module. Then there are natural isomorphisms*

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

Proof. To begin with, note that if we take $N = M$ (or more precisely, N is a copy of M with only the action of H retained), then the identity map between M and N is supposed to correspond both to a homomorphism $\mathrm{Ind}_H^G M \to M$ and to a homomorphism $M \to \mathrm{Ind}_H^G M$. Let us write these maps down first: the map $\mathrm{Ind}_H^G M \to M$ is

$$\sum_{g \in G} m_g \otimes [g] \mapsto \sum_{g \in G} (m_g)^g,$$

while the map $M \to \mathrm{Ind}_H^G M$ is

$$m \mapsto \sum_i m^{g_i} \otimes [g_i^{-1}]$$

where g_i runs over a set of left coset representatives of H in G. This second map doesn't depend on the choice of the representatives; consequently, for $g \in G$, we can use the coset representatives gg_i instead to see that

$$m^g \mapsto \sum_i m^{gg_i} \otimes [g_i^{-1}] = \left(\sum_i m^{gg_i} \otimes [(gg_i)^{-1}] \right) [g].$$

This means that we do in fact get a map compatible with the G-actions. (Note that the composition of these two maps is not the identity! For more on this point, see the discussion of extended functoriality in Section 3.3.)
Now let N be general. Given a homomorphism $M \to N$ of H-modules, we get a corresponding homomorphism $\mathrm{Ind}_H^G M \to \mathrm{Ind}_H^G N$ of G-modules, which we can then compose with the above map $M \to \mathrm{Ind}_H^G M$ to get a homomorphism $M \to \mathrm{Ind}_H^G N$ of G-modules. We thus get a map

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

to get the map in the other direction, start with a homomorphism $M \to \mathrm{Ind}_H^G N$, identify the target with functions $\phi\colon G \to N$, then compose with the map $\mathrm{Ind}_H^G N \to N$ taking ϕ to $\phi(e)$.

In the other direction, given a homomorphism $N \to M$ of H-modules, we get a corresponding homomorphism $\mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G M$ of G-modules, which we can then compose with the above map $\mathrm{Ind}_H^G M \to M$ to get a homomorphism $\mathrm{Ind}_H^G N \to M$ of G-modules. We thus get a map

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

to get the map in the other direction, start with a homomorphism $\mathrm{Ind}_H^G N \to M$ of G-modules and evaluate it on $n \otimes [e]$ to get a homomorphism $N \to M$ of H-modules. ■

Remark 3.2.7 Proposition 3.2.6 asserts that the restriction functor from G-modules to H-modules and the induction functor from H-modules to G-modules form a pair of **adjoint functors** in both directions. This is rather unusual; it is far more common to have such a relationship in only one direction. Indeed, without assuming that G is finite (or at least that $[G : H] < \infty$), then the proof of Proposition 3.2.6 only shows that $\mathrm{Hom}_G(\mathrm{Ind}_H^G N, M) \cong \mathrm{Hom}_H(N, M)$.

Remark 3.2.8 The point of all of this is that it is much easier to embed M into an acyclic G-module than into an injective G-module: use the map $M \to \mathrm{Ind}_1^G M$ constructed in Proposition 3.2.6! An immediate consequence is that if M is finite, it can be embedded into a finite acyclic G-module, and thus $H^i(G, M)$ is finite for all i.

However, contrary to what you might expect, for fixed M, even if M is finite, the groups $H^i(G, M)$ do not necessarily become zero for i large. We'll see explicit examples in the next section.

Another consequence is the following result. (The case $i = 1$ was stated previously in Exercise 2.)

Theorem 3.2.9 *Let L/K be a finite Galois extension of fields. Then*

$$H^i(\mathrm{Gal}(L/K), L) = 0 \text{ for all } i > 0.$$

Proof. Put $G = \mathrm{Gal}(L/K)$. The normal basis theorem (see Lang, *Algebra* or Milne, Lemma II.1.24) states that there exists $\alpha \in L$ whose conjugates form a basis of L as a K-vector space. This implies that $L \cong \mathrm{Ind}_1^G K$, so L is an induced G-module and so is acyclic. ■

Group cohomology via homogeneous cochains

Now let's see an explicit way to compute group cohomology.

Definition 3.2.10 Given a group G and a G-module M, define the G-module N^i for $i \geq 0$ as the set of functions $\phi\colon G^{i+1} \to M$, with the G-action

$$(\phi^g)(g_0, \ldots, g_i) = \phi(g_0 g^{-1}, \ldots, g_i g^{-1})^g.$$

Notice that this module is induced: we have $N^i = \mathrm{Ind}_1^G N_0^i$ where N_0^i is the subset of N^i consisting of functions for which $\phi(g_0, \ldots, g_i) = 0$ when $g_0 \neq e$. ◊

Definition 3.2.11 Define the map $d^i\colon N^i \to N^{i+1}$ by

$$(d^i\phi)(g_0, \ldots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j \phi(g_0, \ldots, \widehat{g_j}, \ldots, g_{i+1}),$$

where the hat over g_j means you omit it from the list. ◊

Lemma 3.2.12 *With notation as in Definition 3.2.10 and Definition 3.2.11, the sequence*

$$0 \to M \to N^0 \to N^1 \to \dots$$

is exact.

Proof. Left to the reader. ∎

Definition 3.2.13 By Corollary 3.2.5 and Lemma 3.2.12, the sequence

$$0 \to M \to N^0 \to N^1 \to \dots$$

is an acyclic resolution of the G-module M. Hence the cohomology of the complex

$$0 \to N^{0G} \to N^{1G} \to \cdots$$

coincides with the cohomology groups $H^i(G, M)$. And now we have something we can actually compute!

Some terminology: the elements of N^{1G} are called **(homogeneous) i-cochains**. The cocycles in the kernel of d^i are called **(homogeneous) i-cocycles**. The ones in the image of d^{i-1} are called **i-coboundaries**. (This terminology makes little sense here; it is transferred from the classical theory of homology of topological spaces, where it has some geometric significance.) ◊

Fun with H^1

Remark 3.2.14 Using the resolution by homogeneous cochains, we can give a very simple description of $H^1(G, M)$. Namely, a 1-cocycle $\phi\colon G^2 \to M$ is determined by $\rho(g) = \phi(e, g)$, which by G-invariance satisfies the relation

$$\begin{aligned} 0 &= (d^1\phi)(e, h, gh) \\ &= \phi(h, gh) - \phi(e, gh) + \phi(e, h) \\ &= (\phi^h)(h, gh) - \rho(gh) + \rho(h) \\ &= \phi(e, g)^h - \rho(gh) + \rho(h) \\ &= \rho(g)^h + \rho(h) - \rho(gh). \end{aligned}$$

It is the image of a 0-cochain $\psi\colon G \to M$ if and only if

$$\rho(g) = \phi(e, g) = \psi(g) - \psi(e) = \psi(e)^g - \psi(e).$$

That is, $H^1(G, M)$ consists of crossed homomorphisms modulo principal crossed homomorphisms, consistent with the definition we gave in Section 1.2.

Definition 3.2.15 We may also interpret $H^1(G, M)$ as the set of isomorphism classes of **principal homogeneous spaces** of M. Such objects are sets A with both a G-action and an M-action, subject to the following restrictions:

1. for any $a \in A$, the map $M \to A$ given by $m \mapsto m(a)$ is a bijection;
2. for $a \in A$, $g \in G$ and $m \in M$, $m(a)^g = m^g(a^g)$ (i.e., the G-action and M-action commute).

To define the associated class in $H^1(G, M)$, pick any $a \in A$, take the map $\rho\colon G \to M$ characterized by $\rho(g)(a) = a^g$, and let ϕ be the 1-cocycle with $\phi(e, g) = \rho(g)$. The verification that this defines a bijection is left to the reader. ◊

Example 3.2.16 The identity in $H^1(G, M)$ corresponds to the trivial principal homogeneous space $A = M$, on which G acts as it does on M while M acts by translation: $m(a) = m + a$. □

Remark 3.2.17 This interpretation of H^1 appears prominently in the theory of elliptic curves.

1. For example, if L is a finite extension of K and E is an elliptic curve over K, then $H^1(\mathrm{Gal}(L/K), E(\bar{K}))$ is the set of K-isomorphism classes of curves whose Jacobians are K-isomorphic to E and which have an L-rational point but not necessarily a K-rational point. For any such curve C, we can define the translation map $E \times_K C \to C$ by first defining it over L, by picking some L-rational point to use as the origin, then observing that the result is independent of the chosen point.

2. For another example, $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(E_{\bar{K}}))$ parametrizes twists of E, elliptic curves defined over K which are L-isomorphic to E. (E.g., $y^2 = x^3 + x + 1$ versus $2y^2 = x^3 + x + 1$, with $L = \mathbb{Q}(\sqrt{2})$.) In this example the translation action is not so obvious, and its existence depends on the fact that $\mathrm{Aut}(E_{\bar{K}})$ is abelian. (One can interpret twists similarly for more general curves, for which the automorphism group need not be abelian, but then H^1 won't make sense the way we have defined it; it will only have the structure of a pointed set.)

See [51], especially Chapter X, for all this and more fun with H^1, including the infamous **Selmer group** and **Tate–Shafarevich group**.

Fun with H^2

Remark 3.2.18 We can also give an explicit interpretation of $H^2(G, M)$ (see [36], example II.1.18(b)). It classifies short exact sequences

$$1 \to M \to E \to G \to 1$$

of (not necessarily abelian) groups on which G has a fixed action on M. The action is given as follows: given $g \in G$ and $m \in M$, choose $h \in E$ lifting G; then $h^{-1}mh$ maps to the identity in G, so comes from M, and we call it m^g since it depends only on g.

The correspondence is constructed as follows. Given an exact sequence as above, choose a map $s\colon G \to E$ (which need not be a homomorphism) such that $s(g)$ maps to g under the map $E \to G$. Then the map $\phi\colon G^3 \to M$ given by

$$\phi(a, b, c) = s(a)^{-1}s(ba^{-1})^{-1}s(cb^{-1})^{-1}s(ca^{-1})s(a)$$

is a homogeneous 2-cocycle, and any two choices of s give maps that differ by a 2-coboundary.

What "classifies" means here is that two sequences give the same element of $H^2(G, M)$ if and only if one can find an arrow $E \to E'$ making the diagram in Figure 3.2.19 commute.

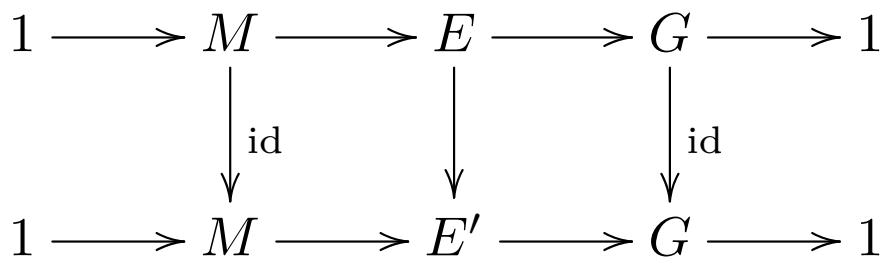

Figure 3.2.19

Note that two sequences may not be isomorphic under this definition even if E and E' are abstractly isomorphic as groups. For example, if $G = M = \mathbb{Z}/p\mathbb{Z}$ and the action is trivial, then $H^2(G, M) = \mathbb{Z}/p\mathbb{Z}$ even though there are only two possible groups E, namely $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Remark 3.2.20 One can similarly interpret $H^i(G, M)$ for $i > 2$ in terms of longer exact sequences; this is similar to the construction of higher Yoneda extension groups. See [22].

Extended functoriality

We already saw that if we have a homomorphism of G-modules, we get induced homomorphisms on cohomology groups. But what if we want to relate G-modules for different groups G, as will happen in our study of class field theory? It turns out that in a suitable sense, the cohomology groups are also functorial with respect to changing G.

Definition 3.2.21 Let M be a G-module and M' a G'-module. Suppose we are given a homomorphism $\alpha\colon G' \to G$ of groups and a homomorphism $\beta\colon M \to M'$ of abelian groups (note that they go in opposite directions!). We say these are **compatible** if $\beta(m^{\alpha(g)}) = \beta(m)^g$ for all $g \in G$ and $m \in M$. In this case, one gets canonical homomorphisms $H^i(G, M) \to H^i(G', M')$: one firsts constructs these on pairs of injective resolutions, then shows that any two choices are homotopic and hence give the same maps on cohomology. We will refer to the construction of such homomorphisms as the **extended functoriality** of group cohomology. ◊

Example 3.2.22 The principal examples of extended functoriality we will be using are the following.

1. Note that cohomology groups don't seem to carry a nontrivial G-action, because you compute them by taking invariants. This can be reinterpreted in terms of extended functoriality: let $\alpha\colon G \to G$ be the conjugation by some fixed h: $g \mapsto h^{-1}gh$, and let $\beta\colon M \to M$ be the map $m \mapsto m^h$. Then the induced homomorphisms $H^i(G, M) \to H^i(G, M)$ are all identity maps.

2. If H is a subgroup of G, M is a G-module, and M' is just M with all but the H-action forgotten, we get the **restriction homomorphisms**

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

   Another way to get the same map: use the adjunction homomorphism $M \to \mathrm{Ind}_H^G M$ from Proposition 3.2.6 sending m to $\sum_i m^{g_i} \otimes [g_i^{-1}]$, where g_i runs over a set of right coset representatives of H in G, then apply Shapiro's lemma (Lemma 3.2.3) to get

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

3. Let M be a G-module and consider the map $\mathrm{Ind}_H^G M \to M$ taking $m \otimes [g]$ to m^g. We then get maps $H^i(G, \mathrm{Ind}_H^G M) \to H^i(G, M)$ which, together with the isomorphisms of Shapiro's lemma (Lemma 3.2.3), give what are called the **corestriction homomorphisms**:

$$\mathrm{Cor}\colon H^i(H, M) \xrightarrow{\sim} H^i(G, \mathrm{Ind}_H^G M) \to H^i(G, M).$$

4. The composition $\mathrm{Cor} \circ \mathrm{Res}$ is induced by the homomorphism of G-modules $M \to \mathrm{Ind}_H^G M \to M$ given by

$$m \mapsto \sum_i m^{g_i} \otimes [g_i^{-1}] \to \sum_i m = [G : H]m.$$

   Thus $\mathrm{Cor} \circ \mathrm{Res}$ acts as multiplication by $[G : H]$ on each (co)homology group.

   Bonus consequence (hereafter excluding the case of H^0): if we take H to be the trivial group, then the group in the middle is isomorphic to $H^i(H, M) = 0$. So every cohomology group for G is killed by $\#G$, and in particular is a torsion group.

   In fact, if M is finitely generated as an abelian group, this means $H^i(G, M)$ is always finite, because each of these will be finitely generated and torsion. Of course, this won't happen in many of our favorite examples, e.g., $H^i(\mathrm{Gal}(L/K), L^*)$ for L/K a finite Galois extension of fields.

5. Let H be a *normal* subgroup of G, let α be the surjection $G \to G/H$, and let β be the injection $M^H \hookrightarrow M$. Note that G/H acts on M^H; in this case, we get the **inflation homomorphisms**

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

   The inflation and restriction maps will interact in an interesting way; see Proposition 4.2.14.

□

Exercises

1. Complete the proof of the correspondence between $H^1(G, M)$ and principal homogeneous spaces (Definition 3.2.15).

2. The set $H^2(G, M)$ has the structure of an abelian group. Describe the corresponding structure on short exact sequences $0 \to M \to E \to G \to 0$. (A related concept in homological algebra is the **Baer sum**.)

3.3 Homology and Tate groups

Reference. [36], II.2.

You may not be surprised to learn that there is a "dual" theory to the theory of group cohomology, namely group homology. What you may be surprised to learn is that one can actually fit the two together, so that in a sense the homology groups become cohomology groups with negative indices. (Since the arguments are similar to those for cohomology, I'm going to skip some details.)

Homology

Definition 3.3.1 Let M_G denote the maximal quotient of M on which G acts trivially. In other words, M_G is the quotient of M by the submodule spanned by $m^g - m$ for all $m \in M$ and $g \in G$. In yet other words, $M_G = M/MI_G$, where I_G is the **augmentation ideal** of the group algebra $\mathbb{Z}[G]$:

$$I_G = \left\{ \sum_{g \in G} z_g[g] : \sum_g z_g = 0 \right\}.$$

Or if you like, $M_G = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. Since M^G is the group of G-invariants, we call M_G the group of **G-coinvariants**. ◊

The functor $M \to M^G$ is right exact but not left exact: if $0 \to M' \to M \to M'' \to 0$, then $M'_G \to M_G \to M''_G \to 0$ is exact but the map on the left is not injective. Again, we can fill in the exact sequence by defining homology groups.

Definition 3.3.2 A G-module M is **projective** if for any surjection $N \to N'$ of G-modules and any map $\phi : M \to N'$, there exists a map $\psi : M \to N$ lifting ϕ. This definition is dual to the definition of an injective G-module, but this symmetry is a bit misleading: it is much easier to find projectives than injectives. For example, any G-module which is a free module over the ring $\mathbb{Z}[G]$ is projective such as $\mathbb{Z}[G]$ itself! ◊

Definition 3.3.3 A **projective resolution** of M is an exact sequence $\cdots \to P_1 \to P_0 \to M \to 0$ of G-modules in which the P_i are projective. Given such a resolution, take coinvariants to get a complex

$$\cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \to 0,$$

then put $H_i(G, M) = \ker(d_{i-1})/\operatorname{im}(d_i)$. Again, this is canonically independent of the resolution and functorial, and there is a long exact sequence which starts out

$$\cdots \to H_1(G, M'') \xrightarrow{\delta} H_0(G, M') \to H_0(G, M) \to H_0(G, M'') \to 0.$$

◊

Definition 3.3.4 We say that M is **acyclic (for homology)** if $H_i(G, M) = 0$ for $i > 0$. As with group cohomology, we can replace a projective resolution with an acyclic resolution and get the same homology groups. For example, induced modules are again acyclic and the analogue of Shapiro's lemma holds (key point: any free $\mathbb{Z}[H]$-module induces to a free $\mathbb{Z}[G]$-module). ◊

Remark 3.3.5 One can give a concrete description of homology as well, but we won't need it for our purposes. Even without one, though, we can calculate $H_1(G, \mathbb{Z})$, using the exact sequence

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

By the long exact sequence in homology,

$$0 = H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G])$$

is exact, i.e. $0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G$ is exact. The last map is induced by $I_G \hookrightarrow \mathbb{Z}[G]$ and so is the zero map. Thus $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$; recall that in Exercise 3, it was shown that the map $g \mapsto [g] - 1$ defines an isomorphism $G^{\mathrm{ab}} \to I_G/I_G^2$. This can be thought of as an algebraic analogue

of the fact that the first homology group of a (reasonable) topological space equals the abelianization of the fundamental group.

The Tate groups

We now "fit together" the long exact sequences of cohomology and homology to get a doubly infinite exact sequence.

Definition 3.3.6 Let M be a G-module. Define the map $\mathrm{Norm}_G : M \to M$ by

$$\mathrm{Norm}_G(m) = \sum_{g \in G} m^g.$$

Then Norm_G induces a homomorphism

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

$\Diamond$

Remark 3.3.7 You might be wondering why Norm_G is called a "norm" rather than a "trace". The reason is that in practice, our modules M will most often be groups which are most naturally written multiplicatively, e.g., the nonzero elements of a field.

Definition 3.3.8 We now define the **Tate cohomology groups** (or **Tate homology groups** if you prefer) as follows:

$$H_T^i = \begin{cases} H^i(G, M) & i > 0 \\ M^G / \mathrm{Norm}_G M & i = 0 \\ \ker(\mathrm{Norm}_G)/MI_G & i = -1 \\ H_{-i-1}(G, M) & i < -1. \end{cases}$$

$\Diamond$

Lemma 3.3.9 *For any short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules, we have a canonical exact sequence*

$$\cdots \to H_T^{i-1}(G, M'') \to H_T^i(G, M') \to H_T^i(G, M) \to H_T^i(G, M'') \to H_T^{i+1}(G, M') \to \cdots$$

which extends infinitely in both directions.

Proof. Since we already have long exact sequences for homology and cohomology, the only remaining issue is exactness between $H_T^{-2}(G, M'')$ and $H_T^1(G, M')$ inclusive. This follows by diagram-chasing, as in the proof of the snake lemma (Lemma 3.1.16) on the commutative diagram Figure 3.3.10 with exact rows, noting that the diagram remains commutative with the dashed arrows added. ■

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

Figure 3.3.10

Remark 3.3.11 If M is an induced G-module, then $H_T^i(G, M) = 0$ for all i (see Exercise 1. That is, induced modules are acyclic for all of cohomology, homology, and Tate (co)homology.

Extended functoriality revisited

The extended functoriality for cohomology groups (Definition 3.2.21) has analogues for homology groups and Tate cohomology groups, but under more restrictive conditions.

Definition 3.3.12 Again, let M be a G-module and M' a G'-module, and consider a homomorphism $\alpha : G' \to G$ of groups and a homomorphism $\beta : M \to M'$ of abelian which are compatible in the sense of Definition 3.2.21. We would like to obtain canonical homomorphisms $H_i(G, M) \to H_i(G', M')$, but for this we need to add an additional condition to ensure that $M \to M'$ induces a well-defined map $M_G \to M'_{G'}$. For instance, this holds if α is surjective.

For Tate cohomology groups, there is a further complication that the map $M^G \to (M')^{G'}$ does not necessarily induce a map $\mathrm{Norm}(M) \to \mathrm{Norm}(M')$. However, this does occur if α is injective, so for instance we have well-defined restriction maps $\mathrm{Res} : H^0_T(G, M) \to H^0_T(H, M)$ whenever H is a subgroup of G. ◊

Remark 3.3.13 In Example 3.2.22, we used the restriction and corestriction maps to show that for G a finite group and M a G-module, the groups $H^i(G, M)$ are torsion groups killed by $\#G$ for all $i > 0$. While we cannot extend the corestriction map to Tate cohomology, we may still argue directly that $H^0_T(G, M)$ is killed by $\#G$.

Exercises

1. Prove that if M is an induced G-module, then $H^i_T(G, M) = 0$ for all $i \in \mathbb{Z}$.

Hint. Use the fact that induced G-modules are acyclic for both cohomology and homology to reduce to checking the cases $i = -1, 0$. Another option is to extend Shapiro's lemma to Tate cohomology groups.

2. Let $G \subseteq H$ be an inclusion of finite groups. Show that via the identification from Remark 3.3.5, the map $\mathrm{Res} : H_T^{-2}(G, \mathbb{Z}) \to H_T^{-2}(H, \mathbb{Z})$ corresponds to the transfer (Verlagerung) map $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. This provides another way to derive the existence of the latter.

3.4 Cohomology of cyclic groups

Reference. [37], IV.7; [33], IX.1.

We next specialize attention to the case of a finite *cyclic* group, which will play a key role in many of our calculations. In this case, the cohomology, homology, and Tate groups satisfy a key periodicity property (Theorem 3.4.1) which allows us to define and manipulate a sort of "Euler characteristic", the **Herbrand quotient** (Definition 3.4.4).

The periodicity theorem

In general, for any given G and M, it is at worst a tedious exercise to compute $H^i_T(G, M)$ for any single value of i, but try to compute all of these at once and you discover that they exhibit very little evident structure. Thankfully, there is an exception to that dreary rule when G is cyclic.

Theorem 3.4.1 *Let G be a finite cyclic group and M a G-module. Then there is a functorial isomorphism $H^i_T(G, M) \to H^{i+2}_T(G, M)$ for all $i \in \mathbb{Z}$; moreover, these isomorphisms are all determined by the choice of a generator of G.*

Proof. Choose a generator g of G. We start with the four-term exact sequence of G-modules

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

in which the first map is $1 \mapsto \sum_{g \in G}[g]$, the second map is $[h] \mapsto [hg] - [h]$, and the third map is $[h] \mapsto 1$. Since everything in sight is a free abelian group, we can tensor over $\mathbb{Z}$ with M and get another exact sequence:

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

The terms in the middle are just $\mathrm{Ind}_1^G M$, where we first restrict M to a module for the trivial group and then induce back up. Thus their Tate groups are all zero. The desired result now follows from the following general fact: if

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to 0$$

is exact and B and C have all Tate groups zero, then there is a canonical isomorphism $H_T^{i+2}(G, A) \to H_T^i(G, D)$. To see this, apply the long exact sequence to the short exact sequences

$$0 \to A \to B \to B/\operatorname{im}(f) \to 0$$
$$0 \to B/\ker(g) \to C \to D \to 0$$

to get

$$H^{i+2}(G, A) \cong H^{i+1}(G, B/\operatorname{im}(f)) = H^{i+1}(G, B/\ker(g)) \cong H^i(G, D).$$

■

Remark 3.4.2 In particular, when G is cyclic, the long exact sequence of a short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules curls up into an exact hexagon as in Figure 3.4.3.

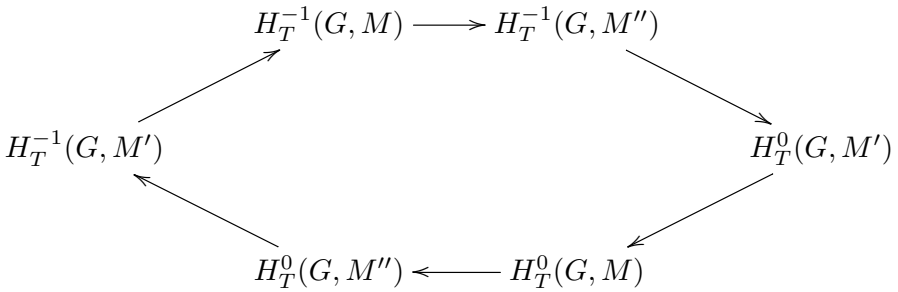

Figure 3.4.3

Herbrand quotients

Definition 3.4.4 Let G be a finite cyclic group and let M be a G-module. If the groups $H_T^i(G, M)$ are finite, we define the **Herbrand quotient** as the ratio

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

From the exactness of the hexagon in Figure 3.4.3, we see that if M', M, M'' all have Herbrand quotients, then

$$h(M) = h(M')h(M'').$$

◊

Remark 3.4.5 Expanding on the previous point, if two of M', M, M'' have Herbrand quotients, then so does the third. For example, if M' and M'' have Herbrand quotients, i.e., their Tate groups are finite, then we have an exact sequence

$$H_T^{-1}(G, M') \to H_T^{-1}(G, M) \to H_T^{-1}(G, M'')$$

and the outer groups are all finite. In particular, the first map is out of a finite group and so has finite image, and modulo that image, $H_T^{-1}(G, M)$ injects into another finite group. So it's also finite, and so on.

Remark 3.4.6 In practice, it will often be much easier to compute the Herbrand quotient of a G-module than to compute either of its Tate groups directly. The Herbrand quotient will then do half of the work for free: once one group is computed directly, at least the order of the other will be automatically known.

Remark 3.4.7 If M is finite, then $h(M) = 1$. To wit, the sequences

$$0 \to M^G \to M \to M \to M_G \to 0$$
$$0 \to H_T^{-1}(G, M) \to M_G \stackrel{\mathrm{Norm}_G}{\to} M^G \to H_T^0(G, M) \to 0$$

are exact, where $M \to M$ is the map $m \mapsto m^g - m$; thus M_G and M^G have the same order, as do H_T^{-1} and H_T^0.

Exercises

1. The periodicity of the Tate groups for G cyclic means that there is a canonical (up to the choice of a generator of G) isomorphism between $H_T^{-1}(G, M)$ and $H_T^1(G, M)$, i.e., between $\ker(\mathrm{Norm}_G)/MI_G$ and the set of equivalence classes of 1-cocycles. What is this isomorphism explicitly? In other words, given an element of $\ker(\mathrm{Norm}_G)/MI_G$, what is the corresponding 1-cocycle?

2. Put $K = \mathbb{Q}_p(\sqrt{p})$. Compute the Herbrand quotient of K^* as a G-module for $G = \mathrm{Gal}(\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p)$.

Hint. Use the exact sequence $1 \to \mathfrak{o}_K^* \to K^* \to \mathbb{Z} \to 1$.

3. Let $G = S_3$ (the symmetric group on three letters), let $M = \mathbb{Z}^3$ with the natural G-action permuting the factors, and let $N = M^G$. Compute $H^i(G, M/N)$ for $i = 1, 2$ however you want: you can explicitly compute cochains, use the alternate interpretations given above, or use the exact sequence $0 \to N \to M \to M/N \to 0$. Better yet, use more than one method and make sure that you get the same answer.

Hint. Part of the point of this exercise is that even in this relatively simple-looking situation, it is not all that easy to do the computation. One approach that minimizes the computational complexity is to use the **Hochschild-Serre spectral sequence** (see [36], Remark II.1.35>) to reduce to working with the cyclic groups $H = A_3 \cong \mathbb{Z}/3\mathbb{Z}$ and $G/H = S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, for which periodicity is applicable.

3.5 Profinite groups and infinite Galois theory

Reference. [37], IV.1 and IV.2 (for profinite groups only, not their cohomology); [36], II.4.

We've mostly spoken so far about finite extensions of fields and the corresponding finite Galois groups. However, Galois theory can be made to work

perfectly well for infinite extensions, and it's convenient to do so; it will be more convenient at times to work with the absolute Galois group of field instead of with the Galois groups of individual extensions.

Profinite groups

Recall the Galois correspondence for a finite extension.

Proposition 3.5.1 *Let L/K be a finite Galois extension of fields and put $G = \mathrm{Gal}(L/K)$. Then the (normal) subgroups H of G correspond to the (Galois) subextensions M of L, the correspondence in each direction being given by*

$$H \mapsto \mathrm{Fix}\, H, \qquad M \mapsto \mathrm{Gal}(L/M).$$

Proof. We will state a stronger result in Theorem 3.5.7. ■

To see what we have to be careful about for infinite extensions, consider the following example.

Example 3.5.2 Let $\mathbb{F}_q$ be a finite field; recall that $\mathbb{F}_q$ has exactly one finite extension of any degree. Moreover, for each n, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of degree n, generated by the Frobenius map σ which sends x to x^q. In particular, σ generates a cyclic subgroup of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. But this Galois group is much bigger than that! Namely, let $\{s_n\}_{n=1}^{\infty}$ be a sequence with $s_n \in \mathbb{Z}/n\mathbb{Z}$, such that if $m|n$, then $s_m \equiv s_n \pmod{m}$. The set of such sequences forms a group $\widehat{\mathbb{Z}}$ by componentwise addition. This group is much bigger than $\mathbb{Z}$, and any element gives an automorphism of $\overline{\mathbb{F}_q}$: namely, the automorphism acts on $\mathbb{F}_{q^n}$ as σ^{s_n}. In fact, $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$, and it is not true that every subgroup of $\widehat{\mathbb{Z}}$ corresponds to a subfield of $\overline{\mathbb{F}_q}$: the subgroup generated by σ has fixed field $\mathbb{F}_q$, and you don't recover the subgroup generated by σ by taking automorphisms over the fixed field. □

In order to recover the Galois correspondence, we need to impose a little extra structure on Galois groups; namely, we give them a topology.

Definition 3.5.3 A **profinite group** is a topological group which is Hausdorff and compact, and which admits a basis of neighborhoods of the identity consisting of normal subgroups. More explicitly, a profinite group is a group G plus a collection of subgroups of G of finite index designated as **open subgroups**, such that the intersection of two open subgroups is open, but the intersection of all of the open subgroups is trivial. Profinite groups act a lot like finite groups; some of the ways in which this is true are reflected in the exercises. ◊

Example 3.5.4 Examples of profinite groups include the group $\widehat{\mathbb{Z}}$ in which the subgroups $n\widehat{\mathbb{Z}}$ are open, and the p-adic integers $\mathbb{Z}_p$ in which the subgroups $p^n\mathbb{Z}_p$ are open. More generally, for any local field K, the additive group $\mathfrak{o}_K$ and the multiplicative group $\mathfrak{o}_K^*$ are profinite. (The additive and multiplicative groups of K are not profinite, because they're only locally compact, not compact.) For a nonabelian example, see Exercise 2. □

Remark 3.5.5 Warning. A profinite group may have subgroups of finite index that are not open. For example, let $G = 1 + t\mathbb{F}_p[[t]]$ (under multiplication). Then G is profinite with the subgroups $1 + t^n\mathbb{F}_p[[t]]$ forming a basis of open subgroups; in particular, it has countably many open subgroups. But G is isomorphic to a countable direct product of copies of $\mathbb{Z}_p$, with generators $1 + t^i$ for i not divisible by p. Thus it has *uncountably* many subgroups of finite index, most of which are not open!

By contrast, a theorem of Nikolov and Segal asserts that any *finitely gener-*

ated profinite group (i.e., one which admits a dense finitely generated subgroup) has the property that every subgroup of finite index is open. See [39].

Infinite Galois groups

Definition 3.5.6 If L/K is a Galois extension, but not necessarily finite, we make $G = \mathrm{Gal}(L/K)$ into a profinite group by declaring that the open subgroups of G are precisely $\mathrm{Gal}(L/M)$ for all finite subextensions M of L. ◊

Theorem 3.5.7 The Galois correspondence. *Let L/K be a Galois extension (not necessarily finite). Then there is a correspondence between (Galois) subextensions M of L and (normal)* closed *subgroups H of* $\mathrm{Gal}(L/K)$*, given by*

$$H \mapsto \mathrm{Fix}\, H, \qquad M \mapsto \mathrm{Gal}(L/M).$$

Proof. See [24], Theorem 8.16. ■

Example 3.5.8 The Galois correspondence of Theorem 3.5.7 holds for $\overline{\mathbb{F}_q}/\mathbb{F}_q$ because the open subgroups of $\widehat{\mathbb{Z}}$ are precisely $n\widehat{\mathbb{Z}}$ for all positive integers n. □

Another way to construct profinite groups uses **inverse limits** (or **projective limits** or sometimes just **limits**).

Definition 3.5.9 Suppose we are given a partially ordered set I, a family $\{G_i\}_{i\in I}$ of finite groups and a map $f_{ij} : G_i \to G_j$ for each pair $(i, j) \in I \times I$ such that $i > j$. For simplicity, let's assume the f_{ij} are all surjective (this is slightly more restrictive than absolutely necessary, but is always true for Galois groups). Then there is a profinite group G with open subgroups H_i for $i \in I$ such that $G/H_i \cong G_i$ in a manner compatible with the f_{ij}: let G be the set of families $\{g_i\}_{i\in I}$, where each g_i is in G_i and $f_{ij}(g_i) = g_j$. ◊

Example 3.5.10 The group $\mathbb{Z}_p$ can be viewed either as the completion of $\mathbb{Z}$ for the p-adic absolute value or as the inverse limit of the groups $\mathbb{Z}/p^n\mathbb{Z}$. Similarly, the group $\widehat{\mathbb{Z}}$ can be viewed as the inverse limit of the groups $\mathbb{Z}/n\mathbb{Z}$, with the usual surjections from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ if m is a multiple of n (that is, the ones sending 1 to 1). In fact, *any* profinite group can be reconstructed as the inverse limit of its quotients by open subgroups. (And it's enough to use just a set of open subgroups which form a basis for the topology, i.e., for $\mathbb{Z}_p$, you can use $p^{2n}\mathbb{Z}_p$ as the subgroups.) □

Remark 3.5.11 Rule of thumb. If profinite groups make your head hurt, you can always think instead of inverse systems of finite groups. But that might make your head hurt more!

Cohomology of profinite groups

One can do group cohomology for groups which are profinite, not just finite, but one has to be a bit careful: these groups only make sense when you carry along the profinite topology.

Definition 3.5.12 If G is profinite, by a **G-module** we mean a topological abelian group M with a *continuous* G-action $M \times G \to M$. In particular, we say M is **discrete** if it has the discrete topology; that implies that the stabilizer of any element of M is open, and that M is the union of M^H over all open subgroups H of G. Canonical example: $G = \mathrm{Gal}(L/K)$ acting on L^*, even if L is not finite.

The category of discrete G-modules has enough injectives, so you can define cohomology groups for any discrete G-module, and all the usual abstract

nonsense will still work. The main point is that you can compute them from their finite quotients. ◊

Proposition 3.5.13 *The group $H^i(G, M)$ is the direct limit of $H^i(G/H, M^H)$ using the inflation homomorphisms.*

Proof. See [36], Proposition II.4.4. ■

Let us unpack this statement.

Definition 3.5.14 For $H_1 \subseteq H_2 \subseteq G$ inclusions of finite index, we have the **inflation homomorphism**

$$\mathrm{Inf} : H^i(G/H_2, M^{H_2}) \to H^i(G/H_1, M^{H_1}).$$

Via these homomorphisms, the groups $H^i(G/H, M^H)$ form a direct system and Proposition 3.5.13 asserts that $H^i(G, M)$ is the **direct limit** (or **inductive limit** or **colimit**) of the $H^i(G/H, M^H)$. In concrete terms, you take the disjoint union of $H^i(G/H, M^H)$ over all H, then identify together pairs of elements that become the same somewhere down the line. ◊

Remark 3.5.15 One can also compute the groups $H^i(G, M)$ using **continuous cochains**: this amounts to considering continuous maps $G^{i+1} \to M$ that satisfy the same algebraic conditions as do the usual cochains. One consequence of this interpretation is that $H^1(G, M)$ classifies continuous crossed homomorphisms modulo principal ones.

Remark 3.5.16 Warning. The passage from finite to profinite groups is only well-behaved for cohomology. In particular, we will not attempt to define either homology or the Tate groups in the profinite setting. (Remember that the formation of the Tate groups involves the norm map, i.e., summing over elements of the group.)

Exercises

1. Prove that every open subgroup of a profinite group contains an open normal subgroup.

2. For any ring R, we denote by $\mathrm{GL}_n(R)$ the group of $n \times n$ matrices over R which are invertible (equivalently, whose determinant is a unit). Prove that $\mathrm{GL}_n(\widehat{\mathbb{Z}})$ is a profinite group, and say as much as you can about its open subgroups.

3. Let A be an abelian torsion group. Show that $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ is a profinite group, if we take the open subgroups to be all subgroups of finite index. This group is called the **Pontryagin dual** of A.

4. A closed subgroup H of a profinite group G is called a **Sylow p-subgroup** of G if, for every open normal subgroup N of G, the image of H in G/N (a/k/a HN/N) is a Sylow p-subgroup of G/N. (It is enough to check this for N running over a neighborhood basis of the identity.) Using the Sylow theorems for finite groups, prove that:

   (a) For every prime p, there exists a Sylow p-subgroup of G. (Beware that this subgroup need not be open in G.)

   (b) Every subgroup of G, the quotient of which by any open normal subgroup is a p-group, is contained in a Sylow p-subgroup.

   (c) Every two Sylow p-subgroups of G are conjugate.

   Hint. See [37] exercise IV.2.4.

5. Compute the Sylow p-subgroups of $\widehat{\mathbb{Z}}$, of $\mathbb{Z}_p^*$, and of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Hint. See [37], exercise IV.2.4.

6. **Artin-Schreier extensions.**Let L/K be a $\mathbb{Z}/p\mathbb{Z}$-extension of fields of characteristic $p > 0$. Prove that $L = K(\alpha)$ for some α such that $\alpha^p - \alpha \in K$.

Hint. Let K^{sep} be a separable closure of K containing L, and consider the short exact sequence $0 \to \mathbb{F}_p \to K^{\mathrm{sep}} \to K^{\mathrm{sep}} \to 0$ in which the map $K^{\mathrm{sep}} \to K^{\mathrm{sep}}$ is given by $x \mapsto x^p - x$.

Chapter 4

Local class field theory

We will spend the entirety of Chapter 4 establishing **local class field theory**, a classification of the abelian extensions of a local field. This will serve two purposes. On one hand, the results of local class field theory can be used to assist in the proofs of the global theorems, as we saw with Kronecker-Weber. On the other hand, they also give us a model set of proofs which we will attempt to emulate in the global case.

Recall that the term **local field** refers to a finite extension either of the field of p-adic numbers $\mathbb{Q}_p$ or of the field of power series $\mathbb{F}_q((t))$. I'm going to abuse language and ignore the second case, although all but a few things I'll say go through in the second case, and I'll try to flag those when they come up. (One big one: a lot of extensions have to be assumed to be separable for things to work right.)

4.1 Overview of local class field theory

Reference. [36], I.1; [37], V.1.

The local reciprocity law

The main theorem of local class field theory is the following.

Definition 4.1.1 For K a local field, let K^{ab} be the maximal abelian extension of K. ◊

Theorem 4.1.2 Local Reciprocity Law. *Let K be a local field. Then there is a unique map $\phi_K : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying the following conditions:*

1. *for any uniformizer π of K and any finite unramified extension L of K, $\phi_K(\pi)$ acts on L as the Frobenius automorphism;*
2. *for any finite abelian extension L of K, the group of norms $\mathrm{Norm}_{L/K} L^*$ is in the kernel of ϕ_K, and the induced map $K^*/\mathrm{Norm}_{L/K} L^* \to \mathrm{Gal}(L/K)$ is an isomorphism.*

Proof. See the discussion in Section 4.3. ■

Definition 4.1.3 The map ϕ_K in Theorem 4.1.2 is variously called the **local reciprocity map** or the **norm residue symbol**. ◊

Example 4.1.4 Using the local Kronecker-Weber theorem (Theorem 1.1.5), the statement of Theorem 4.1.2 can be explicitly verified for $K = \mathbb{Q}_p$. To wit,

we have $K^{\mathrm{ab}} = K_1 K_2$ where $K_1 = \bigcup_n \mathbb{Q}_p(\zeta_{p^n})$ and $K_2 = \bigcup_n \mathbb{Q}_p(\zeta_{p^n-1})$, and $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K_1/K) \times \mathrm{Gal}(K_2/K)$. Since p is totally ramified in K_1, we have

$$\mathrm{Gal}(K_1/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^*.$$

Since p is unramified in K_2, we have

$$\mathrm{Gal}(K_2/K) \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}.$$

However, it will be more convenient to think of the image as sitting inside

$$\mathrm{Gal}(\bigcup_n \mathbb{Q}(\zeta_{p^n-1})/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^*/\mathbb{Z}_p^* \cong \prod_{q \neq p} \mathbb{Z}_q^*$$

(here using global Kronecker-Weber and Artin reciprocity). That is, we are looking for a map

$$\phi_K : \mathbb{Z}_p^* \times p^{\mathbb{Z}} \cong \mathbb{Q}_p^* \to \mathrm{Gal}(K_1/K) \times \mathrm{Gal}(K_2/K) \subset \mathbb{Z}_p^* \times \prod_{q \neq p} \mathbb{Z}_q^*;$$

the map we want is the identity on the first factor and the map $p \mapsto p$ on the second factor. See Exercise 1. □

The local reciprocity law is an analogue of the Artin reprocity law for number fields. We also get an analogue of the existence of ray class fields.

Theorem 4.1.5 Local existence theorem. *For every finite (not necessarily abelian) extension L of K, $\mathrm{Norm}_{L/K} L^*$ is an open subgroup of K^* of finite index. Conversely, for every (open) subgroup U of K^* of finite index, there exists a finite abelian extension L of K such that $U = \mathrm{Norm}_{L/K} L^*$.*

Proof. For the first assertion, see Exercise 3 (or Exercise 4 for the case of characteristic p). For the second assertion, see Theorem 4.3.11. ■

Remark 4.1.6 In Theorem 4.1.5, the topology on K^* is the one given by taking the disjoint union of the sets $\pi^n \mathfrak{o}_K^*$ for $n \in \mathbb{Z}$, where $\pi \in K^\times$ is a uniformizer. In fact, it is only necessary to keep track of this topology in the function field case; for K a finite extension of $\mathbb{Q}_p$, one can show that every subgroup of K^* of finite index is open.

Another way to identify the correct topology on K^* is to equip K with its usual topology (the norm topology defined by an extension of the p-adic absolute value) and then take the subspace topology for the inclusion of K^* into $K \times K$ given by $x \mapsto (x, x^{-1})$. While this does coincide with the subspace topology for the inclusion of K^* into K, there are good reasons not to view it this way; see Exercise 6.

The local existence theorem says that if we start with a nonabelian extension L, then $\mathrm{Norm}_{L/K} L^*$ is also the group of norms of an abelian extension. But which one? The following theorem gives the answer.

Theorem 4.1.7 Norm limitation theorem. *Let M be the maximal abelian subextension of L/K. Then $\mathrm{Norm}_{L/K} L^* = \mathrm{Norm}_{M/K} M^*$.*

Proof. See the discussion in Section 4.3. ■

Remark 4.1.8 In Theorem 4.1.7, it is evident that $\mathrm{Norm}_{L/K} L^* \subseteq \mathrm{Norm}_{M/K} M^*$ because $\mathrm{Norm}_{L/K} = \mathrm{Norm}_{M/K} \circ \mathrm{Norm}_{L/M}$. Since the group $\mathrm{Norm}_{L/K} L^*$ can be shown directly to be an open subgroup of finite index (see Exercise 3), Theorem 4.1.5 implies that it has the form $\mathrm{Norm}_{N/K} N^*$ for some finite abelian extension N of K. Theorem 4.1.2 then implies that $M \subseteq N$. The

subtle point that remains to be proven is that the inclusion $M \subseteq N$ is actually an equality.

Remark 4.1.9 For each uniformizer π of K, let K_π be the composite of all finite abelian extensions L such that $\pi \in \mathrm{Norm}_{L/K} L^*$. Then the local reciprocity map implies that $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{unr}}$.

It turns out that K_π can be explicitly constructed as the extension of K by certain elements, thus giving a generalization of local Kronecker-Weber to arbitrary local fields! These elements come from **Lubin-Tate formal groups**, which we will not discuss further.

Note that for L/K a finite extension of local fields, the map

$$K^*/\mathrm{Norm}_{L/K} L^* \to \mathrm{Gal}(L/K) = G$$

obtained by combining the local reciprocity law with the norm limitation theorem is in fact an isomorphism of $G = G^{\mathrm{ab}} = H_T^{-2}(G, \mathbb{Z})$ with $K^*/\mathrm{Norm}_{L/K} L^* = H_T^0(G, L^*)$. We will in fact show something stronger, from which we will deduce both the local reciprocity law and the norm limitation theorem.

Theorem 4.1.10 *For any finite Galois extension L/K of local fields with Galois group G, there is a canonical isomorphism $H_T^i(G, \mathbb{Z}) \to H_T^{i+2}(G, L^*)$.*

Proof. See the discussion in Section 4.3. ■

Remark 4.1.11 The map in Theorem 4.1.10 can be written in terms of the **cup product** in group cohomology (see [36], Proposition II.1.38). We will not develop this point of view here.

The local invariant map

We will first prove the following.

Theorem 4.1.12 *For any local field K, there exist canonical isomorphisms*

$$H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), (K^{\mathrm{unr}})^*) \to H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*)$$
$$\mathrm{inv}_K : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. This will follow from Proposition 4.2.1. ■

Definition 4.1.13 In Theorem 4.1.12, the first map is an inflation homomorphism; the second map is called the **local invariant map**. More precisely, for L/K finite of degree n, we have an isomorphism

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

and these isomorphisms are compatible with inflation. (In particular, we don't need to prove the first isomorphism separately. But that can be done, by considerations involving the Brauer group; see below.) ◊

To use Theorem 4.1.12 to prove Theorem 4.1.10 and hence the local reciprocity law (Theorem 4.1.2) and the norm limitation theorem (Theorem 4.1.7), we employ the following theorem of Tate.

Theorem 4.1.14 *Let G be a finite group and M a G-module. Suppose that for each subgroup H of G (including $H = G$), $H^1(H, M) = 0$ and $H^2(H, M)$ is cyclic of order $\#H$. Then there exist isomorphisms $H_T^i(G, \mathbb{Z}) \to H_T^{i+2}(G, M)$ for all i; these are canonical once you fix a choice of a generator of $H^2(G, M)$.*

Proof. See Theorem 4.3.1. ■

Definition 4.1.15 For any field K, the group $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*)$ is called the **Brauer group** of K. See Section 7.6 for further discussion. ◊

Abstract class field theory

Having derived local class field theory once, we will do it again a slightly different way in Chapter 5. In the course of proving the above results, we will show (among other things) that if L/K is a cyclic extension of local fields,

$$\#H_T^0(\mathrm{Gal}(L/K), L^*) = [L:K], \qquad \#H_T^{-1}(\mathrm{Gal}(L/K), L^*) = 1.$$

It turns out that this alone is enough number-theoretic input to prove local class field theory! More precisely, we will identify "minimal" properties of a field K with $G = \mathrm{Gal}(\overline{K}/K)$, a surjective continuous homomorphism $d : G \to \widehat{\mathbb{Z}}$ (defining "unramified" extensions of K), a continuous G-module A (playing the role of $\overline{K}^*$), and a homomorphism $v : A^G \to \widehat{\mathbb{Z}}$ (playing the role of the valuation map) that will suffice to yield the reciprocity map. See Section 5.4 for the continuation of this discussion.

Exercises

1. Building on Example 4.1.4, verify Theorem 4.1.2 in the case $K = \mathbb{Q}_p$.

Hint. The first assertion of Theorem 4.1.2 follows from global Artin reciprocity (Definition 1.1.7). To check the second assertion for $L = \mathbb{Q}(\zeta_n)$, use the fact that $\mathrm{Norm}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}(1 - \zeta_{p^m}) = p$ for any positive integer m. Alternatively, see Lemma 7.5.3.

2. For $K = \mathbb{Q}_p$, take $\pi = p$ in Remark 4.1.9. Determine K_π, again using local Kronecker-Weber.

Hint. You should get $K_\pi = \mathbb{Q}(\zeta_{p^\infty})$.

3. Prove that for any finite extension L/K of finite extensions of $\mathbb{Q}_p$, $\mathrm{Norm}_{L/K} L^*$ is an open subgroup of K^*.

Hint. Show that already $\mathrm{Norm}_{L/K} K^*$ is open! The corresponding statement in positive characteristic is more subtle; see Exercise 4.

4. Prove that for any finite extension L/K of finite separable extensions of $\mathbb{F}_p((t))$, $\mathrm{Norm}_{L/K} L^*$ is an open subgroup of K^*.

Hint. Reduce to the case of a cyclic extension of prime degree. If the degree is prime to p, you may imitate Exercise 3; otherwise, that approach fails because $\mathrm{Norm}_{L/K} K^*$ lands inside the subfield K^p, but you can use this to your advantage to make an explicit calculation.

5. A **quaternion algebra** over a field K is a central simple algebra over K of dimension 4. If K is not of characteristic 2, any such algebra has the form

$$K \oplus Ki \oplus Kj \oplus Kk, \qquad i^2 = a, j^2 = b, ij = -ji = k$$

for some $a, b \in K^*$. (For example, the case $K = \mathbb{R}$, $a = b = -1$ gives the standard Hamilton quaternions.) A quaternion algebra is **split** if it is isomorphic to the ring of 2×2 matrices over K. Show that if K is a local field, then any two quaternion algebras which are not split are isomorphic to each other.

Hint. While this can be done using elementary methods, it will also follow from Theorem 4.1.12 via the cohomological description of Brauer groups; see Lemma 7.6.2.

6. Let K be a finite extension of $\mathbb{Q}_p$. Show that K^* can be viewed as a closed subspace of $K \times K$ via the inclusion $x \mapsto (x, x^{-1})$, and deduce from this that K^* is a locally compact abelian group for the subspace topology It can also be viewed as a subspace of K, but not as a closed subspace; this distinction will show up more seriously when we talk about adèles and idèles (Remark 6.2.3).

4.2 Cohomology of local fields: some computations

Reference. [36], III.1 and III.2; [37], V.1.

Notation convention. If you catch me writing $H^i(L/K)$ for L/K a Galois extension of fields, that's shorthand for $H^i(\mathrm{Gal}(L/K), L^*)$. Likewise for H_i or H^i_T.

Overview

We now make some computations of $H^i_T(L/K)$ for L/K a Galois extension of local fields. To begin with, recall that by "Theorem 90" (Lemma 1.2.3), $H^1(L/K) = 0$. Our next goal will be to supplement this fact with a computation of $H^2(L/K)$.

Proposition 4.2.1 *For any finite Galois extension L/K of local fields, $H^2(L/K)$ is cyclic of order $[L : K]$. Moreover, this group can be canonically identified with $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ in such a way that if M/L is another finite extension such that M/K is also Galois, the inflation homomorphism $H^2(L/K) \to H^2(M/K)$ corresponds to the inclusion $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subseteq \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z}$.*

Proof. For the first assertion, see Proposition 4.2.17 and Proposition 4.2.18. For the second assertion, see Lemma 4.2.21. ■

Remark 4.2.2 Before continuing, it is worth keeping in a safe place the exact sequence

$$1 \to \mathfrak{o}_L^* \to L^* \to L^*/\mathfrak{o}_L^* = \pi_L^{\mathbb{Z}} \to 1.$$

In this exact sequence of $G = \mathrm{Gal}(L/K)$-modules, the action on $\pi_L^{\mathbb{Z}}$ is always trivial (since the valuation on L is Galois-invariant).

Remark 4.2.3 Another basic fact to keep in mind is that any finite Galois extension of local fields is *solvable*. To wit, the maximal unramified extension is cyclic,; the maximal tamely ramified extension is cyclic over that; and the rest is a Galois extension whose degree is a power of p, and every finite p-group is solvable.

This will allow us to simplify some of the following arguments by writing a general Galois extension as a tower of successive cyclic extensions. Of course we will have no such shortcut in the global case, because the Galois group of a Galois extension of number fields can be any group whatsoever; in fact the inverse Galois problem asks whether this always occurs for an extension over $\mathbb{Q}$, and no counterexample is known.

The unramified case

Recall that unramified extensions are cyclic, since their Galois groups are also the Galois groups of extensions of finite fields.

Proposition 4.2.4 *For any finite extension L/K of* finite *fields, the map* $\mathrm{Norm}_{L/K} : L^* \to K^*$ *is surjective.*

Proof. One can certainly give an elementary proof of this using the fact that L^* is cyclic (see Exercise 1). But one can also see it using the machinery we have at hand. Because L^* is a finite module, its Herbrand quotient is 1. Also, we know $H^1_T(L/K)$ is trivial by Lemma 1.2.3. Thus $H^0_T(L/K)$ is trivial too, that is, $\mathrm{Norm}_{L/K} : L^* \to K^*$ is surjective. ∎

Proposition 4.2.5 *For any finite unramified extension L/K of local fields, the map* $\mathrm{Norm}_{L/K} : \mathfrak{o}_L^* \to \mathfrak{o}_K^*$ *is surjective.*

Proof. Say $u \in \mathfrak{o}_K^*$ is a unit. By Proposition 4.2.4, we may pick $v_0 \in \mathfrak{o}_L^*$ such that in the residue fields, the norm of v_0 coincides with u. Thus $u/\operatorname{Norm}(v_0) \equiv 1 \pmod{\pi}$, where π is a uniformizer of K. Now we construct units $v_i \equiv 1 \pmod{\pi^i}$ such that $u_i = u/\operatorname{Norm}(v_0 \cdots v_i) \equiv 1 \pmod{\pi^{i+1}}$: simply take v_i so that $\mathrm{Trace}((1 - v_i)/\pi^i) \equiv (1 - u_{i-1})/\pi^i \pmod{\pi}$. (That's possible because the trace map on residue fields is surjective by the normal basis theorem.) Then the product $v_0 v_1 \cdots$ converges to a unit v with norm u. ∎

Corollary 4.2.6 *For any finite unramified extensions L/K of local fields, $H^i_T(\mathrm{Gal}(L/K), \mathfrak{o}_L^*) = 1$ for all $i \in \mathbb{Z}$.*

Proof. Again, $\mathrm{Gal}(L/K)$ is cyclic, so by Theorem 3.4.1 we need only check this for $i = 0, 1$. For $i = 0$, it is Proposition 4.2.5. For $i = 1$, note that because L/K is unramified, we can split the surjection $L^* \to L^*/\mathfrak{o}_L^*$ by choosing a uniformizer π_K of K and writing $L^* = \mathfrak{o}_L^* \pi_K^{\mathbb{Z}}$. Hence $H^1_T(\mathrm{Gal}(L/K), \mathfrak{o}_L^*)$ is a direct summand of $H^1_T(\mathrm{Gal}(L/K), L^*)$, and the latter vanishes by Lemma 1.2.3. ∎

Proposition 4.2.7 *For any finite unramified extension L/K of local fields, $H^2(L/K)$ is cyclic of order $[L : K]$.*

Proof. Using the Herbrand quotient, we get $h(L^*) = h(\mathfrak{o}_L^*)h(\mathbb{Z})$. Corollary 4.2.6 says that $h(\mathfrak{o}_L^*) = 1$, and

$$\begin{aligned} h(L^*/\mathfrak{o}_L^*) &= h(\mathbb{Z}) \\ &= \#H^0_T(\mathrm{Gal}(L/K), \mathbb{Z})/\#H^1_T(\mathrm{Gal}(L/K), \mathbb{Z}) \\ &= \#\,\mathrm{Gal}(L/K)^{\mathrm{ab}}/\#\,\mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Z}) \\ &= [L : K]. \end{aligned}$$

Since $H^1_T(\mathrm{Gal}(L/K), L^*)$ is trivial, we conclude that $H^0_T(\mathrm{Gal}(L/K), L^*)$ has order $[L : K]$. Moreover, the long exact sequence of Tate groups gives an exact sequence

$$1 \to H^0_T(\mathrm{Gal}(L/K), L^*) \to H^0_T(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathrm{Gal}(L/K) \to 1,$$

where the ends vanish by Corollary 4.2.6 again; so by periodicity (Theorem 3.4.1) we also get that $H^0_T(\mathrm{Gal}(L/K), L^*) \cong H^2(L/K)$ is cyclic of order $[L : K]$. ∎

Let us now make the description of $H^2(L/K)$ more canonical. Consider the short exact sequence

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

of modules with trivial Galois action. The module $\mathbb{Q}$ is injective as a G-module for any group G (Exercise 2). Thus we get an isomorphism $H^0_T(\mathrm{Gal}(L/K), \mathbb{Z}) \to H^{-1}_T(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$. But the latter is

$$H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z});$$

since $\mathrm{Gal}(L/K)$ has a canonical generator (Frobenius), we can evaluate there and get a canonical map

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \to \mathbb{Z}/[L:K]\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}..$$

Putting it all together, we get a canonical map

$$H^2(\mathrm{Gal}(L/K), L^*) \cong H^0_T(\mathrm{Gal}(L/K), L^*) \cong H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

In this special case, this is none other than the local invariant map! In fact, by taking direct limits, we get a canonical isomorphism

$$H^2(K^{\mathrm{unr}}/K) \cong \mathbb{Q}/\mathbb{Z}.$$

Remark 4.2.8 What's really going on here is that $H^0_T(\mathrm{Gal}(L/K), L^*)$ is a cyclic group generated by a uniformizer π (since every unit is a norm). Under the map $H^0_T(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$, that uniformizer is being mapped to $1/[L:K]$.

The cyclic case

Let L/K be a cyclic but possibly ramified extension of local fields. Again, $H^1_T(L/K)$ is trivial by Lemma 1.2.3, so all there is to compute is $H^0_T(L/K)$. We are going to show again that it has order $[L:K]$. (It's actually cyclic again, but we won't prove this just yet.)

Lemma 4.2.9 *Let L/K be a finite Galois extension of local fields. Then there is an open, Galois-stable subgroup V of $\mathfrak{o}_L$ such that $H^i(\mathrm{Gal}(L/K), V) = 0$ for all $i > 0$ (i.e., V is acyclic for cohomology).*

Proof. By the normal basis theorem, there exists $\alpha \in L$ such that $\{\alpha^g : g \in \mathrm{Gal}(L/K)\}$ is a basis for L over K. Without loss of generality, we may rescale to get $\alpha \in \mathfrak{o}_L$; then put $V = \sum \mathfrak{o}_K \alpha^g$. As in the proof of Theorem 3.2.9, V is induced: $V = \mathrm{Ind}_1^G \mathfrak{o}_K$, so is acyclic. ■

The following proof uses that we are in characteristic 0, but it can be modified to work also in the function field case.

Lemma 4.2.10 *Let L/K be a finite Galois extension of local fields. Then there is an open, Galois-stable subgroup W of $\mathfrak{o}_L^*$ such that $H^i(\mathrm{Gal}(L/K), W) = 0$ for all $i > 0$.*

Proof. Take V as in Lemma 4.2.9. If we choose α sufficiently divisible, then V lies in the radius of convergence of the exponential series

$$\exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}$$

(you need $v_p(x) > 1/(p-1)$, to be precise), and we may take $W = \exp(V)$. ■

Proposition 4.2.11 *For L/K a cyclic extension of local fields, $\#H^0_T(\mathrm{Gal}(L/K), L^*) = [L:K]$.*

Proof. Take W as in Lemma 4.2.10. Since W has finite index in $\mathfrak{o}_L^*$, we have $h(\mathfrak{o}_L^*/W) = 1$ and hence $h(\mathfrak{o}_L^*) = h(W) = 1$ by Lemma 4.2.10. So again we may conclude that $h(L^*) = h(\mathfrak{o}_L^*)h(\mathbb{Z}) = [L:K]$, and so $H^0_T(\mathrm{Gal}(L/K), L^*) = [L:K]$. ■

Remark 4.2.12 Notwithstanding Proposition 4.2.11, at this stage we cannot yet check that $H^0_T(\mathrm{Gal}(L/K), L^*)$ is cyclic, because the groups $H^1_T(\mathrm{Gal}(L/K), \mathfrak{o}_L^*)$

are not guaranteed to vanish. See Exercise 3.

Remark 4.2.13 Note. This is all that we need for "abstract" local class field theory. We'll revisit this point later.

The general case

For those in the know, there is a **spectral sequence** underlying this next result; compare Exercise 3.

Proposition 4.2.14 Inflation-restriction exact sequence. *Let G be a finite group, let H be a normal subgroup, and let M be a G-module. If $H^i(H, M) = 0$ for $i = 1, \dots, r-1$, then the sequence*

$$0 \to H^r(G/H, M^H) \overset{\text{Inf}}{\to} H^r(G, M) \overset{\text{Res}}{\to} H^r(H, M)$$

is exact.

Proof. For $r = 1$, the condition on H^i is empty. In this case, $H^1(G, M)$ classifies crossed homomorphisms $\phi : G \to M$. If one of these factors through G/H, it becomes a constant map when restricted to H; if that constant value itself belongs to M^H, then it must be zero and so the restriction to H is trivial. Conversely, if there exists some $m \in M$ such that $\phi(h) = m^h - m$ for all $h \in H$, then $\phi'(g) = \phi(g) - m^g + m$ is another crossed homomorphism representing the same class in $H^1(G, M)$, but taking the value 0 on each $h \in H$. For $g \in G, h \in H$, we have

$$\phi'(hg) = \phi'(h)^g + \phi'(g) = \phi'(g),$$

so ϕ' is constant on cosets of H and so may be viewed as a crossed homomorphism from G/H to M. On the other hand,

$$\phi'(g) = \phi'(gh) = \phi'(g)^h + \phi(h) = \phi'(g)^h$$

so ϕ' takes values in M^H. Thus the sequence is exact at $H^1(G, M)$; exactness at $H^i(G/H, M^H)$ is similar but easier.
If $r > 1$, we induct on r by dimension shifting. Recall (from Proposition 3.2.6) that there is an injective homomorphism $M \to \text{Ind}_1^G M$ of G-modules. Let N be the G-module which makes the sequence

$$0 \to M \to \text{Ind}_1^G M \to N \to 0$$

exact. We construct a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{r-1}(G/H, N^H) & \xrightarrow{\text{Inf}} & H^{r-1}(G, N) & \xrightarrow{\text{Res}} & H^{r-1}(H, N) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^r(G/H, M^H) & \xrightarrow{\text{Inf}} & H^r(G, M) & \xrightarrow{\text{Res}} & H^r(H, M).
\end{array}$$

Figure 4.2.15

The second vertical arrow arises from the long exact sequence for G-cohomology; since $\text{Ind}_1^G M$ is an induced G-module, this arrow is an isomorphism. Similarly, the third vertical arrow arises from the long exact sequence for H-cohomology, and it is an isomorphism because $\text{Ind}_1^G M$ is also an induced H-module; moreover, $H^i(H, N) = 0$ for $i = 1, \dots, r-2$. Finally, taking H-invariants yields another exact sequence

$$0 \to M^H \to (\text{Ind}_1^G M)^H \to N^H \to H^1(H, M) = 0,$$

so we may take the long exact sequence for G/H-cohomology to obtain the first vertical arrow; it is an isomorphism because $(\mathrm{Ind}_1^G M)^H$ is an induced G/H-module. The induction hypothesis implies that the top row is exact, so the bottom row is also exact. ■

Corollary 4.2.16 *If $M/L/K$ is a tower of fields with M/K and L/K finite and Galois, the sequence*

$$0 \to H^2(L/K) \overset{\mathrm{Inf}}{\to} H^2(M/K) \overset{\mathrm{Res}}{\to} H^2(M/L)$$

is exact.

Proof. This follows from Proposition 4.2.14 using Lemma 1.2.3. ■

We now prove the following.

Proposition 4.2.17 *For any finite Galois extension L/K of local fields, the group $H^2(\mathrm{Gal}(L/K), L^*)$ has order at most $[L:K]$.*

Proof. We've checked the case of L/K cyclic, so we may use it as the basis for an induction. If L/K is not cyclic, since it is solvable (Remark 4.2.3), we can find a Galois subextension M/K. Now the exact sequence

$$0 \to H^2(M/K) \to H^2(L/K) \to H^2(L/M)$$

from Corollary 4.2.16 implies that $\#H^2(L/K) \leq \#H^2(M/K)\#H^2(L/M) = [M:K][L:M] = [L:K]$. ■

To complete the proof that $H^2(L/K)$ is cyclic of order $[L:K]$, it now suffices to produce a cyclic subgroup of order $[L:K]$.

Proposition 4.2.18 *Let L/K be a finite Galois extension of local fields. Let M/K be an unramified extension of degree $[L:K]$. Then the image of $H^2(L/K)$ in $H^2(ML/K)$ contains the image of $H^2(M/K)$ in $H^2(ML/K)$. Consequently (by Proposition 4.2.7 and Corollary 4.2.16), the group $H^2(\mathrm{Gal}(L/K), L^*)$ contains a cyclic subgroup of order $[L:K]$.*

Proof. Consider the diagram

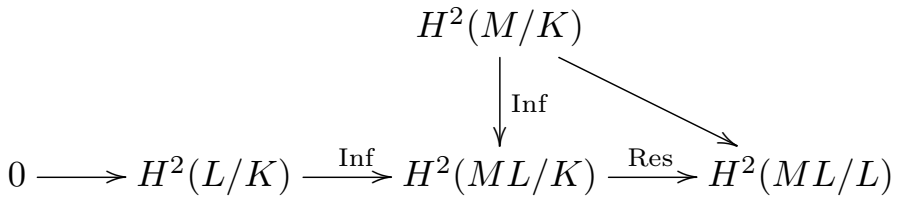

Figure 4.2.19

in which the bottom row is exact and the vertical arrow is injective, both by Corollary 4.2.16. It suffices to show that the diagonal arrow $H^2(M/K) \to H^2(ML/L)$ is the zero map, as this will imply an inclusion $H^2(M/K) \subseteq H^2(L/K)$ within $H^2(ML/K)$ and we already know that $H^2(M/K)$ is cyclic of order $[M:K] = [L:K]$ by Proposition 4.2.7.

Let $e = e(L/K)$ and $f = f(L/K)$ be the ramification index and residue field degree, so that $[ML:L] = e$. Let U be the maximal unramified subextension of L/K; then we have a canonical isomorphism $\mathrm{Gal}(ML/L) \cong \mathrm{Gal}(M/U)$ of cyclic groups. By using the same generators in both groups, we can make a commutative diagram

$$\begin{array}{ccccc} H^0_T(M/K) & \xrightarrow{\text{Res}} & H^0_T(M/U) & \longrightarrow & H^0_T(ML/L) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(M/K) & \xrightarrow{\text{Res}} & H^2(M/U) & \longrightarrow & H^2(ML/L) \end{array}$$

Figure 4.2.20

in which the vertical arrows are isomorphisms. (Remember from Definition 3.3.12 that restriction maps on Tate homology make sense in degree 0; that gives the first horizontal arrow in Figure 4.2.20.) The composition in the bottom row is the map $H^2(M/K) \to H^2(ML/L)$ which we want to be zero; it thus suffices to check that the top row composes to zero.
Let us rewrite this composition concretely as

$$K^*/\operatorname{Norm}_{M/K} M^* \to U^*/\operatorname{Norm}_{M/U} M^* \to L^*/\operatorname{Norm}_{ML/L}(ML)^*$$

where the maps are induced by the inclusions $K^* \to U^* \to L^*$. Now $K^*/\operatorname{Norm}_{M/K} M^*$ is a cyclic group of order ef generated by π_K, a uniformizer of K, and $L^*/\operatorname{Norm}_{ML/L}(ML)^*$ is a cyclic group of order e generated by π_L, a uniformizer of L. But π_K is a unit of $\mathfrak{o}_L$ times π_L^e, so the map in question is indeed zero. ■

The local invariant map

We have now proved the first assertion of Proposition 4.2.1 (by combining Proposition 4.2.17 and Proposition 4.2.18). We now turn to the second assertion. In the process, we will also see that $H^2(\overline{K}/K) \cong \mathbb{Q}/\mathbb{Z}$.

Lemma 4.2.21 *For any Galois extension L/K of local fields, the group $H^2(L/K)$ can be canonically identified with $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ in such a way that if M/K is another Galois extension containing L, the inflation homomorphism $H^2(L/K) \to H^2(M/K)$ corresponds to the inclusion $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subseteq \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z}$.*

Proof. By Corollary 4.2.16 we have an injection $H^2(K^{\text{unr}}/K) \to H^2(\overline{K}/K)$, and the former is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$; so we have to prove that this injection is actually also surjective. Remember that $H^2(\overline{K}/K)$ is the direct limit of $H^2(M/K)$ running over all finite extensions M of K. What we just showed above is that if $[M : K] = n$ and L is the unramified extension of K of degree n, then the images of $H^2(M/K)$ and $H^2(L/K)$ in $H^2(ML/K)$ are the same. In particular, that means that $H^2(M/K)$ is in the image of the map $H^2(K^{\text{unr}}/K) \to H^2(\overline{K}/K)$. Since that's true for any M, we get that the map is indeed surjective, hence an isomorphism. ■

Remark 4.2.22 By combining Proposition 4.2.18 with Lemma 4.2.21, we see that for any local field K, the map $H^2(K^{\text{unr}}/K) \to H^2(\overline{K}/K)$ is an isomorphism. We can use this to see the effect of changing K on this group; see Proposition 4.2.23 below.

Proposition 4.2.23 *For L/K a finite extension of local fields of degree n, the map* Res : $H^2(K^{\text{unr}}/K) \to H^2(L^{\text{unr}}/L)$ *translates, via the local reciprocity map, into the map from $\mathbb{Q}/\mathbb{Z}$ to itself given by multiplication by n.*

Proof. We compute the map following [36], Proposition III.1.8. Put $e = e_{L/K}, f = f_{L/K}$. We form a commutative diagram

$$\begin{array}{ccccccc} H^2(K^{\mathrm{unr}}/K) & \xrightarrow{v_K} & H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K),\mathbb{Z}) & \xleftarrow{\delta} & H^1(\mathrm{Gal}(K^{\mathrm{unr}}/K),\mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle e\,\mathrm{Res}} & & \downarrow{\scriptstyle \times ef} \\ H^2(L^{\mathrm{unr}}/L) & \xrightarrow{v_L} & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L),\mathbb{Z}) & \xleftarrow{\delta} & H^1(\mathrm{Gal}(L^{\mathrm{unr}}/L),\mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

Figure 4.2.24

as follows. The left square comes from the valuation maps. The middle square comes from the connecting homomorphisms for the sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ with the trivial actions; note that these connecting homomorphisms are isomorphisms by Exercise 2. The right square comes from evaluating crossed homomorphisms at Frobenius. Since $ef = n$, this yields the claim. ■

Exercises

1. Give an elementary proof (without cohomology) that the norm map from one finite field to another is always surjective.

Hint. Write everything in terms of a generator of the multiplicative group of the larger field.

2. \times Let G be a finite group. Let M be a G-module whose underlying abelian group is a $\mathbb{Q}$-vector space. Prove that M is an acyclic G-module.

Hint. First show that the groups $H^i(G, M)$ are divisible, say using the description in terms of cochains. Then combine with the fact that these group are killed by the order of G (Example 3.2.22).

3. Give an example of a cyclic ramified extension L/K of local fields in which the groups $H^i_T(\mathrm{Gal}(L/K), \mathfrak{o}_L^*)$ are nontrivial.

4.3 Local class field theory via Tate's theorem

Reference. [36] II.3, III.5.

For L/K a finite extension of local fields (of characteristic 0), we have now computed that $H^1(L/K) = 0$ (Lemma 1.2.3) and $H^2(L/K)$ is cyclic of order $[L : K]$ (Proposition 4.2.1). We next use these ingredients to establish all of the statements of local class field theory.

Tate's theorem

We first prove the theorem of Tate stated earlier (Theorem 4.1.14). Note that right now, we only need this for solvable groups because every finite Galois extension of local fields has solvable Galois group (Remark 4.2.3); this allows for some simplification in the arguments. However, we will do the extra work to do the general case for later use in the global setting.

Theorem 4.3.1 Tate. *Let G be a finite group and let M be a G-module. Suppose that for all subgroups H of G (including G itself), $H^1(H, M) = 0$ and $H^2(H, M)$ is cyclic of order $\#H$. Then there are isomorphisms $H^i_T(G, \mathbb{Z}) \to H^{i+2}_T(G, M)$ which are canonical up to a choice of generator of $H^2(G, M)$.*

Proof. Let γ be a generator of $H^2(G, M)$. Since $\mathrm{Cor} \circ \mathrm{Res} = [G : H]$ (Example 3.2.22), $\mathrm{Res}(\gamma)$ generates $H^2(H, M)$ for any H. We start out by explicitly constructing a G-module containing M in which γ becomes a coboundary.

Choose a 2-cocycle $\phi : G^3 \to M$ representing γ; by the definition of a cocycle,

$$\phi(g_0 g, g_1 g, g_2 g) = \phi(g_0, g_1, g_2)^g,$$
$$\phi(g_1, g_2, g_3) - \phi(g_0, g_2, g_3) + \phi(g_0, g_1, g_3) - \phi(g_0, g_1, g_2) = 0.$$

Moreover, ϕ is a coboundary if and only if it's of the form $d(\rho)$, that is, $\phi(g_0, g_1, g_2) = \rho(g_1, g_2) - \rho(g_0, g_2) + \rho(g_0, g_1)$. This ρ must itself be G-invariant: $\rho(g_0, g_1)^g = \rho(g_0 g, g_1 g)$. Thus ϕ is a coboundary if $\phi(e, g, hg) = \rho(e, h)^g - \rho(e, hg) + \rho(e, g)$.

Let $M[\phi]$ be the direct sum of M with the free abelian group with one generator x_g for each element g of $G - \{e\}$, with the G-action

$$x_h^g = x_{hg} - x_g + \phi(e, g, hg).$$

(The symbol x_e should be interpreted as the element $\phi(e, e, e)$ of M.) Using the cocycle property of ϕ, one may verify that this is indeed a G-action; by construction, the cocycle ϕ becomes zero in $H^2(G, M[\phi])$ by setting $\rho(e, g) = x_g$. (Milne calls $M[\phi]$ the **splitting module** of ϕ.) Moreover, by the same token, for any H, the restriction of ϕ to H also becomes zero in $H^2(H, M)$.

The map $\alpha : M[\phi] \to \mathbb{Z}[G]$ sending M to zero and x_g to $[g] - 1$ is a homomorphism of G-modules. Actually it maps into the augmentation ideal I_G, and the sequence

$$0 \to M \to M[\phi] \to I_G \to 0$$

is exact. (Note that this is backwards from the usual exact sequence featuring I_G as a submodule, which will appear again momentarily.) For any subgroup H of G, we can restrict to H-modules, then take the long exact sequence:

$$0 = H^1(H, M) \to H^1(H, M[\phi]) \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M[\phi]) \to H^2(H, I_G).$$

To make headway with this, view $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ as an exact sequence of H-modules. Since $\mathbb{Z}[G]$ is induced, its Tate groups all vanish. So we get a dimension shift:

$$H^1(H, I_G) \cong H_T^0(H, \mathbb{Z}) = \mathbb{Z}/(\#H)\mathbb{Z}.$$

Similarly, $H^2(H, I_G) \cong H^1(H, \mathbb{Z}) = 0$. Also, the map $H^2(H, M) \to H^2(H, M[\phi])$ is zero because we constructed this map so as to kill off the generator ϕ. Thus $H^2(H, M[\phi]) = 0$ and $H^1(H, I_G) \to H^2(H, M)$ is surjective. But these groups are both finite of the same order! So the map is also injective, and $H^1(H, M[\phi])$ is also zero.

Now apply Lemma 4.3.2 below to conclude that $H_T^i(G, M[\phi]) = 0$ for all i. This allows us to use the four-term exact sequence

$$0 \to M \to M[\phi] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

(as in the proof of Theorem 3.4.1) to conclude that $H_T^i(G, \mathbb{Z}) \cong H_T^{i+2}(G, M)$. ∎

Lemma 4.3.2 *Let G be a finite group and M a G-module. Suppose that $H^i(H, M) = 0$ for $i = 1, 2$ and H any subgroup of G (including G itself). Then $H_T^i(G, M) = 0$ for all $i \in \mathbb{Z}$.*

Proof. Let us first check that $H_T^i(G, M) = 0$ for all $i \geq 0$. For G cyclic, this follows by periodicity. For G solvable, we prove the general result by induction on $\#G$. Since G is solvable, it has a proper subgroup H for which G/H is cyclic. By the induction hypothesis, $H_T^i(H, M) = 0$ for all i. Thus by the

inflation-restriction exact sequence (Proposition 4.2.14),

$$0 \to H^i(G/H, M^H) \to H^i(G, M) \to H^i(H, M)$$

is exact for all $i > 0$. The term on the end being zero, we have $H^i(G/H, M^H) \cong H^i(G, M) = 0$ for $i = 1, 2$. By periodicity (Theorem 3.4.1), $H_T^i(G/H, M^H) = 0$ for all i, so $H^i(G/H, M^H) = 0$ for all $i > 0$, and $H^i(G, M) = 0$ for $i > 0$. As for $i = 0$, note that $H_T^0(G/H, M^H) = H^2(G/H, M^H) = 0$, so for any $x \in M^G$ there exists $y \in M^H$ such that $\mathrm{Norm}_{G/H}(y) = x$. Since $H_T^0(H, M) = 0$, there exists $z \in M$ such that $\mathrm{Norm}_H(z) = x$. Now $\mathrm{Norm}_G(z) = \mathrm{Norm}_{G/H} \circ \mathrm{Norm}_H(z) = x$. Thus $H_T^0(G, M) = 0$, as desired.

We next extend the previous argument from G solvable to G general (this can be skipped if you only want the final result for solvable G). For $i > 0$, we already know that the group $H^i(G, M)$ is torsion (Example 3.2.22), so it suffices to show that its p-primary component vanishes for any prime p. To check this, let G_p be any Sylow p-subgroup of G. As per Example 3.2.22 again, the composition of $\mathrm{Res} : H^i(G, M) \to H^i(H, M)$ with $\mathrm{Cor} : H^i(H, M) \to H^i(G, M)$ is multiplication by $[G : G_p]$, which is prime to p. Consequently, Res induces an injective map on p-primary components. Since G_p is solvable, we already know that $H^i(G_p, M) = 0$, yielding the desired vanishing. For $i = 0$, we argue as in Remark 3.3.13: we know that $H_T^0(G_p, M) = 0$, so the map $\mathrm{Norm}_{G_p} : M \to M^{G_p}$ is surjective. In particular, for any $x \in M^G$, we can find $y \in M$ such that $x = \sum_{g \in G_p} y^g$. Then $\mathrm{Norm}_G(y) = [G : G_p]x$, so the group $H_T^0(G, M)$ is torsion and killed by $[G : G_p]$; again varying over p shows that $H_T^0(G, M) = 0$.

Finally, we treat the case $i < 0$ by dimension shifting. Make the exact sequence

$$0 \to N \to \mathrm{Ind}_1^G M \to M \to 0$$

in which $m \otimes [g]$ maps to m^g. The term in the middle is acyclic, so $H_T^{i+1}(H', N) \cong H_T^i(H', M)$ for any subgroup H' of G. In particular, $H^1(H', N) = H^2(H', N) = 0$, so the above argument gives $H_T^i(G, N) = 0$ for $i \geq 0$. Now from $H_T^0(G, N) = 0$ we get $H_T^{-1}(G, M) = 0$; since the same argument applies to N, we also get $H_T^{-2}(G, M) = 0$ and so on. ■

Local reciprocity and norm limitation

Let L/K be a finite Galois extension of local fields. For any intermediate extension M/K, we know that $H^1(L/M) = 0$ and $H^2(L/M)$ is cyclic of order $[L : M]$. We may thus apply Theorem 4.3.1 with $G = \mathrm{Gal}(L/K)$, $M = L^*$ to obtain isomorphisms $H_T^i(G, \mathbb{Z}) \to H_T^{i+2}(G, M)$, thus proving Theorem 4.1.10. This yields a canonical isomorphism

$$K^*/\mathrm{Norm}_{L/K} L^* = H_T^0(L/K) \to H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

This establishes the existence of the local reciprocity map (Theorem 4.1.2), keeping in mind that part (a) follows from the explicit computations in Section 4.2), together with the norm limitation theorem (Theorem 4.1.7), modulo one subtlety: if M/K is another finite Galois extension containing L, we need to know that the diagram

$$\begin{array}{ccc} K^*/\mathrm{Norm}_{M/K} M^* & \longrightarrow & \mathrm{Gal}(M/K)^{\mathrm{ab}} \\ \downarrow & & \downarrow \\ K^*/\mathrm{Norm}_{L/K} L^* & \longrightarrow & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

Figure 4.3.3

commutes, so that the maps $K^* \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$ fit together to give a map $K^* \to \mathrm{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{ab}}$. In other words, we need a commuting diagram

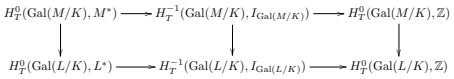

Figure 4.3.4

The right square in Figure 4.3.4 comes from taking long exact sequences in the commutative diagram with exact rows:

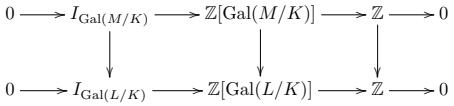

Figure 4.3.5

To construct the left square in Figure 4.3.4, we similarly need to construct a commutative diagram with exact rows:

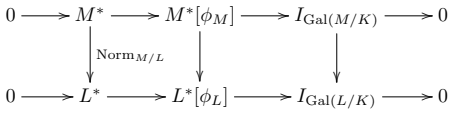

Figure 4.3.6

I claim we can arrange for this as follows. First choose a cocycle $\phi_M : \mathrm{Gal}(M/K)^3 \to M^*$ representing the preferred generator of $H^2(M/K)$. Then there exists a unique map ϕ_L fitting into the following commuting square:

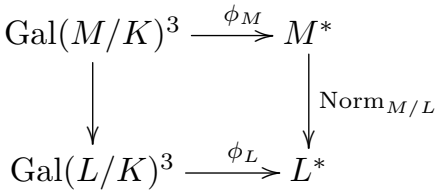

Figure 4.3.7

and this will necessarily give a cocycle representing the preferred generator of $H^2(L/K)$. Further details omitted.

The local existence theorem

It remains to prove the local existence theorem (Theorem 4.1.5). This does not follow directly from cohomological considerations; instead we need to construct some extensions with small norm groups. Fortunately, since we have already established the norm limitation theorem, we do not need to construct *abelian* extensions; this will give us some flexibility.

We begin with a lemma, in which we take advantage of Kummer theory to establish a special case of the existence theorem.

Lemma 4.3.8 *Let ℓ be a prime number. Let K be a local field containing a primitive ℓ-th root of unity. Then $x \in K^*$ is an ℓ-th power in K if and only if belongs to $\mathrm{Norm}_{L/K} L^*$ for every cyclic extension L of K of degree ℓ.*

Proof. Let M be the compositum of all cyclic ℓ-extensions of K. The group $K^*/(K^*)^\ell$ is finite (Exercise 1), and hence is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^n$ for some positive integer n. By Kummer theory (Theorem 1.2.9), we also have $\mathrm{Gal}(M/K) \cong$

$(\mathbb{Z}/\ell\mathbb{Z})^n$. By the local reciprocity law (Theorem 4.1.2), $K^*/\operatorname{Norm}_{M/K} M^* \cong (\mathbb{Z}/\ell\mathbb{Z})^n$; consequently, on one hand $(K^*)^\ell \subseteq \operatorname{Norm}_{M/K} M^*$, and on other hand these subgroups of K^* have the same index ℓ^n. They are thus equal, proving the claim. ■

Remark 4.3.9 The conclusion of Lemma 4.3.8 remains true even if ℓ is not prime; see Exercise 3. This statement can be interpreted in terms of the **Hilbert symbol**, whose properties generalize quadratic reciprocity to higher powers; see [36], III.4.

This allows to deduce a corollary of the existence theorem which is needed in its proof. (The argument we give here depends squarely on characteristic 0; some patching is needed in the positive characteristic case.)

Corollary 4.3.10 *Let K be a local field of characteristic 0. Then the intersection of the groups $\operatorname{Norm}_{L/K} L^*$ for all finite extensions L of K is the trivial group.*

Proof. Let D_K be the intersection in question; note that $D_K \subseteq \mathfrak{o}_K^*$ by considering unramified extensions of K, so D_K is in particular a compact topological group. By Lemma 4.3.8, every element of D_K is an ℓ-th power in K for every prime ℓ. We will show that in fact every element of D_K is the ℓ-th power of an element of D_K itself; this will show that D_K is a divisible abelian group, and in particular every element is an n-th power for every positive integer n. This will then imply using Exercise 2 that D_K is the trivial group. (Alternatively, one can follow the suggestion of Remark 4.3.9 and prove that the conclusion of Lemma 4.3.8 retains true when ℓ is replaced by an arbitrary positive integer n, and then apply Exercise 2 directly.)
We first need to verify something which might seem obvious but isn't quite: for L/K a finite extension,

$$\operatorname{Norm}_{L/K} D_L = D_K.$$

This isn't obvious because for $x \in D_K$, for each individual finite extension M of K we can write $x = \operatorname{Norm}_{M/K}(z)$ for some $z \in M^*$, but it is not apparent that we can force the elements $y = \operatorname{Norm}_{M/L}(z)$ to all be equal. It is nonetheless true because, for any given M the set of such y is a nonempty compact subset of U_L, and any finite intersection of these subsets is nonempty (because we can pass to a large enough field to contain all of the M in question and bring an element from there); so the whole intersection is nonempty.
Now let ℓ be a prime and choose $x \in D_K$. For each finite extension L of K containing a primitive ℓ-th root of unity, let $E(L)$ be the set of ℓ-th roots of x in K which belong to $\operatorname{Norm}_{L/K} L^*$. This set is finite (of cardinality at most ℓ) and nonempty: we have $x = \operatorname{Norm}_{L/K}(y)$ for some $y \in D_L$ by the previous paragraph, so y has an ℓ-th root z in L and $\operatorname{Norm}_{L/K}(z) \in E(L)$. By the previous paragraph, $E(M) \subseteq E(L)$ whenever $L \subseteq M$, so we may again conclude using the finite intersection property. Alternatively, just note that if each of the (finitely many!) elements of $E(K)$ fails to survive to some larger field, we can take a compositum to get a single field L such that no element of $E(K)$ belongs to $E(L)$, which is absurd since $E(L) \neq \emptyset$. ■

We now return to the proof of the local existence theorem (Theorem 4.1.5).

Theorem 4.3.11 Local existence theorem. *For every (open) subgroup U of K^* of finite index, there exists a finite abelian extension L of K such that $U = \operatorname{Norm}_{L/K} L^*$.*

Proof. We note first that by the local reciprocity law (Theorem 4.1.2), it is enough to construct L so that U contains $\operatorname{Norm}_{L/K} L^*$: in this case, we will have $\operatorname{Gal}(L/K) \cong K^*/\operatorname{Norm}_{L/K} L^*$, and then $U/\operatorname{Norm}_{L/K} L^*$ will corresponding to

$\mathrm{Gal}(L/M)$ for some intermediate extension M/K having the desired effect. We note next that by the norm limitation theorem (Theorem 4.1.7), it suffices to produce *any* finite extension L/K, not necessarily abelian, such that U contains $\mathrm{Norm}_{L/K} L^*$.

Let $m\mathbb{Z} \subseteq \mathbb{Z}$ be the image of U in $K^*/\mathfrak{o}_K^* \cong \mathbb{Z}$; by choosing L to contain the unramified extension of K of degree m, we may ensure that the image of $\mathrm{Norm}_{L/K} L^*$ in $K^*/\mathfrak{o}_K^*$ is also contained in $m\mathbb{Z}$. It thus remains to further ensure that

$$(\mathrm{Norm}_{L/K} L^*) \cap \mathfrak{o}_K^* \subseteq U \cap \mathfrak{o}_K^*.$$

Since $\mathfrak{o}_K^*$ is compact, each open subgroup $(\mathrm{Norm}_{L/K} L^*) \cap \mathfrak{o}_K^*$ is also closed and hence compact. By Corollary 4.3.10, as L/K runs over all finite extensions of K, the intersection of the groups $(\mathrm{Norm}_{L/K} L^*) \cap \mathfrak{o}_K^*$ is trivial; in particular, the intersection of the compact subsets

$$((\mathrm{Norm}_{L/K} L^*) \cap \mathfrak{o}_K^*) \cap (\mathfrak{o}_K^* \setminus U)$$

of $\mathfrak{o}_K^*$ is empty. By the finite intersection property (and taking a compositum), there exists a single L/K for which $(\mathrm{Norm}_{L/K} L^*) \cap \mathfrak{o}_K^* \subseteq U \cap \mathfrak{o}_K^*$, as desired. ■

Exercises

1. Prove that for any local field K and any positive integer n not divisible by the characteristic of K, the group $K^*/(K^*)^n$ is finite.

2. Prove that for any local field K of characteristic 0, the intersection of the groups $(K^*)^n$ over all positive integers n is the trivial group.

Hint. First get the intersection into $\mathfrak{o}_K^*$, then use prime-to-p exponents to get it into the 1-units, then use powers of p to finish. The last step is the only one which fails in characteristic p.

3. Extend Lemma 4.3.8 to the case where ℓ is an arbitrary positive integer, not necessarily prime.

Hint. It may help to use the structure theorem for finite abelian groups.

4.4 Ramification filtrations and local reciprocity

Reference. [46], IV; [37], II.10.

For K a finite extension of $\mathbb{Q}_p$, the local reciprocity map defines an isomorphism of $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ with the profinite completion of K. The natural filtration on the unit group $\mathfrak{o}_K^\times$ thus defines a filtration on $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$; but which one? It turns out that the answer is related to a natural filtration on the entire group $\mathrm{Gal}(\overline{K}/K)$; we give Hadamard's description of this.

The lower numbering filtration

Remark 4.4.1 Recall that for any extension L/K of finite extensions of $\mathbb{Q}_p$, the ring $\mathfrak{o}_L$ is a **monogenic** extension of $\mathfrak{o}_K$: there exists an element $\alpha \in \mathfrak{o}_L$ such that $\mathfrak{o}_L = \mathfrak{o}_K[\alpha]$, meaning that the $\mathfrak{o}_K$-linear homomorphism $\mathfrak{o}_K[x] \to \mathfrak{o}_L$ taking x to α is an isomorphism. (See [46], II.6, Proposition 12 or [37], Lemma II.10.4.)

Lemma 4.4.2 *Let L/K be a Galois extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. Let v_L be the valuation on L and choose a uniformizer π_L of*

L (so that $v_L(\pi_L) = 1$). Choose $\alpha \in \mathfrak{o}_L$ such that $\mathfrak{o}_L = \mathfrak{o}_K[\alpha]$. For every $g \in G$ and every integer $i \geq -1$, the following conditions are equivalent.

1. *The action of g on the ring $\mathfrak{o}_L/\pi_L^{i+1}$ is trivial.*
2. *For all $x \in \mathfrak{o}_L$, $v_L(x^g - x) \geq i + 1$.*
3. *We have $v_L(\alpha^g - \alpha) \geq i + 1$.*

Proof. The first two conditions are equivalent more or less by definition. They both immediately imply the third condition; conversely, the third condition implies the others because g fixes $\mathfrak{o}_K$ and $\mathfrak{o}_L = \mathfrak{o}_K[\alpha]$. ■

Definition 4.4.3 Let L/K be a Galois extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. For each integer $i \geq -1$, let G_i be the set of $g \in G$ satisfying the equivalent conditions of Lemma 4.4.2. The G_i form a decreasing sequence of subgroups of G; these together form the **lower numbering ramification filtration** on G. In particular, $G_{-1} = G$ and G_0 equals the inertia subgroup of G.

For convenience later, we extend the definition of the filtration G_i to arbitrary *real* values $i \geq -1$ by setting $G_i = G_{\lceil i \rceil}$.

From the definition, we see that the formation of the lower numbering filtration is compatible with subgroups: if $H = \mathrm{Gal}(L/M)$ is a subgroup of G, then $H_i = H \cap G_i$ for all $i \geq -1$. However, it is not at all clear what happens when we pass from G to a quotient. ◊

Lemma 4.4.4 *With notation as in Lemma 4.4.2, for $i \geq 0$, an element $g \in G_0$ belongs to G_i if and only if $\pi_L^g/\pi_L \equiv 1 \pmod{\pi_L^i}$.*

Proof. Reduce to the case where L/K is totally ramified; we may then deduce the claim directly from Lemma 4.4.2. See also [46], IV.2, Proposition 5. ■

Definition 4.4.5 For $i \geq 0$, let U_L^i be the subgroup of $\mathfrak{o}_L^*$ consisting of elements α for which $v_L(\alpha - 1) \geq i$. The group U_L^0/U_L^1 is naturally isomorphic to the group of units of the residue field $\mathfrak{o}_L/\pi_L$. For $i > 0$, the group U_L^i/U_L^{i+1} carries the structure of a one-dimensional vector space over $\mathfrak{o}_L/\pi_L$; for any choice of the uniformizer π_L we may use the class of π_L^i as the basis element, but there is *no distinguished choice* without this breaking of symmetry.

By Lemma 4.4.4, for $i \geq 0$ we may view G_i as the maximal subgroup of G carrying U_L^0 into itself. In particular, the quotient G_i/G_{i+1} is naturally isomorphic to a subgroup of U_L^i/U_L^{i+1}.

This gives us the following structural properties of G. First, the group G_{-1}/G_0 is isomorphic to the residue field extension, which is cyclic. Next, G_0/G_1 is isomorphic to a subgroup of U_L^0/U_L^1, and so is cyclic of order prime to p. Finally, for $i \geq 1$, G_i/G_{i+1} is a subgroup of U_L^i/U_L^{i+1}, and so is an elementary abelian p-group. In particular, G is a solvable group, as noted in Remark 4.2.3. ◊

The Herbrand functions

We now introduce Herbrand's recipe to convert the **lower numbering** used in the definition of the ramification filtration into an **upper numbering** that behaves well with respct to passage to quotients.

Definition 4.4.6 Retain notation as in Definition 4.4.3. Define the function $\varphi_{L/K} : [-1, \infty) \to [-1, \infty)$ by the formula

$$\varphi_{L/K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.$$

This function is continuous, piecewise linear, increasing, and concave, and satisfies $\varphi_{L/K}(u) = u$ for $u \in [-1, 0]$. Consequently, it admits an inverse $\psi_{L/K} : [-1, \infty) \to [-1, \infty)$ which is continuous, piecewise linear, increasing, and convex.

We define the **upper numbering** on the ramification groups by the formula

$$G^i = G_{\psi(i)} \Leftrightarrow G^{\varphi(i)} = G_i.$$

$\Diamond$

Lemma 4.4.7 *Let L/K be a finite Galois extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. Let H be a normal subgroup of G with fixed field K'. For $i \geq -1$, $(G/H)_i = G_{\phi_{L/K'}(i)}H/H$.*

Proof. See [46], IV.3, Lemma 5. ■

Lemma 4.4.8 *Let L/K be a finite Galois extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. Let H be a normal subgroup of G with fixed field K'. Then*

$$\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'}, \qquad \psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}.$$

Proof. See [46], IV.3, Proposition 15. ■

Proposition 4.4.9 *Let L/K be a finite Galois extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. Let H be a normal subgroup of G with fixed field K'. For all $i \geq -1$, $(G/H)^i = G^i H/H$.*

Proof. Using Lemma 4.4.7 and Lemma 4.4.8, we see that

$$\begin{aligned}(G/H)^i &= (G/H)_{\psi_{K'/K}(i)} \\ &= G_{\psi_{L/K'} \circ \psi_{K'/K}(i)} \\ &= G_{\psi_{L/K}(i)}\end{aligned}$$

as desired. ■

Definition 4.4.10 Let L/K be a Galois extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. We define the **breaks** in the ramification filtration for the lower numbering (respectively, the upper numbering) as the values of i for which $G_i \neq G_j$ for all $j > i$ (resp. $G^i \neq G^j$ for all $j > i$).

By definition, the breaks for the lower numbering are integers, while the breaks for the upper numbering are only guaranteed to be rational numbers. In fact, it is possible to exhibit examples where the breaks for the upper numbering are not integers (see Exercise 2 and Exercise 3). However, in the next section we will see that this cannot occur for abelian extensions. $\Diamond$

The Hasse-Arf theorem

Theorem 4.4.11 *Let L/K be an* abelian *extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. Then the breaks in the ramification filtration for the upper numbering are integers.*

Proof. See [46], V.7, Theorem 1. ■

Example 4.4.12 Consider the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$. One can compute directly (see Exercise 1) that the ramification breaks occur at $1, \ldots, n$. This will also follow from the comparison with local reciprocity (Theorem 4.4.14). □

Remark 4.4.13 The Hasse-Arf theorem is more general than we have stated here; it holds whenever L/K is a finite abelian extension of complete discretely valued fields in which the residue field extension is separable. That is, not only is there no restriction to characteristic 0, but the residue fields are not required to be finite.

At the same level of generality, one can use the Hasse-Arf theorem to deduce that the Artin conductor of a Galois representation is always integral. See [46], VI.2, Theorem 1.

Theorem 4.4.14 *Let L/K be an abelian extension of finite extensions of $\mathbb{Q}_p$ with Galois group G. Let $r_{L/K} : K^*/\operatorname{Norm}_{L/K} L^* \to G$ be the local reciprocity isomorphism. Then for each positive integer i, the inverse image of G^i in $\mathfrak{o}_K^*$ equals U_K^i.*

Proof. See [37], Theorem V.6.2. (This proof uses the Lubin-Tate construction.) ■

Exercises

1. Compute the ramification breaks for the lower and upper numbering for the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ directly from the definitions (i.e., without using local reciprocity). In particular, you should find that the breaks for the upper numbering are $1, \ldots, n$.

2. Let K be the splitting field of the polynomial $x^4 + 2x + 2$ over $\mathbb{Q}_2$. Show that in the ramification filtration on $\operatorname{Gal}(K/\mathbb{Q}_2)$, the largest break for the upper numbering occurs at $4/3$.

Hint. This example is taken from the L-Functions and Modular Forms Database. Note that in this case the Galois group is S_4.

3. Let G be the quaternion group of order 8; that is, $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Let $C = \{\pm 1\}$ be the center of G. Suppose that L/K is a totally ramified Galois extension of finite extensions of $\mathbb{Q}_2$ satisfying $\operatorname{Gal}(L/K) = G$ and $G_4 = \{1\}$. Show that

$$G = G_0 = G_1, \qquad C = G_2 = G_3$$

and deduce that

$$G^i = \begin{cases} G & i \leq 1 \\ C & 1 < i \leq \frac{3}{2} \\ \{1\} & i > \frac{3}{2}. \end{cases}$$

4.5 Making the reciprocity map explicit

It is natural to ask whether the local reciprocity map can be described more explicitly. In fact, given an explicit cocycle ϕ generating $H^2(L/K)$, we can trace through the arguments to get the local reciprocity map. However, the argument is somewhat messy, so I won't torture you with all of the details; the point is simply to observe that everything we've done can be used for explicit computations. (This observation is apparently due to Dwork.)

If you find this indigestible, you may hold out until we hit abstract class field theory. That point of view will give a different (though of course related) mechanism for computing the reciprocity map (see Section 5.2).

Initial setup

Put $G = \mathrm{Gal}(L/K)$. First recall that $G^{\mathrm{ab}} = H_T^{-2}(G, \mathbb{Z})$ is isomorphic to $H_T^{-1}(G, I_G) = I_G/I_G^2$, with $g \mapsto [g] - 1$. Next, use the exact sequence

$$0 \to M \to M[\phi] \to I_G \to 0$$

and apply the "snaking" construction: pull $[g] - 1$ back to $x_g \in M[\phi]$, take the norm to get $\prod_h x_g^h = \prod_h (x_{gh} x_h^{-1} \phi(e, h, gh))$ (switching to multiplicative notation). The x_{gh} and x_h term cancel out when you take the product, so we get $\prod_h \phi(e, h, gh) \in L^*$ as the inverse image of $g \in \mathrm{Gal}(L/K)$.

As noted above, one needs ϕ to make this truly explicit; one can get ϕ using explicit generators of L/K if you have them. For $K = \mathbb{Q}_p$, one can use roots of unity; for general K, one can use the Lubin-Tate construction. Alternatively, one can argue as in our proof that $H^2(L/K)$ is cyclic of order n; see below.

An explicit cocycle via periodicity

Let M/K be unramified of degree n; then $H^2(M/K) \to H^2(ML/K)$ is injective, and its image lies in the image of $H^2(L/K) \to H^2(ML/K)$.

Now $H^2(M/K)$ is isomorphic to $H_T^0(M/K) = K^*/\operatorname{Norm}_{M/K} M^*$, which is generated by a uniformizer $\pi \in K$. To explicate that isomorphism, we recall generally how to construct the isomorphism $H_T^0(G, M) \to H_T^2(G, M)$ for G cyclic with a distinguished generator g. Recall the exact sequence we used to produce the isomorphism in Theorem 3.4.1:

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

(Remember, G acts on both factors in $M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. The first map is $m \mapsto \sum_{h \in G} m \otimes [h]$, the second is $m \otimes [h] \mapsto m \otimes ([gh] - [h])$, and the third is $[h] \mapsto 1$.) Let $A = M \otimes_{\mathbb{Z}} I_G$ be the kernel of the third arrow, so $0 \to M \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to A \to 0$ and $0 \to A \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \to 0$ are exact.

Given $x \in H_T^0(M/K) = M^G/\operatorname{Norm}_G(M)$, lift it to $x \otimes [1]$. Now view this as a 0-cochain $\phi_0 : G \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ given by $\phi_0(h) = x \otimes [h]$. Apply d to get a 1-cocycle:

$$\phi_1(h_0, h_1) = \phi_0(h_1) - \phi_0(h_0) = x \otimes ([h_1] - [h_0])$$

which actually takes values in A. Now snake again: pull this back to a 1-cochain $\psi_1 : G^2 \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ given by

$$\psi_1(g^i, g^{i+j}) = x \otimes ([g^i] + [g^{i+1}] + \cdots + [g^{j-1}])$$

for $i, j = 0, \ldots, \#G - 1$. Apply d again: now we have a 2-cocycle $\psi_2 : G^3 \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ given by (again for $i, j = 0, \ldots, \#G - 1$)

$$\begin{aligned}
\psi_2(e, g^i, g^{i+j}) &= \psi_1(g^i, g^{i+j}) - \psi_1(e, g^{i+j}) + \psi_1(e, g^i) \\
&= x \otimes ([e] + \cdots + [g^{i-1}] + [g^i] + \cdots + [g^{i+j-1}] - [e] - \cdots - [g^{i+j-1}]) \\
&= \begin{cases} 0 & i + j < \#G \\ -x \otimes ([e] + \cdots + [g^{\#G-1}]) & i + j \geq \#G. \end{cases}
\end{aligned}$$

This pulls back to a 2-cocycle $\phi_2 : G^3 \to M$ given by

$$\phi_2(e, g^i, g^{i+j}) = \begin{cases} 0 & i+j < \#G \\ -x & i+j \geq \#G. \end{cases}$$

If you prefer, you can shift by a coboundary to get x if $i+j < \#G$ and 0 if $i+j \geq \#G$.

From a cocycle to reciprocity

Back to the desired computation. Applying this to $\mathrm{Gal}(M/K)$ acting on M^*, with the canonical generator g equal to the Frobenius, we get that $H^2(M/K)$ is generated by a cocycle ϕ with $\phi(e, g^i, g^{i+j}) = \pi$ if $i+j < \#G$ and 1 otherwise. Now push this into $H^2(ML/K)$; the general theory says the image comes from $H^2(L/K)$. That is, for $h \in \mathrm{Gal}(ML/K)$, let $f(h)$ be the integer i such that h restricted to $\mathrm{Gal}(M/K)$ equals g^i. Then there exists a 1-cochain $\rho : \mathrm{Gal}(ML/K)^2 \to (ML)^*$ such that $\phi(e, h_1, h_2h_1)/(\rho(h_1, h_2h_1)\rho(e, h_2h_1)^{-1}\rho(e, h_1))$ belongs to L^* and depends only on the images of h_1, h_2 in $\mathrm{Gal}(M/K)$. Putting $\sigma(h) = \rho(e, h)$, we thus have

$$\frac{\phi(e, h_1, h_2h_1)\sigma(h_2h_1)}{\sigma(h_2)^{h_1}\sigma(h_1)}$$

depends only on h_1, h_2 modulo $\mathrm{Gal}(ML/L)$.

The upshot: once you compute such a σ (which I won't describe how to do, since it requires an explicit description of L/K), to find the inverse image of $g \in \mathrm{Gal}(L/K)$ under the Artin map, choose a lift g_1 of g into $\mathrm{Gal}(ML/K)$, then compute

$$\prod_h \frac{\phi(e, h, gh)\sigma(gh)}{\sigma(g)^h\sigma(h)}$$

for h running over a set of lifts of the elements of $\mathrm{Gal}(L/K)$ into $\mathrm{Gal}(ML/K)$.

Chapter 5

Abstract class field theory

We now turn to an alternate method for deriving the results of local class field theory, particularly the local reciprocity law (Theorem 4.1.2). This method, based on a presentation of Artin and Tate (the method of "class formations" introduced in [1]), isolates the main cohomological inputs in the local case and gives an outline of how to proceed to global class field theory. We conclude with a preview of how the method will apply in the global case; see Section 5.4.

Caveat. In the context of abstract class field theory, we will assign certain words (e.g., **unramified**) new meanings that will coincide with their existing definitions when the abstract setup is specialized to local class field theory. We will then transfer these meanings to the global application of abstract class field theory, where we will usually use scare quotes (i.e., "unramified").

5.1 The setup of abstract class field theory

Reference. [37], IV.4-IV.6. Remember that Neukirch's cohomology groups are all Tate groups, so he doesn't put the subscript "T" on them.

Abstract multiplicative groups and the class field axiom

We first introduce an abstract analogue of the groups K^*, for K a finite extension of k, and the norm maps between them. This enables us to state a key cohomological assumption.

Definition 5.1.1 Let k be a field, let $\overline{k}$ be an algebraic extension of k, and put $G = \mathrm{Gal}(\overline{k}/k)$. Let A be a G-module; for any subextension K of $\overline{k}/k$, define $A_K = A^{\mathrm{Gal}(\overline{k}/K)}$. (In the example where k is a local field, we will take $\overline{k}$ to be the separable closure and $A = \overline{k}^*$.) ◊

Remark 5.1.2 In this discussion, we are not going to make any explicit use of the field k; we are really just working with the profinite group G. One could extend this discussion to a general profinite group G, as is done in [37], by "pretending" that the profinite group corresponds to a field and its extensions via the Galois correspondence. That is, a "field extension" of k corresponds to a closed subgroup of G; a "finite extension" of k corresponds to an open subgroup of G; and so on.

Definition 5.1.3 For L/K a finite extension of subextensions of $\overline{k}/k$, define the **norm map** $\mathrm{Norm}_{L/K} : A_L \to A_K$ by $\mathrm{Norm}_{L/K}(a) = \prod_g a^g$, where g runs over a set of right coset representatives of G_L in G_K. In the Galois case this coincides with the norm map used in the definition of the Tate cohomology groups, except that we are using multiplicative notation rather than additive notation.

For L/K an infinite extension of subextensions of $\overline{k}/k$, we don't have a well-defined norm map from A_L to A_K. By convention, however, we still write $\mathrm{Norm}_{L/K} A_L$ to mean the intersection of $\mathrm{Norm}_{M/K} A_M$ over all finite subextensions M of L/K. ◊

Definition 5.1.4 Set notation as in Definition 5.1.1. We say that A satisfies the **class field axiom** if for every *cyclic* extension L/K of finite subextensions of $\overline{k}/k$,

$$\#H_T^i(\mathrm{Gal}(L/K), A_L) = \begin{cases} [L:K] & i = 0 \\ 1 & i = -1. \end{cases}$$

Note that in general, it is not enough to impose this condition when $K = k$

Since L/K is cyclic here, Theorem 3.4.1 implies that the groups $H_T^i(\mathrm{Gal}(L/K), A_L)$ repeat with period 2. It will sometimes be convenient to work with $i = 1$ instead of $i = -1$, or with $i = 2$ instead of $i = 0$. ◊

Under the class field axiom and the other conditions of abstract class field theory, for each finite Galois extension L/K of finite subextensions of $\overline{k}/k$, we will define a canonical isomorphism

$$r_{L/K} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K / \mathrm{Norm}_{L/K} A_L$$

(Theorem 5.3.9), which will moreover satisfy some compatibilities as we vary the field extension (Proposition 5.2.10, Proposition 5.2.10). Since we've already checked the class field axiom in the example where k is a local field and $A = \overline{k}^*$, this will recover the local reciprocity law (Theorem 4.1.2).

Abstract ramification theory

We next encode the key aspects of ramification theory into an abstract framework. At the moment this has nothing to do with the abstract units; the relationship will be made when we introduce abstract valuations a bit later.

Definition 5.1.5 With notation as in Definition 5.1.1, let $d : G \to \widehat{\mathbb{Z}}$ be a continuous surjective homomorphism. The example we have in mind is when k is a local field and d is the surjection of G onto $\mathrm{Gal}(k^{\mathrm{unr}}/k) \cong \widehat{\mathbb{Z}}$.

Define the **Weil group** of k as the subgroup $d^{-1}(\mathbb{Z})$ of G. This group will play an important role in the construction of the reciprocity map (see Definition 5.2.1). ◊

We now set some more notation to mimic the example case.

Definition 5.1.6 Define the **inertia group** I_k to be the kernel of d. Define the **maximal unramified extension** k^{unr} of k to be the fixed field of I_k. Likewise, for any subextension K of $\overline{k}/k$, put $I_K = G_K \cap I_k$ and let $K^{\mathrm{unr}} = k^{\mathrm{unr}} K$ be the fixed field of I_K.

We say an extension L/K of subextensions of $\overline{k}/k$ is **unramified** if $L \subseteq K^{\mathrm{unr}}$. This implies that G_L contains I_K, necessarily as a normal subgroup, and that $G_L/I_K \subseteq G_K/I_K$ injects via d into $\widehat{\mathbb{Z}}$. Hence G_L/I_K is abelian and any finite quotient of it is cyclic; in particular, G_K is normal in G_L and $\mathrm{Gal}(L/K) = G_L/G_K$ is cyclic. (Note also that K^{unr} is the compositum of K and k^{unr}; see Example 5.1.9.) ◊

If $K \neq k$, then d need not map G_K onto $\widehat{\mathbb{Z}}$, so it will be convenient to renormalize things.

Definition 5.1.7 Put

$$d_K = \frac{1}{[\widehat{\mathbb{Z}} : d(G_K)]} d;$$

then $d_K : G_K \to \widehat{\mathbb{Z}}$ is surjective and induces an isomorphism $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \widehat{\mathbb{Z}}$.

Given a finite extension L/K of subextensions of $\overline{k}/k$, define the **inertia degree** (or **residue field degree**)

$$f_{L/K} = [d(G_K) : d(G_L)]$$

and the **ramification degree**

$$e_{L/K} = [I_K : I_L].$$

By design we have multiplicativity:

$$e_{M/K} = e_{M/L} e_{L/K}, \qquad f_{M/K} = f_{M/L} f_{L/K}.$$

Moreover, if L/K is Galois, we have an exact sequence

$$1 \to I_K/I_L \to \mathrm{Gal}(L/K) \to d(G_K)/d(G_L) \to 1,$$

so the "fundamental identity" holds:

$$e_{L/K} f_{L/K} = [L : K].$$

The fundamental identity also holds if L/K is not Galois: let M be a Galois extension of K containing L, then apply the fundamental identity to M/L and M/K and use multiplicativity. ◊

Abstract valuation theory

We next introduce an abstract analogue of the valuation maps on unit groups, which tie d and A together in a crucial way. The catch is that these valuations will be valued not in $\mathbb{Z}$ but only in $\widehat{\mathbb{Z}}$; however, this is okay because we only need them to normalize the definition of the reciprocity map.

Definition 5.1.8 With notation as in Definition 5.1.1 and Definition 5.1.5, a **henselian valuation** of A_k with respect to d is a homomorphism $v : A_k \to \widehat{\mathbb{Z}}$ such that:

1. the group $Z = \mathrm{im}(v)$ contains $\mathbb{Z}$ and satisfies $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$ for all positive integers n;
2. for every finite extension K of k, $v(\mathrm{Norm}_{K/k} A_K) = f_{K/k} Z$.

In this case, for each finite subextension K of $\overline{k}/k$, we obtain a henselian valuation $v_K : A_K \to Z$ by setting

$$v_K = \frac{1}{f_{K/k}} \mathrm{Norm}_{K/k}.$$

Then $v_K(a) = v_{K^g}(a^g)$ for any $a \in A$ and $g \in G$, and for L/K a finite extension of finite subextensions of $\overline{k}/k$, $v_K(\mathrm{Norm}_{L/K}(a)) = f_{L/K} v_L(a)$ for any $a \in A_L$. ◊

Example 5.1.9 By design, the previous conditions are satisfied in the case where:

- k is a local field of characteristic 0 and $\overline{k}$ is its algebraic closure;
- $A = \overline{k}^*$ (the class field axiom is confirmed by Lemma 1.2.3 for H_T^1 and Proposition 4.2.11 for H_T^0);
- $d : \mathrm{Gal}(\overline{k}/k) \to \widehat{\mathbb{Z}}$ the map coming from the identification of $\mathrm{Gal}(k^{\mathrm{unr}}/k)$ with $\widehat{\mathbb{Z}}$;
- $v : A_k \to \widehat{\mathbb{Z}}$ is the composition of the valuation $k^* \to \mathbb{Z}$ with the inclusion $\mathbb{Z} \to \widehat{\mathbb{Z}}$.

One piece of content in this statement is the assertion that for any finite extension K of k, $K^{\mathrm{unr}} \subseteq Kk^{\mathrm{unr}}$. This holds because for any finite unramified extension L of K, we can write $L = KL_0$ where L_0 is the unramified extension of k with the same residue field as L. □

Example 5.1.10 A basic example of these constructions occurs for k finite; see Exercise 1. A closely related example can be obtained from Example 5.1.9 by replacing the algebraic closure of k with its maximal unramified subextension. □

Remark 5.1.11 Suppose that we have an instance of Definition 5.1.8. Then for any $c \in \widehat{\mathbb{Z}}^*$, the map v is also a henselian valuation of A_k with respect to cd, but the definition of the reciprocity map will be affected; see Exercise 3.

Now suppose further that $cZ = Z$. Then cv is also a henselian valuation of A_k with respect to cd, and in this case the definition of the reciprocity map will be unaffected; see Exercise 4.

Cohomology of units

Before defining the reciprocity map, we collect some direct consequences of the class field axiom. These are very similar to arguments we used in the proof of local reciprocity except that there, we used the cohomology of unramified extensions to establish the class field axiom, whereas here we are moving information in the opposite direction!

Hypothesis 5.1.12 *For the remainder of Chapter 5, fix k, A, d, v as in Definition 5.1.1, Definition 5.1.5, and Definition 5.1.8. In particular, A satisfies the class field axiom and v is a henselian valuation of A_k with respect to d.*

Definition 5.1.13 For any finite subextension K of $\overline{k}/k$, define the **unit subgroup** U_K as the set of $u \in A_K$ with $v_K(u) = 0$; this definition extends naturally to infinite subextensions. We say that $\pi \in A_K$ is a **uniformizer** for K if $v_K(\pi) = 1$. ◊

Proposition 5.1.14 *Under Hypothesis 5.1.12, let L/K be an unramified extension of finite subextensions of $\overline{k}/k$.*

1. *The groups $H_T^i(\mathrm{Gal}(L/K), U_L)$ are all trivial.*
2. *The group $H_T^0(\mathrm{Gal}(L/K), A_L)$ is cyclic, generated by any uniformizer π_L for L.*

Proof. We'll drop $\mathrm{Gal}(L/K)$ from the notation, because it's the same group throughout the proof. Keep in mind that an unramified extension is always Galois and cyclic, so we can apply periodicity of Tate groups (Theorem 3.4.1) and Herbrand quotients.

Consider the short exact sequence

$$0 \to U_L \to A_L \to A_L/U_L \to 0.$$

In this sequence, A_L/U_L is isomorphic to $Z = \mathrm{im}(v)$ with trivial group action, so $H_T^0(Z) = Z/\operatorname{Norm}(Z)$ is cyclic of order $[L : K]$ generated by π_L and $H_T^{-1}(Z) = \ker(\mathrm{Norm})$ is trivial. Using the class field axiom, we see that the long exact sequence in Tate groups looks like

$$1 = H_T^{-1}(A_L/U_L) \to H_T^0(U_L) \to H_T^0(A_L) \to H_T^0(A_L/U_L) \to H_T^1(U_L) \to H_T^1(A_L) = 1$$

and the two groups in the middle have the same order. It is thus enough to show that one of the outer groups is trivial, as then the middle map will be an isomorphism.
We have now reduced to checking that $H_T^1(U_L) = 1$. Here is where we use that L/K is unramified, not just cyclic: this means that any uniformer of K is also a uniformizer of L, which allows us to split the surjection $A_L \to A_L/U_L$ of $\mathrm{Gal}(L/K)$-modules. This in turn means that $H_T^1(U_L)$ is a direct summand of $H_T^1(A_L)$, and the latter vanishes by the class field axiom. ■

Corollary 5.1.15 *Under Hypothesis 5.1.12, for L/K an unramified extension of finite subextensions of $\overline{k}/k$, then $U_K = \operatorname{Norm}_{L/K} U_L$. (Remember, this makes sense even if L/K is not finite!)*

Proof. Apply the $i = 0$ case of Proposition 5.1.14 to each finite subextension of L/K. ■

Exercises

1. Show that the hypotheses of abstract class field theory (i.e., the class field axiom and the conditions on a henselian valuation) are satisfied in the following case:

- k is a finite field and $\overline{k}$ is its algebraic closure;
- $d : \mathrm{Gal}(\overline{k}/k) \to \widehat{\mathbb{Z}}$ is the usual isomorphism;
- A is the group $\mathbb{Z}$ with the trivial action;
- $v : A_k \to \widehat{\mathbb{Z}}$ is the inclusion of $\mathbb{Z}$ into its profinite completion.

5.2 The abstract reciprocity map

We next define the reciprocity map in abstract class field theory (Definition 5.2.6). As a bonus, this definition will give an explicit recipe for computing the reciprocity map in local class field theory, but we will not expand on this point.

Construction of the reciprocity map

In order to define a candidate $r : \mathrm{Gal}(L/K) \to A_K/\operatorname{Norm}_{L/K} A_L$ for the reciprocity map, we must first give a partial definition using a different domain. See Remark 5.2.9 for motivation.

Definition 5.2.1 Under Hypothesis 5.1.12, let L/K be a Galois extension of finite subextensions of $\overline{k}/k$. Let H be the semigroup of $g \in \mathrm{Gal}(L^{\mathrm{unr}}/K)$ such

that $d_K(g)$ is a positive integer. Define the map

$$r' : H \to A_K / \operatorname{Norm}_{L/K} A_L$$

as follows. For $g \in \operatorname{Gal}(L^{\mathrm{unr}}/K)$, let M be the fixed field of g, so that

$$e(M/K) = e((M \cap L)/K), \qquad f(M/K) = d_K(g).$$

We may set $r'(g) = \operatorname{Norm}_{M/K}(\pi_M)$ for some uniformizer π_M for M, once we check that this doesn't depend on the choice of π_M. To wit, if π'_M is another uniformizer for M, then $\pi_M/\pi'_M \in U_L$ belongs to $\operatorname{Norm}_{L^{\mathrm{unr}}/L} U_{L^{\mathrm{unr}}}$ by Corollary 5.1.15, so $\operatorname{Norm}_{M/K}(\pi_M/\pi'_M)$ belongs to $\operatorname{Norm}_{L^{\mathrm{unr}}/K} U_{L^{\mathrm{unr}}} \subseteq \operatorname{Norm}_{L/K} U_L$. So at least r' is now a well-defined map, if not yet a semigroup homomorphism. ◊

Remark 5.2.2 Before getting into the weeds, let's make some other observations about Definition 5.2.1.

First, r' is invariant under conjugation: if we replace g by $h^{-1}gh$, then its fixed field M is replaced by M^h and we can take the uniformizer π_M^h.

Next, if $g \in H$ is actually in $\operatorname{Gal}(L^{\mathrm{unr}}/L)$, then $r'(g) \in \operatorname{Norm}_{L/K} A_L$. In that case, M contains L, so $r'(g) = \operatorname{Norm}_{M/K}(\pi_M)$ can be rewritten as $\operatorname{Norm}_{L/K} \operatorname{Norm}_{M/L}(\pi_M) \in \operatorname{Norm}_{L/K} A_L$. That is, if r' were known to be multiplicative, it would induce a group homomorphism from $\operatorname{Gal}(L/K)$ to $A_K/\operatorname{Norm}_{L/K} A_L$.

The remaining difficulty is to check that r' is multiplicative. The issue here is that the definition of $r'(g)$ involves taking the norm from a field extension that depends on g, so it is hopeless to directly compare different values of g. Instead, we rewrite the definition in a more uniform manner.

Proposition 5.2.3 *With notation as in Definition 5.2.1, put $n = d_K(g)$ and choose $\phi \in H$ with $d_K(\phi) = 1$. Then for $x \in A_M$,*

$$\operatorname{Norm}_{M/K}(x) = \operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(x x^{\phi} \cdots x^{\phi^{n-1}}).$$

Proof. Put $U = M \cap K^{\mathrm{unr}}$, so that $\operatorname{Norm}_{M/K} = \operatorname{Norm}_{U/K} \circ \operatorname{Norm}_{M/U}$. The group $\operatorname{Gal}(U/K)$ is of order n generated by ϕ, so for $y \in A_U$ we have $\operatorname{Norm}_{U/K}(y) = y y^{\phi} \cdots y^{\phi^{n-1}}$. Meanwhile, on A_M we can view $\operatorname{Norm}_{M/U}$ as the restriction of $\operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}$, so $\operatorname{Norm}_{M/U}(x) = \operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(x)$. By taking $y = \operatorname{Norm}_{M/U}(x)$ and rewriting y^{ϕ^i} as $\operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(x)^{\phi^i} = \operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(x^{\phi^i})$, we deduce the claim. ■

Using the formula from Proposition 5.2.3, we can now establish multiplicativity, following [37], Proposition IV.5.5.

Lemma 5.2.4 *With notation as in Definition 5.2.1, put $G = \operatorname{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}})$ and choose $\phi \in H$ with $d_K(\phi) = 1$. If $x \in H_0(G, U_M)$ is fixed by ϕ, then $\operatorname{Norm}_G(x)$ vanishes in $H^0(G, U_M)$.*

Proof. By hypothesis, x is the class of some $u \in U_M$ for which there exist $u_1, \dots, u_r \in U_M$ and $\tau_1, \dots, \tau_r \in G$ such that

$$u^{\phi - 1} = \prod_{i=1}^{r} u_i^{\tau_i - 1}.$$

Put $n = [M : K]$ and $\sigma = \phi^n$, and let Σ be the fixed field of σ, which contains M. Let Σ_n be the unramified extension of Σ of degree n; it is the fixed field of σ^n. Since $H^0_T(\operatorname{Gal}(\Sigma_n/\Sigma), U_{\Sigma_n})$ vanishes by Proposition 5.1.14, we can find

$\tilde{u}, \tilde{u}_i \in U_{\Sigma_n}$ such that

$$u = \mathrm{Norm}_{\Sigma_n/\Sigma}(\tilde{u}) = \tilde{u}\tilde{u}^{\sigma} \cdots \tilde{u}^{\sigma^{n-1}}$$
$$u_i = \mathrm{Norm}_{\Sigma_n/\Sigma}(\tilde{u}_i) = \tilde{u}_i\tilde{u}_i^{\sigma} \cdots \tilde{u}_i^{\sigma^{n-1}}.$$

Since $H_T^{-1}(\mathrm{Gal}(\Sigma_n/\Sigma), U_{\Sigma_n})$ vanishes by Proposition 5.1.14 again, we can find $\tilde{y} \in U_{\Sigma_n}$ with

$$\tilde{u}^{\phi-1} / \prod_{i=1}^{r} \tilde{u}_i^{\tau_i - 1} = \tilde{y}^{\sigma-1},$$

and so (because $\sigma = \phi^n$)

$$\tilde{u}^{\phi-1} = (\tilde{y}\tilde{y}^{\phi} \cdots \tilde{y}^{\phi^{n-1}})^{\phi-1} \prod_{i=1}^{r} \tilde{u}_i^{\tau_i - 1}.$$

Applying Norm_G yields

$$\mathrm{Norm}_G(\tilde{u})^{\phi-1} = \mathrm{Norm}_G(\tilde{y}\tilde{y}^{\phi} \cdots \tilde{y}^{\phi^{n-1}})^{\phi-1}.$$

That is, if we set

$$z = \mathrm{Norm}_G(\tilde{u}) / \mathrm{Norm}_G(\tilde{y}\tilde{y}^{\phi} \cdots \tilde{y}^{\phi^{n-1}}),$$

we have $z^{\phi-1} = 1$ and so $z \in U_K$. Put

$$y = \tilde{y}\tilde{y}^{\sigma} \cdots \tilde{y}^{\sigma^n - 1} = \mathrm{Norm}_{\Sigma_n/\Sigma}(\tilde{y}) \in U_{\Sigma};$$

using Proposition 5.2.3 we obtain

$$\begin{aligned} \mathrm{Norm}_G(u) &= \mathrm{Norm}_G(\tilde{u}\tilde{u}^{\sigma} \cdots \tilde{u}^{\sigma^{n-1}}) \\ &= \mathrm{Norm}_G(yy^{\phi} \cdots y^{\phi^{n-1}}) z^n \\ &= \mathrm{Norm}_{\Sigma/K}(y) \, \mathrm{Norm}_{M/K}(u) \in \mathrm{Norm}_{M/K} U_M, \end{aligned}$$

proving the claim. (Compare [37], Lemma IV.5.4.) ■

Lemma 5.2.5 *The map $r' : H \to A_K / \mathrm{Norm}_{L/K} A_L$ exhibited in Definition 5.2.1 is a homomorphism of semigroups.*

Proof. Let $g_1, g_2 \in H$ be arbitrary and put $g_3 = g_1 g_2$. Let M_i be the fixed field of g_i, let $\pi_i \in A_{M_i}$ be a uniformizer of M_i, and put $\rho_i = r'(g_i) = \mathrm{Norm}_{M_i/K}(\pi_i) \in A_K$. Put $\rho = \rho_1\rho_2/\rho_3$; note that

$$v_K(\rho_i) = f(M_i/K) v_{M_i}(\pi_i) = f(M_i/K) = d_K(g_i),$$

which implies that $v_K(\rho) = 0$ and hence $\rho \in U_K$. Our goal is to check that $\rho \in \mathrm{Norm}_{L/K} A_L$; our plan is to rephrase this as a relation among units, to which Lemma 5.2.4 will apply.

We first make an adjustment at the level of group elements. Put $G = \mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}})$. Choose $\phi \in H$ such that $d_K(\phi) = 1$. Put $d_i = d_K(g_i)$ and $\tau_i = g_i^{-1}\phi^{d_i} \in G$; then

$$\tau_3 = g_2^{-1} g_1^{-1} \phi^{d_1 + d_2} = g_2^{-1} \phi^{d_2} (\phi^{-d_2} g_1 \phi^{d_2})^{-1} \phi^{d_1}.$$

It will be convenient to replace g_1 and τ_1 with

$$g_1' = \phi^{-d_2} g_1 \phi^{d_2}, \qquad \tau_1' = (g_1')^{-1} \phi^{g_1},$$

so that $\tau_1'\tau_2 = \tau_3$. We correspondingly define M_1' to be the fixed field of g_1' and set $\pi_1' = \pi_1^{\phi^{n_2}} \in A_{M_1'}$, noting that $\mathrm{Norm}_{M_1'/K}(\pi_1') = \mathrm{Norm}_{M_1/K}(\pi_1) = \rho_1$. Let N be a finite subextension of L^{unr}/L containing M_1, M_2, M_3, M_1'. Set

$$\sigma_i = \pi_i \pi_i^{\phi} \cdots \pi_i^{\phi^{d_i-1}}, \qquad \sigma_1' = (\pi_1')(\pi_1')^{\phi} \cdots (\pi_1')^{\phi^{d_1-1}}$$

and $u = \sigma_1'\sigma_2/\sigma_3 \in U_N$; by Proposition 5.2.3 we have $\rho = \mathrm{Norm}_G(u)$. By defining

$$u_1 = (\pi_1')^{1-\tau_2}, u_2 = \pi_2/\pi_1', u_3 = \pi_3/\pi_1' \in U_N$$

and using the equality $\tau_1'\tau_2 = \tau_3$, we compute that

$$u^{\phi-1} = (\pi_1')^{\tau_1'-1}\pi_2^{\tau_2-1}/\pi_3^{\tau_3-1} = u_1^{\tau_1'-1}u_2^{\tau_2-1}/u_3^{\tau_3-1}$$

vanishes in $H_0(G, U_N)$; by Lemma 5.2.4 we obtain $\mathrm{Norm}_G(u) \in \mathrm{Norm}_{N/K} U_N$, proving the claim. ■

Definition 5.2.6 With notation as in Definition 5.2.1, by combining Definition 5.2.1, Remark 5.2.2, and Lemma 5.2.5, we obtain a semigroup homomorphism $r' : H \to A_K/\mathrm{Norm}_{L/K} A_L$ which kills $\mathrm{Gal}(L^{\mathrm{unr}}/L)$ and thus induces a homomorphism $r = r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Norm}_{L/K} A_L$. We call $r_{L/K}$ the **reciprocity map**. ◊

Here are some consequences of the construction whose proofs are left to the reader.

Proposition 5.2.7 *Under Hypothesis 5.1.12, if L/K and L'/K' are Galois extensions of finite subextensions of $\overline{k}/k$ such that $K \subseteq K'$ and $L \subseteq L'$, then the diagram in Figure 5.2.8 commutes.*

$$\begin{array}{ccc} \mathrm{Gal}(L'/K')^{\mathrm{ab}} & \xrightarrow{r_{L'/K'}} & A_{K'}/\mathrm{Norm}_{L'/K'} A_{L'} \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Norm}_{K'/K}} \\ \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{r_{L/K}} & A_K/\mathrm{Norm}_{L/K} A_L \end{array}$$

Figure 5.2.8

Proof. See Exercise 1. ■

Remark 5.2.9 Note that Proposition 5.2.7 dictates the form of Definition 5.2.1: we want to be able to compute the map $r : \mathrm{Gal}(L/K) \to A_K/\mathrm{Norm}_{L/K} A_L$ by first computing the map $r : \mathrm{Gal}(ML/M) \to A_M/\mathrm{Norm}_{ML/M} A_{ML}$, which should take Frobenius to a uniformizer (as ML/M is an unramified extension), and then applying $\mathrm{Norm}_{M/L}$. We will use this picture again in Lemma 5.3.2.

Proposition 5.2.10 *Under Hypothesis 5.1.12, if L/K is a Galois extension of finite subextensions of $\overline{k}/k$ and K' is an intermediate field, then the diagram in Figure 5.2.11 commutes. Here $V : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/K')^{\mathrm{ab}}$ denotes the transfer map for the inclusion $\mathrm{Gal}(L/K') \subseteq \mathrm{Gal}(L/K)$ (Theorem 2.3.7).*

$$\begin{array}{ccc} \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{r_{L/K}} & A_K/\mathrm{Norm}_{L/K} A_L \\ \downarrow{\scriptstyle V} & & \downarrow \\ \mathrm{Gal}(L/K')^{\mathrm{ab}} & \xrightarrow{r_{L/K'}} & A_{K'}/\mathrm{Norm}_{L/K'} A_L \end{array}$$

Figure 5.2.11

Proof. See Exercise 2. ■

Exercises

1. Prove Proposition 5.2.7.

Hint. See [37], Proposition IV.5.8.

2. Prove Proposition 5.2.10.

Hint. See [37], Proposition IV.5.9.

3. Under Hypothesis 5.1.12, choose $c \in \widehat{\mathbb{Z}}^*$ and let $s_{L/K}$ be the reciprocity map defined using cd instead of d. Show that $s_{L/K} = c^{-1} r_{L/K}$.

4. Under Hypothesis 5.1.12, choose $c \in \widehat{\mathbb{Z}}^*$ which acts on $\mathrm{im}(v)$, and let $s_{L/K}$ be the reciprocity map defined using cd, cv instead of d, v. Show that $s_{L/K} = r_{L/K}$.

5.3 The theorems of abstract class field theory

We now establish that the reciprocity map is an isomorphism (Theorem 5.3.9). We also obtain an analogue of the norm limitation theorem (Corollary 5.3.11) and some tools which will help with the existence theorem (Remark 5.3.14).

Proof of the reciprocity law

Our goal is to prove that the homomorphism $r_{L/K}$ from Definition 5.2.6 induces an isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K / \mathrm{Norm}_{L/K} A_L$. Any resemblance with the proof of the local reciprocity law is not at all coincidental!

Lemma 5.3.1 *Under Hypothesis 5.1.12, for L/K an unramified extension of finite subextensions of $\overline{k}/k$, $r_{L/K} : \mathrm{Gal}(L/K) \to A_K / \mathrm{Norm}_{L/K} A_L$ is an isomorphism sending the Frobenius of $\mathrm{Gal}(L/K)$ to a uniformizer of K.*

Proof. Let $g \in \mathrm{Gal}(L/K)$ be the Frobenius and choose $h \in \mathrm{Gal}(L^{\mathrm{unr}}/K)$ lifting g. Then the fixed field of h is K itself, and from the definition of r', $r(g) = r'(h)$ is a uniformizer of K. By Proposition 5.1.14, $r(g)$ generates $H^0(\mathrm{Gal}(L/K), A_L)$. By the class field axiom, $r_{L/K}$ maps between two groups of the same order, and the previous paragraph implies that the map is surjective. It is thus an isomorphism. ■

Lemma 5.3.2 *Under Hypothesis 5.1.12, for L/K a cyclic, totally ramified extension of finite subextensions of $\overline{k}/k$, the map $r_{L/K} : \mathrm{Gal}(L/K) \to A_K / \mathrm{Norm}_{L/K} A_L$ is an isomorphism.*

Proof. Put $n = [L : K]$. The extension L^{unr}/K is the compositum of two linearly disjoint extensions L/K and K^{unr}/K, so its Galois group is canonically a product $\mathrm{Gal}(L/K) \times \mathrm{Gal}(K^{\mathrm{unr}}/K)$. Let g be a generator of the first factor (which we can also identify with $\mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}})$) and let ϕ be a generator of the second factor with $d_K(\phi) = 1$. Put $\tau = g\phi$ and let M be the fixed field of τ. Let N be the compositum of L and M and put $N_0 = N \cap K^{\mathrm{unr}}$. We now have the field diagram Figure 5.3.3 in which each line denotes a $\mathbb{Z}/n\mathbb{Z}$-extension, the dashed lines represent unramified extensions, and each label indicates one or more generators of the Galois group g.

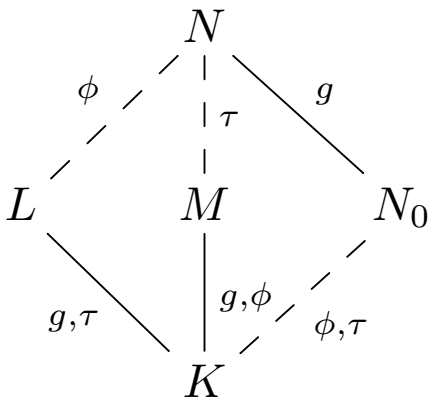

Figure 5.3.3

Pick uniformizers π_L and π_M of L and M, respectively. Since $d_K(\tau) = 1$, by Proposition 5.2.3 we have $r_{L/K}(g) = \mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\pi_M)$.
Let j be the order of $r_{L/K}(g)$ in $A_K/\mathrm{Norm}_{L/K} A_L$ and put $u = \pi_M^j/\pi_L^j \in U_N$. Since both $\mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\pi_M^j)$ and $\mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\pi_L^j) = \mathrm{Norm}_{L/K}(\pi_L^j)$ belong to $\mathrm{Norm}_{L/K} A_L$, we can choose $v \in A_L$ such that

$$\mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(u) = \mathrm{Norm}_{L/K}(v) = \mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(v).$$

Since $\mathrm{Norm}_{L/K}(v) \in A_K \cap U_N = U_K$, we must have $v \in U_L$.
Applying the class field axiom to N/N_0 yields

$$0 = H_T^{-1}(\mathrm{Gal}(N/N_0), A_N) = \frac{\ker(\mathrm{Norm}_{N/N_0} : A_N \to A_{N_0})}{\{a^{g-1} : a \in A_N\}}.$$

Since $\mathrm{Norm}_{N/N_0}(u/v) = \mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(u/v) = 1$, we can write u/v in the form $a^{g-1} = a^g/a$ for some $a \in A_N$. Then

$$(\pi_L^j v)^{g-1} = (\pi_L^j v)^{\tau-1} = (\pi_M^j v/u)^{\tau-1} = (v/u)^{\tau-1} = (a/a^\tau)^{g-1}.$$

If we put $x = (\pi_L^j v)(a^\tau/a)$, then $x^g = x$ and so $x \in A_{N_0}$. Hence

$$j = v_N(x) = n v_{N_0}(x) \in n\widehat{\mathbb{Z}}.$$

That is, the order of $r_{L/K}(g)$ in $A_K/\mathrm{Norm}_{L/K} A_L$ is divisible by n in $\widehat{\mathbb{Z}}$, and hence also in $\mathbb{Z}$.
By the class field axiom, $r_{L/K}$ maps between two groups of the same order n, and the previous paragraph implies that the map has image of size at least n. It is thus an isomorphism. ■

Before continuing, we record a key commutative diagram which will be the scene of a lot of diagram-chasing.

Remark 5.3.4 For L/K a Galois extension of finite subextensions of $\overline{k}/k$ and M/K a Galois subextension, the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(L/M) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle r_{L/M}} & & \downarrow{\scriptstyle r_{L/K}} & & \downarrow{\scriptstyle r_{M/K}} & & \\
 & & A_M/\mathrm{Norm}_{L/M} A_L & \xrightarrow{\mathrm{Norm}_{M/K}} & A_K/\mathrm{Norm}_{L/K} A_L & \longrightarrow & A_K/\mathrm{Norm}_{M/K} A_M & \longrightarrow & 1
\end{array}$$

Figure 5.3.5

commutes (thanks to Proposition 5.2.7) and the rows are exact.

Lemma 5.3.6 *Under Hypothesis 5.1.12, for L/K an abelian extension of finite subextensions of $\overline{k}/k$, the map $r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Norm}_{L/K} A_L$ is an isomorphism.*

Proof. If L/K is cyclic of prime order, We induct on $[L : K]$. then either it is unramified or totally ramified, and we already know $r_{L/K}$ is an isomorphism in those cases (by Lemma 5.3.1 or Lemma 5.3.2, respectively). Otherwise, let M be a subextension of L/K. Then diagram chasing through Figure 5.3.5 gives that $r_{L/K}$ is surjective. If L/K is cyclic, then the class field axiom implies that $r_{L/K}$ is a map between two groups of the same order, and hence must be an isomorphism. Otherwise, we see from Figure 5.3.5 again that the kernel of $r_{L/K}$ lies in the kernel of $\mathrm{Gal}(L/K) \to \mathrm{Gal}(N/K)$ for *every* cyclic subextension N of L/K. Since L/K is abelian and not cyclic, the intersection of these kernels is trivial. Thus $r_{L/K}$ is also injective, so is an isomorphism. ■

Lemma 5.3.7 *Under Hypothesis 5.1.12, for L/K a Galois extension of finite subextensions of $\overline{k}/k$, the homomorphism $r_{L/K}$ from Definition 5.2.6 induces an injection $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\mathrm{Norm}_{L/K} A_L$.*

Proof. Let M be the maximal abelian subextension of L/K. We have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{r_{L/K}} & A_K/\mathrm{Norm}_{L/K} A_L \\ \downarrow & & \downarrow \\ \mathrm{Gal}(M/K) & \xrightarrow{r_{M/K}} & A_K/\mathrm{Norm}_{M/K} A_M \end{array}$$

Figure 5.3.8

in which the left vertical arrow and bottom horizontal arrows are isomorphisms (the latter by Lemma 5.3.6). Thus the composite $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\mathrm{Norm}_{M/K} A_M$ is an isomorphism, so $r_{L/K}$ must be injective. ■

Theorem 5.3.9 Reciprocity law. *Under Hypothesis 5.1.12, for each Galois extension L/K of finite subextensions of $\overline{k}/k$, the homomorphism $r_{L/K}$ from Definition 5.2.6 induces an isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\mathrm{Norm}_{L/K} A_L$.*

Proof. The map in question is injective by Lemma 5.3.7, so it only remains to check that $r_{L/K}$ itself is surjective. If L/K is solvable, we may deduce surjectivity from Lemma 5.3.6 by induction on $[L : K]$ again by a diagram chase on Figure 5.3.5.

For general L/K, we instead check that $r_{L/K}$ becomes a surjection upon restriction to p-Sylow subgroups for each prime p. That is, for M the fixed field of a Sylow p-subgroup of $\mathrm{Gal}(L/K)$ and S_p the Sylow p-subgroup of $A_K/\mathrm{Norm}_{L/K} A_L$, the composition

$$\mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \overset{r_{L/K}}{\to} A_K/\mathrm{Norm}_{L/K} A_L \to S_p$$

is surjective. (Compare the proof of Lemma 4.3.2.)

Here some caution is required because M/K need not be Galois, so we cannot draw the full diagram Figure 5.3.5. However, the left square in that diagram still makes sense and commutes. Meanwhile, we may apply the previous paragraph to see that the left vertical arrow $r_{L/M}$ is an isomorphism. Now note that the composition $A_K \subseteq A_M \overset{\mathrm{Norm}_{M/K}}{\to} A_K$ is multiplication by $[M : K]$, which is coprime to p; it follows that the bottom horizontal arrow induces a surjection

of Sylow p-subgroups. (One can also apply Proposition 5.2.10 here.) ■

Remark 5.3.10 Alternatively, one can derive Theorem 5.3.9 by an argument closer to what we did in local class field theory. In this approach, one first simulates the proofs of Proposition 4.2.17 and Proposition 4.2.18 to show that $H^2(\mathrm{Gal}(L/K), A_L)$ is cyclic of order $[L : K]$; the latter argument ends up being quite similar to the proof of Lemma 5.3.2, with the role of Theorem 90 (Lemma 1.2.3) being played by the H_T^{-1} aspect of the class field axiom. One must then check that the reciprocity map agrees with the map given by Tate's theorem Theorem 4.3.1; we leave the details to the interested reader, but see Section 7.5 for a similar argument in the setting of global class field theory.

This directly implies a version of the norm limitation theorem.

Corollary 5.3.11 Norm limitation theorem. *Under Hypothesis 5.1.12, for L/K an arbitrary extension of finite subextensions of $\overline{k}/k$ and M the maximal abelian subextension of L/K, we have* $\mathrm{Norm}_{L/K} A_L = \mathrm{Norm}_{M/K} A_M$. *In particular,* $\mathrm{Norm}_{L/K} A_L$ *depends only on the Galois closure of L/K.*

Proof. The only issue is the inclusion $\mathrm{Norm}_{M/K} A_M \subseteq \mathrm{Norm}_{L/K} A_L$, which we are free to check after enlarging L (as long as we do not change M). We may thus assume that L/K is Galois.
By Proposition 5.2.7 and Theorem 5.3.9, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K)^{\mathrm{ab}} & \longrightarrow & A_K/\mathrm{Norm}_{L/K} A_L \\ \| & & \downarrow \\ \mathrm{Gal}(M/K)^{\mathrm{ab}} & \longrightarrow & A_K/\mathrm{Norm}_{M/K} A_M \end{array}$$

Figure 5.3.12

in which the horizontal arrows are isomorphisms. This implies the claim. ■

By similar logic, we also obtain a uniqueness result.

Corollary 5.3.13 *Under Hypothesis 5.1.12, let L_1/K and L_2/K be abelian extensions of finite subextensions of $\overline{k}/k$. If* $\mathrm{Norm}_{L_1/K} A_{L_1} = \mathrm{Norm}_{L_2/K} A_{L_2}$, *then $L_1 = L_2$.*

Proof. The compositum $L = L_1 L_2$ is also a finite abelian extension of K. By Proposition 5.2.7, $\mathrm{Gal}(L_1/K) \cong A_K/\mathrm{Norm}_{L_1/K} A_{L_1}$ and $\mathrm{Gal}(L_2/K) \cong \mathrm{Norm}_{L_2/K} A_{L_2}$ must be the same quotient of $\mathrm{Gal}(L/K) \cong A_K/\mathrm{Norm}_{L/K} A_L$, which forces $L_1 = L_2$. ■

Remark 5.3.14 In a similar vein, note that every subgroup of A_K containing a subgroup of the form $\mathrm{Norm}_{M/K} A_M$ for some finite extension M/K must itself occur as $\mathrm{Norm}_{L/K} A_L$ for some finite (and even abelian) extension L/K. Consequently, proving an analogue of the existence theorem in this setting amounts to computing the intersection of the groups $\mathrm{Norm}_{M/K} A_M$.

Following [37], one can view the groups $\mathrm{Norm}_{M/K} A_M$ as the open subgroups for a certain topology on A_K, called the **norm topology**. One can then assert that $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is isomorphic to the profinite completion of A_K, or equivalently its maximal Hausdorff quotient, for the family of quotients by open subgroups in the norm topology.

5.4 A look ahead

We conclude our treatment of abstract class field theory by asking ourselves: what does the construction of an abstract reciprocity law tell us about the

global Artin reciprocity law (Theorem 2.2.6)? See Section 6.5 for a continuation of this discussion with more of the details filled in.

Replacing the multiplicative group

For L/K a finite abelian extension of number fields, we need to compare $\mathrm{Gal}(L/K)$ to a generalized ideal class group of K. This means that the group A must somehow be related to ideal classes. You might try taking the group of fractional ideals in L, then taking the direct limit over all finite extensions L of K. In this case, we would have to find $H^i(\mathrm{Gal}(L/K), A_L)$ for A_L the group of fractional ideals in L, where L/K is cyclic and $i = 0, -1$. Unfortunately, these groups are not so well-behaved as that!

The cohomology groups would behave better if A_L were "complete" in some sense, in the way that K^* is complete when K is a local field. But there is no good reason to distinguish one place over another in the global case. So we're going to make the target group A by "completing K^* at all places simultaneously".

Replacing the unramified extensions and the valuation

Even without A, I can at least tell you what d is going to be over $\mathbb{Q}$. To begin with, note that there is a surjective map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$ that turns an automorphism into its action on roots of unity. The latter group is unfortunately isomorphic to the multiplicative group $\widehat{\mathbb{Z}}^*$ rather than the additive group $\widehat{\mathbb{Z}}$, but this is a start. To make more progress, write $\widehat{\mathbb{Z}}$ as the product $\prod_p \mathbb{Z}_p$, so that $\widehat{\mathbb{Z}}^* \cong \prod_p \mathbb{Z}_p^*$. Then recall that there exist isomorphisms

$$\mathbb{Z}_p^* \cong \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p & p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_p & p = 2. \end{cases}$$

In particular, $\mathbb{Z}_p^*$ modulo its torsion subgroup is isomorphic to $\mathbb{Z}_p$, but not in a canonical way. Paying this no mind, let us choose an isomorphism for each p and then obtain a surjective map $\widehat{\mathbb{Z}}^* \to \widehat{\mathbb{Z}}$. Composing, we get a surjective map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}$ which in principle depends on some choices, but the ultimate statements of the theory will be independent of these choices. (Note that in this setup, every "unramified" extensions of a number field is a subfield of a cyclotomic extension, but not conversely.)

As for the valuation v, this will be more straightforward. In the situation we end up considering, the group $A_{\mathbb{Q}}$ will end up having a natural map to $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$, which we can then use to map to $\widehat{\mathbb{Z}}$. This again involves an artificial choice, but as long as we make the *same* artificial choice as we did for d, we get the necessary compatibility between d and v.

Further remarks

Remark 5.4.1 In the function field setting, we have a much more straightforward alternative to the use of cyclotomic extensions: we may take the map to the Galois group of the base finite field. The point is that in this case we have an ample supply of *everywhere unramified* extensions of the base field (without quotation marks).

In the number field setting, using cyclotomic extensions as a proxy for abelian, everywhere unramified extensions is a rather productive idea even outside of class field theory. For one, it is the central premise of **Iwasawa theory**, in which one studies the behavior of class fields in certain towers of

number fields and their relationship with p-adic L-functions (and other related concepts). For another, it is the starting point of **p-adic Hodge theory**, in which one studies the relationship between different cohomology theories associated to algebraic varieties over local fields.

Remark 5.4.2 One can also apply the framework of abstract class field theory to prove some forms of **higher-dimensional class field theory**, taking the group A to be something coming from algebraic K-theory. See the remark at the end of [37], IV.6.

Chapter 6

The adelic formulation

The p-adic numbers, and more general local fields, were introduced into number theory as a way to translate local facts about number fields (i.e., facts concerning a single prime ideal) into statements of a topological flavor. To prove the statements of class field theory, we need an analogous global construction. To this end, we construct a topological object that includes all of the completions of a number field, including both the archimedean and nonarchimedean ones. This object will be the ring of **adèles**, and it will lead us to the right target group for use in the abstract class field theory we have just set up.

Remark 6.0.1 Spelling note. There is a lack of consensus regarding the presence or absence of accents in the words *adèle* and *idèle*. The term *idèle* is thought to be a contraction of "ideal element"; it makes its first appearance, with the accent, in Chevalley's 1940 paper [6]. The term *adèle* appeared in the 1950s, possibly as a contraction of "additive idèle"; it appears to have been suggested by Weil as a replacement for Tate's term "valuation vector" and Chevalley's term "repartition". Based on this history, we have opted for the accented spellings here.

6.1 Adèles

Reference. [36]; [37], VI.1 and VI.2; [33], VII.

Lattices of number fields

The basic idea is that we want some sort of "global completion" of a number field K. Let us first recall an older version of this idea: Minkowski's construction of the Euclidean lattice associated to a number field. We follow [37], I.5.

Definition 6.1.1 Let K be a number field of degree n. It then has n distinct embeddings $\tau : K \to \mathbb{C}$. The product embedding

$$j : K \to \prod_{\tau} \mathbb{C}, \qquad a \mapsto (\tau(a))_{\tau}$$

induces an isomorphism of $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$ with $\prod_{\tau} \mathbb{C}$.

The ring $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$ admits an involution F which fixes K and acts on $\mathbb{C}$ via complex conjugation. The corresponding action on $\prod_{\tau} \mathbb{C}$ is

$$(z_{\tau})_{\tau} \mapsto (\overline{z_{\overline{\tau}}})_{\tau}$$

where $\overline{\tau}$ denotes the composition of τ with complex conjugation on $\mathbb{C}$. The fixed subring under F is $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$.

Equip $K_{\mathbb{C}} \cong \prod_\tau \mathbb{C}$ with the standard Hermitian inner product, that is,

$$\langle z_1, z_2 \rangle = \sum_\tau z_{1,\tau} \overline{z_{2,\tau}}.$$

This restricts to a positive definite inner product on $K_{\mathbb{R}}$.

Via the embedding of K into $K_{\mathbb{R}}$, $\mathfrak{o}_K$ corresponds to a **lattice** in $K_{\mathbb{R}}$, i.e., a discrete cocompact subgroup. Similarly, any fractional ideal of K corresponds to a lattice in $K_{\mathbb{R}}$. ◊

Profinite completions

Let us put aside the Minkowski construction for the moment and turn to some more arithmetic considerations. We have already used in multiple places the fact that the profinite completion $\widehat{\mathbb{Z}}$ of the group $\mathbb{Z}$ can be identified, via the Chinese remainder theorem, with the product $\prod_p \mathbb{Z}_p$. This generalizes to an arbitrary number field as follows.

Remark 6.1.2 Before continuing, we should clarify our use of notation like $\widehat{\mathfrak{o}_K}$ to denote the profinite completion of $\mathfrak{o}_K$ for K a number field. We originally defined this as an inverse limit over finite *group* quotients of $\mathfrak{o}_K$. However, remember that we can define the same inverse limit using any smaller collection of quotients which is **cofinal** (that is, any finite quotient factors through some chosen quotient). In particular, if G is a subgroup of $\mathfrak{o}_K$ of some finite index n, then $n\mathfrak{o}_K \subseteq G$ and so the quotient map $\mathfrak{o}_K \to \mathfrak{o}_K/G$ factors through the ring quotient $\mathfrak{o}_K/n\mathfrak{o}_K$. That is, $\widehat{\mathfrak{o}_K}$ can be identified with the inverse limit $\varprojlim_n \mathfrak{o}_K/n\mathfrak{o}_K$, and hence also carries the structure of a topological ring.

Lemma 6.1.3 *For K a number field, there is a natural isomorphism of compact topological rings*

$$\widehat{\mathfrak{o}_K} \to \prod_{\mathfrak{p}} \varprojlim_m \mathfrak{o}_K/\mathfrak{p}^m$$

where $\mathfrak{p}$ runs over (nonzero) prime ideals of $\mathfrak{o}_K$.

Proof. As in Remark 6.1.2, we identify $\widehat{\mathfrak{o}_K}$ with $\varprojlim_n \mathfrak{o}_K/n\mathfrak{o}_K$. This ring maps to $\mathfrak{o}_K/\mathfrak{p}^m$ for each prime $\mathfrak{p}$ and each positive integer m; putting these maps together gives us a map $\widehat{\mathfrak{o}_K} \to \varprojlim_m \mathfrak{o}_K/\mathfrak{p}^m$ for each $\mathfrak{p}$, and hence a map to the product.

To see that this map is a bijection, factor the ideal $n\mathfrak{o}_K$ as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ for some primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and some positive integers $e_1, \dots, e_r$. By the Chinese remainder theorem for ideals in a Dedekind domain, the natural map

$$\mathfrak{o}_K/n\mathfrak{o}_K \to \prod_{i=1}^r \mathfrak{o}_K/\mathfrak{p}_i^{e_i}$$

is an isomorphism. This immediately implies that the original map is injective. To see that the original map is surjective, we must also observe that for each prime $\mathfrak{p}$ and each positive integer m, there exists a positive integer n such that $n\mathfrak{o}_K$ is divisible by $\mathfrak{p}^m$; for instance, we may take n to be the absolute norm of $\mathfrak{p}^m$. ■

Remark 6.1.4 We cannot help mentioning a variant of Remark 6.1.2 that plays a key role in p-adic Hodge theory. Let $\mathbb{C}_p$ be a completed algebraic closure

of $\mathbb{Q}_p$. Consider the inverse system

$$\cdots \overset{x \mapsto x^p}{\to} \mathfrak{o}_{\mathbb{C}_p} \overset{x \mapsto x^p}{\to} \mathfrak{o}_{\mathbb{C}_p}.$$

Since the maps are multiplicative but not additive, the inverse limit only appears to carry the structure of a multiplicative monoid. However, it was originally observed by Fontaine that the natural map from this inverse system to the inverse system

$$\cdots \overset{x \mapsto x^p}{\to} \mathfrak{o}_{\mathbb{C}_p}/p\mathfrak{o}_{\mathbb{C}_p} \overset{x \mapsto x^p}{\to} \mathfrak{o}_{\mathbb{C}_p}/p\mathfrak{o}_{\mathbb{C}_p}$$

is an isomorphism. In this inverse system, the maps upgrade to ring homomorphisms because $(x+y)^p = x^p + y^p$ in any ring in which $p = 0$; consequently, the original inverse limit is upgraded to a ring! This then implies that the inverse limit of the system

$$\cdots \overset{x \mapsto x^p}{\to} \mathbb{C}_p \overset{x \mapsto x^p}{\to} \mathbb{C}_p$$

is again a ring; it is in fact an algebraically closed field which is complete with respect to a certain nonarchimedean absolute value. This construction has come to be known as forming the **tilt** of $\mathbb{C}_p$, and generalizes to a large class of fields which are complete with respect to nonarchimedean absolute values (the **perfectoid fields**). See [3] for an introduction to this circle of ideas.

The adèles (rational case)

Our next step is to put the Minkowski construction together with profinite completion to define the ring of adèles. Let us do this first in the case of the rational numbers.

Definition 6.1.5 We define the **ring of finite adèles** $\mathbb{A}_{\mathbb{Q}}^{\mathrm{fin}}$ as any of the following isomorphic objects:

- the tensor product $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$;
- the direct limit of $\frac{1}{n}\widehat{\mathbb{Z}}$ over all nonzero integers n;
- the **restricted direct product** $\prod_p{}' \mathbb{Q}_p$, where we only allow tuples (α_p) for which $\alpha_p \in \mathbb{Z}_p$ for almost all p. See Definition 6.1.6.

This is a locally compact topological ring, with the groups $\frac{1}{n}\widehat{\mathbb{Z}}$ forming a fundamental system of neighborhoods of 0 consisting of compact subgroups. The natural group homomorphism

$$\mathbb{Q}/\mathbb{Z} \to \mathbb{A}_{\mathbb{Q}}^{\mathrm{fin}}/\widehat{\mathbb{Z}}$$

is an isomorphism. ◊

In preparation for the definition of adèles associated to a general number field, we introduce the formalism of restricted products.

Definition 6.1.6 Let I be an index set. For each $i \in I$, let G_i be a set and let H_i be a set of G_i. The **restricted (direct) product** G of the pairs (G_i, H_i) is the set of tuples $(g_i)_{i=1}^{\infty}$ such that $g_i \in H_i$ for all but finitely many indices i. Another way to say this is to define, for each finite subset $S \subseteq I$, the set

$$G_S = \prod_{i \in S} G_i \times \prod_{i \notin S} H_i$$

and take $G = \bigcup_S G_S$.

We upgrade this construction from sets to richer categories as follows.

- If each G_i is a group and each H_i is a subgroup, then G admits a group structure.
- If each G_i is a ring and each H_i is a subring, then G admits a ring structure. (However, if each G_i is a field, then G cannot be a field unless I is a singleton set.)
- If each G_i is a locally compact topological space and each H_i is a compact subspace, then G may be viewed as a locally compact topological space. One way to see this is to use a system of neighborhoods of the identity given by taking products of compact neighborhoods $S_i \subseteq G_i$ in which $S_i = H_i$ for all but finitely many i. (Remember that by Tikhonov's theorem, any product of compact topological spaces is compact.) Another way is to equip each subset G_S with the product topology, then declare a subset $U \subset G$ to be open if its intersection with each G_S is an open subset of G_S.
- Likewise, if each G_i is a locally compact topological group/ring and each H_i is a compact subgroup/subring, then G may be viewed as a locally compact topological group/ring.

$\Diamond$

Definition 6.1.7 Define the **ring of adèles** over $\mathbb{Q}$ as $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \mathbb{A}_{\mathbb{Q}}^{\mathrm{fin}}$. Then $\mathbb{A}_{\mathbb{Q}}$ is a locally compact topological ring with a canonical embedding $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$. We refer to the elements of $\mathbb{Q}$ as **principal adèles** within $\mathbb{A}_{\mathbb{Q}}$.

We may also view $\mathbb{A}_{\mathbb{Q}}$ as a restricted direct product of the pairs

$$(\mathbb{R}, \{0\}), (\mathbb{Q}_2, \mathbb{Z}_2), (\mathbb{Q}_3, \mathbb{Z}_3), \dots;$$

note that taking the subgroup $\{0\}$ of $\mathbb{R}$ has no real effect because the definition of the restricted product involves checking membership in the chosen subgroup for *all but finitely many* indices. $\Diamond$

Remark 6.1.8 Note that $\mathbb{A}_{\mathbb{Q}}$ contains the neighborhood U of 0 consisting of tuples $(x)_v$ where $|x|_\infty < 1$ and $|x|_p \leq 1$ for all primes p. Any element of the intersection $U \cap \mathbb{Q}$ must be an integer (because of the condition at primes), but cannot be a nonzero integer (due to the condition at the real place); hence $U \cap \mathbb{Q} = \{0\}$. That is, just as $\mathbb{Z}$ sits inside $\mathbb{R}$ as a discrete subgroup, $\mathbb{Q}$ sits inside $\mathbb{A}_{\mathbb{Q}}$ as a discrete subgroup.

In fact, we can do somewhat better. Just as the quotient group $\mathbb{R}/\mathbb{Z}$ is covered by the compact subset $[0, 1]$ of $\mathbb{R}$ (and therefore is compact: a continous map from a compact topological space to Hausdorff topological space has compact image), the quotient group $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is covered by a compact subset

$$[0, 1] \times \prod_p \mathbb{Z}_p.$$

(see Exercise 1).

The adèles (general case)

We now put the Minkowski construction together with profinite completion to define the ring of adèles of a number field.

Definition 6.1.9 Let K be a number field. By Lemma 6.1.3, the profinite completion $\widehat{\mathfrak{o}_K}$ is canonically isomorphic to $\prod_{\mathfrak{p}} \mathfrak{o}_{K_{\mathfrak{p}}}$. We may thus define the

ring of finite adèles $\mathbb{A}_K^{\text{fin}}$ as any of the following isomorphic objects:

- the tensor product $\widehat{\mathfrak{o}_K} \otimes_{\mathfrak{o}_K} K$;
- the direct limit of $\frac{1}{\alpha}\widehat{\mathfrak{o}_K}$ over all nonzero $\alpha \in \mathfrak{o}_K$;
- the restricted direct product of the pairs $(K_\mathfrak{p}, \mathfrak{o}_{K_\mathfrak{p}})$ over all primes $\mathfrak{p}$ of K.

The natural homomorphism

$$K/\mathfrak{o}_K \to \mathbb{A}_K^{\text{fin}}/\widehat{\mathfrak{o}_K}$$

is an isomorphism.

The ring of adèles $\mathbb{A}_K$ is the product $K_\mathbb{R} \times \mathbb{A}_K^{\text{fin}}$. In other words, this is the restricted product of the pairs $(K_v, \{0\})$ for infinite places v and $(K_v, \mathfrak{o}_{K_v})$ for finite places v. We again have a diagonal embedding $K \hookrightarrow \mathbb{A}_K$; we again refer to the elements of the image of this embedding as **principal adèles**. ◊

Definition 6.1.10 For each place v of K, let $|\bullet|_v$ be the absolute value on the completion K_v normalized as follows.

- For v real, take the usual real absolute value.
- For v complex, take the *square* of the usual absolute value. (This does not satisfy the triangle inequality; sorry.)
- For v a finite place above the prime p, normalize so that $|p|_v = p^{-1}$.

We then have a well-defined function $|\bullet|$ on $\mathbb{A}_K$ given by

$$|x|_K = \prod_v |x|_v;$$

this makes sense because by virtue of the definition of a restricted direct product, all but finitely many of the values $|x|_v$ are equal to 1. ◊

Proposition 6.1.11 Product formula. *If $\alpha \in K$, then $|\alpha|_K = 1$.*

Proof. The normalizations have been chosen so that for each place v of $\mathbb{Q}$, for each $\alpha \in K$, the product of $|\alpha|_w$ over all places w of K above p equals $|\operatorname{Norm}_{L/K}(\alpha)|_v$. Taking the product over v, we deduce that $|\alpha|_K = |\operatorname{Norm}_{L/K}(\alpha)|_\mathbb{Q}$. That is, the product formula reduces to the case $K = \mathbb{Q}$, which we may check directly: if we write $\alpha = \pm p_1^{e_1} \cdots p_r^{e_r}$, then $|\alpha|_v$ equals $p_1^{e_1} \cdots p_r^{e_r}$ if $v = \infty$, $p_i^{-e_i}$ if $v = p_i$, and 1 otherwise. ■

Corollary 6.1.12 *The subset K of $\mathbb{A}_K$ is discrete.*

Adelic S-integers

Definition 6.1.13 For any finite set S of places, let $\mathbb{A}_{K,S}$ (resp. $\mathbb{A}_{K,S}^{\text{fin}}$) be the subring of $\mathbb{A}_K$ (resp. $\mathbb{A}_K^{\text{fin}}$) consisting of those adèles which are integral at all finite places not contained in S. The elements of $\mathbb{A}_S$ might be thought of as "adelic S-integers". ◊

We can formulate an adelic analogue of the Chinese remainder theorem.

Proposition 6.1.14 *For any finite set S of places, $K + \mathbb{A}_{K,S}^{\text{fin}} = \mathbb{A}_K^{\text{fin}}$ and $K + \mathbb{A}_{K,S} = \mathbb{A}_K$.*

Proof. See Exercise 2. ■

We end up with an adelic analogue of the Minkowski embedding, but with the role of $\mathfrak{o}_K$ played by the entire field K!

Corollary 6.1.15 *The quotient group $\mathbb{A}_K/K$ is compact.*

Proof. Choose a compact subset T of the Minkowski space M containing a fundamental domain for the lattice $\mathfrak{o}_K$. Then every element of $M \times \mathbb{A}_K^{\mathrm{fin}}$ is congruent modulo $\mathfrak{o}_K$ to an element of $T \times \mathbb{A}_K^{\mathrm{fin}}$. By the proposition, the compact set $T \times \mathbb{A}_K^{\mathrm{fin}}$ surjects onto $\mathbb{A}_K/K$, so the latter is also compact. ■

Remark 6.1.16 We mention in passing that just as the various completions of $\mathbb{Q}$ are "rigid" in the sense that they have no nontrivial automorphisms even if you ignore the topology (Exercise 3), the ring $\mathbb{A}_{\mathbb{Q}}$ also has no nontrivial automorphisms even if you ignore the topology (Exercise 6).

The approximation theorem

We already mentioned one analogue of the Chinese remainder theorem (Proposition 6.1.14). Here is another one.

Proposition 6.1.17 Approximation theorem. *Let S be a finite set of places of K. For each $v \in S$, let U_v be an open subgroup of K_v. Then $K \cap \bigcap_{v \in S} U_v \neq \emptyset$.*

Proof. See Exercise 7. ■

Exercises

1. Prove that the map from $[0,1] \times \prod_p \mathbb{Z}_p$ to $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is surjective.

2. Prove Proposition 6.1.14.

3. Let K be a number field and let v be a place of K. Prove that every automorphism of the field K_v (as a ring without topology) is continuous.

Hint. Let q be the cardinality of the residue field of v. Show first that an element of K_v^* belongs to $\mathfrak{o}_{K_v}^*$ if and only if it has an m-th root for every positive integer m coprime to $p(q-1)$. Then note that an element of K_v belongs to $\mathfrak{o}_{K_v}$ iff it is a difference of two elements of $\mathfrak{o}_{K_v}^*$.

4. Let S be a finite set of places of a number field K, none of which is complex. Prove that every automorphism of $\prod_{v \in S} K_v$ (as a ring without topology) is continuous.

Hint. Using Exercise 3, reduce to checking that for two noncomplex places v and w of K, lying over distinct places of $\mathbb{Q}$, the completions K_v and K_w are not isomorphic as underlying rings. To prove this, consider the set of $x \in K$ which are squares in K_v, and similarly for w.

5. Let K be a number field and let v be a place of K which is not complex. Let $Q(x,y,z)$ be a quadratic form over K defined as follows.

- If v is real, put $Q(x,y,z) = x^2 + y^2 + z^2$.
- If v is finite lying over the rational prime p, choose $a \in K \cap \mathfrak{o}_{K_v}^*$ whose image in the residue field of v is not a quadratic residue, and put $Q(x,y,z) = x^2 - ay^2 + pz^2$.

Let T be the intersection of the images of the maps $cQ : \mathbb{A}_K^3 \to \mathbb{A}_K$ over all $c \in K^*$. Prove that $T = \ker(\mathbb{A}_K \to \prod_{w \in S} K_w)$ for some finite set S of places of K containing v.

Hint. Use Hensel's lemma to show that for w a finite place not lying above 2, $a, b, c \in \mathfrak{o}_{K_w}^*$, and $t \in K_w^*$, the equation $ax^2 + by^2 + cz^2 = t$ always

has a solution with $a, b, c \in K_w^*$.

6. Prove that every automorphism of the ring $\mathbb{A}_{\mathbb{Q}}$, *not necessarily continuous*, is trivial.

Hint. Use Exercise 4 and Exercise 5 to prove that the map $\mathbb{A}_{\mathbb{Q}} \to \prod_v \mathbb{Q}_v$ is equivariant for any automorphism of $\mathbb{A}_{\mathbb{Q}}$ and the trivial action on $\prod_v \mathbb{Q}_v$.

7. Prove Proposition 6.1.17.

Hint. Prove by induction on n that given any pairwise distinct places $v_1, \ldots, v_n$, we can find $x \in K$ with

$$|x|_{v_1} @gt; 1, |x|_{v_2} @lt; 1, \ldots, |x|_{v_n} @lt; 1.$$

Then make a careful linear combination of powers of such elements. For more details, see [37], Theorem II.3.4.

6.2 Idèles and class groups

Reference. [36]; [37], VI.1 and VI.2; [33], VII.

We now shift from additive to multiplicative considerations.

Idèles

Definition 6.2.1 Let K be a number field and let $\mathbb{A}_K$ be the ring of adèles associated to K (Definition 6.1.9). We define the **group of idèles** I_K associated to K as the group of units of the ring $\mathbb{A}_K$. In other words, an element of I_K is a tuple (α_v), one element of K_v^* for each place v of K, such that $\alpha_v \in \mathfrak{o}_{K_v}^*$ for all but finitely many finite places v.

As a set, I_K is the restricted product of the pairs $(K_v^*, \{1\})$ for infinite places v and $(K_v, \mathfrak{o}_{K_v}^*)$ for finite places v. We use this interpretation to give I_K the structure of a locally compact topological group. ◊

Definition 6.2.2 For S a finite set, let $I_{K,S}$ be the set of $x \in I_K$ for which $x_v \in \mathfrak{o}_{K_v}^*$ for each finite place $v \notin S$; then $I_K = \bigcup_S I_{K,S}$. By analogy with Definition 6.1.13, the elements of $I_{K,S}$ can be thought of as "adelic S-units". ◊

Remark 6.2.3 Warning. While the embedding of the idèle group I_K into the adèle group $\mathbb{A}_K$ is continuous, the restricted product topology on I_K does not coincide with the subspace topology for the embedding! For example, each set $I_{K,S}$ is open in I_K but is not the intersection with an open subset of $\mathbb{A}_K$.

This is a more serious version of the same issue that came up in Exercise 6, and the same fix applies: namely, identify I_K with $\mathrm{GL}_1(\mathbb{A}_K)$ and topologize it accordingly (Exercise 1).

The idèle class group

Definition 6.2.4 For each $\alpha \in K^*$, the principal adèle $\alpha \in \mathbb{A}_K$ is an idèle, so we have an embedding $K^* \hookrightarrow I_K$. We refer to elements of the image of this embedding as **principal idèles**. Define the **idèle class group** of K as the quotient $C_K = I_K / K^*$ of the idèles by the principal idèles. ◊

The terminology **idèle class group** is justified on account of the following construction.

Definition 6.2.5 There is a homomorphism from I_K to the group of fractional

ideals of K:

$$(\alpha_\nu)_\nu \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})},$$

which is continuous for the discrete topology on the group of fractional ideals. (Note that we are ignoring the infinite places; that is, this map factors through I_K^{fin} viewed as a quotient of I_K.) By unique factorization of fractional ideals, this homomorphism is surjective; its kernel is precisely $I_{K,S}$ for S the set of infinite places.

Under this map, the principal idèle corresponding to $\alpha \in K$ maps to the principal ideal generated by α. Thus we have a surjection $C_K \to \mathrm{Cl}(K)$ with kernel $I_{K,S}K^*/K^*$. ◊

Remark 6.2.6 What are the open subgroups of I_K? For each formal product $\mathfrak{m}$ of places, one gets an open subgroup of idèles $(\alpha_v)_v$ such that:

1. if v is a real place occurring in $\mathfrak{m}$, then $\alpha_v > 0$;
2. if v is a finite place corresponding to the prime $\mathfrak{p}$, occurring to the power e, then $\alpha_v \equiv 1 \pmod{\mathfrak{p}^e}$.

This then projects to an open subgroup of C_K, the quotient by which is the ray class group of modulus $\mathfrak{m}$! (Here we are using the fact that any element of C_K can be represented by an element of I_K which has trivial valuation at any finite place dividing $\mathfrak{m}$. See Definition 7.2.1 for an elaboration of this point.)

Consequently, the quotients of C_K by open subgroups are isomorphic to (and in bijection with) the generalized ideal class groups, with the added convenience that they are all quotients of *one* group (not a group that depends on $\mathfrak{m}$). This correspondence is what will allow us to translate between the classical and adelic versions of Artin reciprocity.

Compactness and consequences

Definition 6.2.7 By the product formula (Proposition 6.1.11), we get a well-defined norm map $|\cdot| : C_K \to \mathbb{R}_+^*$. Let C_K^0 be the kernel of the norm map; then C_K^0 also surjects onto $\mathrm{Cl}(K)$. (The surjection onto $\mathrm{Cl}(K)$ ignores the infinite places, so you can adjust there to force norm 1.) ◊

Proposition 6.2.8 *The group C_K^0 is compact.*

Proof. We first show (see Exercise 2) that there exists a real number $c > 1$ with the following property: every idèle of norm 1 is (multiplicatively) congruent modulo K^* to an idèle whose components all have norms in $[c^{-1}, c]$.
The set of idèles with each component having norm in $[c^{-1}, c]$ is the product of "annuli" in the archimedean places and finitely many of the nonarchimedean places, and the group of units in the rest. (Most of the nonarchimedean places don't have any absolute values strictly between 1 and c.) This is a compact set, the set of idèles therein of norm 1 is a closed subset and so is also compact, and the latter set surjects onto C_K^0, so that's compact too. ■

While Proposition 6.2.8 may look innocuous, it actually implies two key theorems of algebraic number theory which are traditionally proved using the Minkowski lattice construction. (In fact we are really doing the same arguments in slightly different language.)

Corollary 6.2.9 *The class group $\mathrm{Cl}(K)$ of K is finite.*

Proof. The group C_K^0 is compact by Proposition 6.2.8 and it surjects onto $\mathrm{Cl}(K)$, so the latter must also be compact for the discrete topology, and hence finite. ■

Corollary 6.2.10 *There exists a finite set S of places of K such that*

$$I_K = I_{K,S} K^*.$$

In particular, for any such S, C_K is a quotient of $I_{K,S}$.

Proof. Since $\mathrm{Cl}(K) = I_L/K^*$ is finite, it is generated by some finite set of primes. By taking S to include the corresponding places, we achieve the desired effect. ■

Corollary 6.2.11 Dirichlet's units theorem. *The group of units of $\mathfrak{o}_K$ fits into an exact sequence*

$$0 \to \mu_K \to \mathfrak{o}_K^* \to \mathbb{Z}^{r+s-1} \to 0$$

in which μ_K is the (finite cyclic) group of roots of unity of K and r and s are the number of real and complex places, respectively. More generally, for any finite set S of places containing all infinite places, the group of units of the ring $\mathfrak{o}_{K,S}$ of S-integers fits into an exact sequence

$$0 \to \mu_K \to \mathfrak{o}_{K,S}^* \to \mathbb{Z}^{\#S-1} \to 0.$$

Proof. Define the map $\log : I_{K,S} \to \mathbb{R}^{\#S}$ by taking log of the absolute value of the norm of each component in S (normalizing as in Definition 6.1.10). By the product formula (Proposition 6.1.11), this map carries $\mathfrak{o}_{K,S}^*$ into the trace-zero hyperplane H in $\mathbb{R}^{\#S}$. By Kronecker's theorem, any algebraic number with trivial valuation at all finite and infinite places must be a root of unity, so the kernel of $\mathfrak{o}_{K,S}^* \to H$ equals μ_K.
Restricting an element of $\mathfrak{o}_{K,S}^*$ to a bounded subset of H bounds all of its absolute values. Hence the discreteness of K in $\mathbb{A}_K$ (Corollary 6.1.12) implies that the image of the group $\mathfrak{o}_{K,S}^*$ is discrete in H.
Let W be the span in H of the image of $\mathfrak{o}_{K,S}^*$; it remains to check that $W = H$, as this will imply that $\mathfrak{o}_{K,S}^*$ is a lattice in H and hence has rank $\dim H = \#S - 1$. We may check this after enlarging S; by Corollary 6.2.10, we can assume that $I_{K,S} K^* = I_K$ and hence

$$C_K = I_K/K^* \cong I_{K,S}/\mathfrak{o}_{K,S}^*.$$

Using this isomorphism, we obtain a continuous homomorphism $C_K^0 \to H/W$ whose image generates H/W. Since C_K^0 is compact (Proposition 6.2.8), so is its image; this is a contradiction unless H/W is the zero vector space. Thus ■

Remark 6.2.12 One corollary of the proof of Corollary 6.2.9 is that the component group of C_K surjects onto $\mathrm{Cl}(K)$, and hence is nontrivial in general.

This of course does not say anything in the case $K = \mathbb{Q}$, and in this case one can give a more direct description of C_K. Namely, given an arbitrary idèle in $I_{\mathbb{Q}}$, there is a unique positive rational with the same norms at the finite places. Thus

$$C_{\mathbb{Q}} \cong \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^*.$$

Returning to the case of general K, there is a natural way to define a volume measure on C_K in such a way that the volume of the kernel of $C_K^0 \to \mathrm{Cl}(K)$ is exactly the unit regulator of K. Consequently, the total volume of C_K^0 equals the product of the class number and the unit regulator, and it is this product

which shows up in the analytic class number formula (based on the residue of the Dedekind zeta function of K at the point $s = 1$; see Theorem 6.6.9).

Aside: beyond class field theory

Remark 6.2.13 Via the identification $I_K \cong \mathrm{GL}_1(\mathbb{A}_K)$ from Remark 6.2.3, class field theory can be viewed as a correspondence between one-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$ and certain representations of $\mathrm{GL}_1(\mathbb{A}_K)$. This is the form in which class field theory generalizes to the nonabelian case: the Langlands program predicts a correspondence between n-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$ and certain representations of $\mathrm{GL}_n(\mathbb{A}_K)$. See Appendix A for further discussion.

Exercises

1. Show that the restricted direct product topology on I_K is the subspace topology for the embedding into $\mathbb{A}_K \times \mathbb{A}_K$ given by the map $x \mapsto (x, x^{-1})$, and moreover this embedding has closed image.

2. Complete the proof of Proposition 6.2.8 by establishing the existence of the constant c. This can be done using the finiteness of the class group (Corollary 6.2.9) or the units theorem (Corollary 6.2.11); alternatively, with more work one can give a direct proof via which both of the aforementioned results become corollaries of Proposition 6.2.8.

Hint. For the direct approach, see for example [33], Section V.1, Theorem 0.

6.3 Adèles and idèles in field extensions

Reference. [37], VI.1 and VI.2.

Up to now, we have considered the ring of adèles associated to a single number field. We now turn to the effect of a field extension on this construction.

Adèles in field extensions

Definition 6.3.1 If L/K is an extension of number fields, we get an embedding $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$ as follows: given $\alpha \in \mathbb{A}_K$, each place w of L restricts to a place v of K, so it makes sense to declare that the w-component of the image of α shall equal α_v. This embedding induces an inclusion $I_K \hookrightarrow I_L$ of idèle groups.

All automorphisms of L/K act naturally on on $\mathbb{A}_L$ and I_L. More generally, if $g \in \mathrm{Gal}(\overline{K}/K)$, then g maps L to some other extension L^g of K, and g induces isomorphisms

$$\mathbb{A}_L \to \mathbb{A}_{L^g}, \qquad I_L \cong I_{L^g}, \qquad C_L \to C_{L^g}.$$

Explicitly, if $(\alpha_w)_w \in \mathbb{A}_L$ and $g \in G$, then g maps the completion L_w of L to a completion L_{w^g} of L^g. (Remember that a place w of L corresponds to an absolute value $|\cdot|_w$ on L; the absolute value $|\cdot|_{w^g}$ on L^g is given by $|a^g|_{w^g} = |a|_w$.) ◊

Remark 6.3.2 A more conceptual interpretation of the previous discussion is to identify $\mathbb{A}_L$ with the tensor product $\mathbb{A}_K \otimes_K L$. In particular, this is a good way to see the Galois action on $\mathbb{A}_L$. See Exercise 1.

Remark 6.3.3 When K is totally real, it is possible to show that every automorphism of $\mathbb{A}_K$ is induced by an automorphism of K over $\mathbb{Q}$, even if we ignore topology and consider automorphisms of the underlying ring which need not be continuous. See Exercise 4. This breaks down when K has complex places because $\mathbb{C}$ has many automorphisms as a field without topology: the automorphism group acts transitively on $\mathbb{C} \setminus \overline{\mathbb{Q}}$.

Trace and norm

Definition 6.3.4 For L/K an extension of number fields, we define the **trace map** $\mathrm{Trace}_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ and the **norm map** $\mathrm{Norm}_{L/K} : I_L \to I_K$ by the formulas

$$\mathrm{Trace}_{L/K}(x) = \sum_g x^g, \qquad \mathrm{Norm}_{L/K}(x) = \prod_g x^g$$

where g runs over coset representatives of $\mathrm{Gal}(\overline{K}/L)$ in $\mathrm{Gal}(\overline{K}/K)$. Here the sum and product take place in the adèle and idèle rings of the Galois closure of L over K; in particular, if L/K is Galois, g simply runs over $\mathrm{Gal}(L/K)$ and the arithmetic takes place in $\mathbb{A}_L$.

In terms of components, these definitions translate as

$$(\mathrm{Trace}_{L/K}(\alpha))_v = \sum_{w|v} \mathrm{Trace}_{L_w/K_v}(\alpha_w)$$

$$(\mathrm{Norm}_{L/K}(\alpha))_v = \prod_{w|v} \mathrm{Norm}_{L_w/K_v}(\alpha_w).$$

The trace and norm as defined here are compatible with the usual definitions for principal adèles/idèles. In particular, the norm induces a map $\mathrm{Norm}_{L/K} : C_L \to C_K$. ◊

Remark 6.3.5 You can also define the trace of an adèle $\alpha \in \mathbb{A}_L$ as the trace of addition by α as an endomorphism of the finite free $\mathbb{A}_K$-module $\mathbb{A}_L$, and the norm of an idèle $\alpha \in I_L$ as the determinant of multiplication by α as an automorphism of the finite free $\mathbb{A}_K$-module $\mathbb{A}_L$. (Yes, the action is on the *adèles* in both cases. Remember from Remark 6.2.3 that idèles should be thought of as automorphisms of the adèles, not as elements of the adèle ring, in order to topologize them correctly.)

Idèle groups and class groups

Proposition 6.3.6 *If L/K is a Galois extension with Galois group G, then $\mathbb{A}_L^G = \mathbb{A}_K$ and $I_L^G = I_K$.*

Proof. If v is a place of K, then for each place w of K above v, the decomposition group G_w of w is isomorphic to $\mathrm{Gal}(L_w/K_v)$. So if (α) is an adèle or idèle which is G-invariant, then α_w is $\mathrm{Gal}(L_w/K_v)$-invariant for each w, so belongs to K_v. Moreover, G acts transitively on the places w above v, so $\alpha_w = \alpha_{w'}$ for any two places w, w' above v. Thus (α) is an adèle or idèle over K. ■

This has the following consequence for idèle class groups. Note that for L/K any extension of number fields, we can see that $C_K \to C_L$ is injective from the fact that $L^* \cap I_K = K^*$ within I_L, which follows from the fact that $L \cap \mathbb{A}_K = K$ within $\mathbb{A}_L$ (e.g., by Exercise 2).

Corollary 6.3.7 Galois descent. *If L/K is a Galois extension with Galois group G, then G acts on C_L, and the G-invariant elements are precisely C_K.*

Proof. We start with an exact sequence

$$1 \to L^* \to I_L \to C_L \to 1$$

of G-modules. Taking G-invariants, we get a long exact sequence

$$1 \to (L^*)^G = K^* \to (I_L)^G = I_K \to C_L^G \to H^1(G, L^*),$$

and the last term is 1 by Theorem 90 (Lemma 1.2.3). So we again have a short exact sequence, and $C_L^G \cong I_K/K^* = C_K$. ∎

Remark 6.3.8 There is no analogue of Corollary 6.3.7 for ideal class groups: the map $\mathrm{Cl}(K) \to \mathrm{Cl}(L)^G$ is neither injective nor surjective in general (Exercise 5). This is our first hint of why the idèle class group will be a more convenient target for a reciprocity map than the ideal class group.

The group $\mathrm{Cl}(L)^G$ is classically known as the group of **ambiguous classes** of L/K. This is related to the concept of a **Pólya field** from Remark 2.3.13; see [5].

Exercises

1. Let L/K be a finite extension of number fields. Prove that the natural map $\mathbb{A}_K \otimes_K L \to \mathbb{A}_L$ is an isomorphism. In other words, if $\alpha_1, \dots, \alpha_n$ form a basis of L as a K-vector space, then they also form a basis of $\mathbb{A}_L$ as an $\mathbb{A}_K$-module.

Hint. Show first that for any place v of K, any basis of L as a K-vector space also forms a basis of $\prod_{w|v} L_w$ as a K_v-vector space.

2. Let K be a number field. Prove that the integral closure of $\mathbb{Q}$ in $\mathbb{A}_K$ is equal to K.

Hint. Suppose to the contrary that the integral closure contains some larger number field L. By Corollary 2.4.12, there are infinitely many primes of K which do not split in L; use one of these to obtain a contradiction.

3. Prove the following converse to Exercise 2: if L/K is an extension of number fields such that $K + \mathbb{A}_{L,S} = \mathbb{A}_L$ for some finite set of places S of L, prove that $K = L$.

Hint. Use the fact that there are infinitely many primes of K that do not split completely in L (Corollary 2.4.12).

4. Let K be a totally real Galois number field. Prove that the automorphism group of $\mathbb{A}_K$ as a bare ring (ignoring its topology) equals $\mathrm{Gal}(K/\mathbb{Q})$.

Hint. By Exercise 2, any automorphism of $\mathbb{A}_K$ acts on K. We thus have homomorphisms $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(\mathbb{A}_K) \to \mathrm{Gal}(K/\mathbb{Q})$ whose composition is the identity; it thus remains to check that $\mathrm{Aut}(\mathbb{A}_K) \to \mathrm{Gal}(K/\mathbb{Q})$ is injective. For this, apply Exercise 5 as in Exercise 6.

5. Let L/K be a Galois extension of number fields with Galois group G.

(a) Give an example for which $\mathrm{Cl}(K) \to \mathrm{Cl}(L)^G$ fails to be injective.

(b) Give an example for which $\mathrm{Cl}(K) \to \mathrm{Cl}(L)^G$ fails to be surjective.

Hint. One way to produce failures of injectivity is via the principal ideal theorem (Theorem 2.3.1). One way to produce failures of surjectivity is to find quadratic fields with class group $\mathbb{Z}/4\mathbb{Z}$.

6.4 The adelic reciprocity law and Artin reciprocity

We now describe the setup by which we create a reciprocity law in global class field theory, imitating the "abstract" setup from local class field theory but using the idèle class group in place of the multiplicative group of the field. We then work out why the reciprocity law and existence theorem in the adelic setup imply Artin reciprocity and the existence theorem (and a bit more) in the classical language.

Convention note. We are going to fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and regard "number fields" as finite subextensions of $\overline{\mathbb{Q}}/\mathbb{Q}$. That is, we are fixing the embeddings of number fields into $\overline{\mathbb{Q}}$. We'll use these embeddings to decide how to embed one number field in another.

The adelic reciprocity law and existence theorem

Here are the adelic reciprocity law and existence theorem; notice that they look just like the local case except that the multiplicative group has been replaced by the idèle class group.

Theorem 6.4.1 Adelic reciprocity law. *There is a canonical map $r_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ which induces, for each Galois extension L/K of number fields, an isomorphism $r_{L/K} : C_K/\operatorname{Norm}_{L/K} C_L \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$. Moreover, $\operatorname{Norm}_{L/K} C_L$ is an open subgroup of C_K.*

Proof. We will first prove an "abstract" form of this theorem, in which we do not say much about the identity of the map r_K; see Theorem 7.3.8. We then prove a more precise version including a more specific recipe for the map; see Proposition 6.4.5 for the recipe and Proposition 7.5.7 for the comparison with the abstract version. (For the assertion that $\operatorname{Norm}_{L/K} C_L$ is open in C_K, see Remark 7.1.7.) ■

Theorem 6.4.2 Adelic existence theorem. *For every number field K and every open subgroup H of C_K of finite index, there exists a finite (abelian) extension L of K such that $H = \operatorname{Norm}_{L/K} C_L$.*

Proof. See Theorem 7.4.8. ■

We will also obtain a global analogue of the local norm limitation theorem, which was not even suggested by the classical language. (Well, not in this treatment anyway. See Lemma 7.2.2 for an interpretation of the quotient $C_K/\operatorname{Norm}_{L/K} C_L$ in ideal-theoretic terms.)

Theorem 6.4.3 Adelic norm limitation theorem. *Let L/K be an extension of number fields and put $M = L \cap K^{\mathrm{ab}}$. Then $\operatorname{Norm}_{L/K} C_L = \operatorname{Norm}_{M/K} C_M$.*

Proof. See Theorem 7.3.10. ■

More on the reciprocity map

We next use local class field theory and the principle of **local-global compatibility** to come up with a candidate for the map r_K in the adelic reciprocity law (Theorem 6.4.1). We note in passing that this principle also lies at the heart of the extension of class field theory envisioned in the Langlands program (Remark 6.2.13).

Definition 6.4.4 Let L/K be an abelian extension of number fields and v a place of K. Put $G = \mathrm{Gal}(L/K)$ and let G_v be the **decomposition group** of v, that is, the set of $g \in G$ such that $v^g = v$. Then for any place w above v, $G_v \cong \mathrm{Gal}(L_w/K_v)$. We will define a map $r_{K,v} : K_v^* \to G_v \subseteq G$ as follows.

- If v is a finite place, use the local reciprocity map (Theorem 4.1.2).
- If v is a real place, use the sign map $\mathbb{R}^* \to \{\pm 1\} \cong G_v$.
- If v is a complex place, then G_v is trivial and so there is nothing left to specify.

We obtain a well-defined product map

$$\tilde{r}_K : I_K \to G, \qquad (\alpha_v) \mapsto \prod_v r_{K,v}(\alpha_v) :$$

for $(\alpha_v) \in I_K$, α_v is a unit for almost all v and L_w/K_v is unramified for almost all v (we may ignore infinite places here). For the (almost all) v in both categories, $r_{K,v}$ maps α_v to the identity.

Since each of the maps $r_{K,v}$ is continuous, so is the map $\tilde{r}_K$. That means the kernel of $\tilde{r}_K : I_K \to \mathrm{Gal}(L/K)$ is an open subgroup of I_K. ◊

Here is the subtle point, and the real source of "reciprocity" in this construction.

Proposition 6.4.5 *For L/K an abelian extension of number fields, the map $\tilde{r}_K : I_K \to \mathrm{Gal}(L/K)$ is trivial on K^*. It thus factors through a map $r_K : C_K \to \mathrm{Gal}(L/K)$.*

Proof. See Proposition 7.5.7. ■

Remark 6.4.6 In case $L = K(\zeta_n)$ for some n, we can verify Proposition 6.4.5 by an explicit computation, similar to the direct verification of Artin reciprocity for these extensions. This suggests that in general, we must first prove the adelic existence theorem (Theorem 6.4.2) before establishing Proposition 6.4.5. In the interim, we will derive a makeshift form of adelic reciprocity from the framework of abstract class field theory.

Proposition 6.4.7 *Let L/K be an abelian extension of number fields. Given Theorem 6.4.1 and Proposition 6.4.5, let U be the kernel of r_K, identify C_K/U with a generalized ideal class group (Remark 6.2.6) of some conductor $\mathfrak{m}$. Then the map $C_K/U \to \mathrm{Gal}(L/K)$ is the Artin map; consequently, Theorem 2.2.6 holds.*

Proof. The idèle $\alpha = (1, 1, \dots, \pi, \dots)$ with a uniformizer π of $\mathfrak{o}_{K_\mathfrak{p}}$ in the $\mathfrak{p}$ component and 1s elsewhere maps onto the class of $\mathfrak{p}$ in C_K/U. On the other hand, $r_K(\alpha) = r_{K,\mathfrak{p}}(\pi)$ is (because L is unramified over K) precisely the Frobenius of $\mathfrak{p}$. So indeed, $\mathfrak{p}$ is being mapped to its Frobenius, so the map $C_K/U \to \mathrm{Gal}(L/K)$ is indeed Artin reciprocity. ■

Remark 6.4.8 The argument from Proposition 6.4.7 also gives some additional information about the Artin map. First, the Artin map factors through a generalized ideal class group whose conductor $\mathfrak{m}$ is divisible *precisely* by the ramified primes. Second, we can *exactly* describe the kernel of the classical Artin map: it is generated by

- all principal ideals congruent to 1 modulo $\mathfrak{m}$;
- norms of ideals of L not divisible by any ramified primes.

6.5 Adelic reciprocity: what remains to be done

We now pick up the thread from Section 5.4 to outline the proofs of the main results of class field theory, to be presented in Chapter 7. Many of these steps will be analogous to the steps in local class field theory; however, we do *not* directly attempt to verify Proposition 6.4.7 except for cyclotomic extensions, for which the explicit calculation suggested in Remark 6.4.6 will be an important input into the machine. Instead, we postpone this step all the way until the end.

Abstract reciprocity

Our first goal is to establish the conditions for abstract class field theory (Section 5.1), in the setup described at the end of Section 5.3 using the idèle class groups C_K. This requires verifying the class field axiom (Definition 5.1.4), plus a compatibility between the homomorphism d on the absolute Galois group and the valuation map v.

We treat the class field axiom in two steps. The first step is to show that for L/K cyclic, the Herbrand quotient of C_L as a $\mathrm{Gal}(L/K)$-module is $[L:K]$. This implies the **First Inequality** (Theorem 7.1.2):

$$\#H_T^0(\mathrm{Gal}(L/K), C_L) \geq [L:K].$$

The argument will be to replace the group I_L with the subgroup $I_{L,T}$ for some suitable set of places T of L, and reduce to studying lattices in the manner of the proof of Dirichlet's units theorem Corollary 6.2.11).

The next step will to prove the **Second Inequality** (Theorem 7.2.10):

$$\#H_T^0(\mathrm{Gal}(L/K), C_L) \leq [L:K],$$

which combined with the previous point yields

$$\#H_T^0(\mathrm{Gal}(L/K), C_L) = [L:K], \qquad \#H_T^1(\mathrm{Gal}(L/K), C_L) = 1.$$

This step is trivial in local CFT by Theorem 90 (Lemma 1.2.3), but is pretty subtle in the global case. We will first describe a proof using analytic methods (properties of L-functions); there is also an algebraic approach, more on which below.

Finally, we check the compatibility between d and v using the explicit nature of Artin reciprocity for cyclotomic extensions. Plugging into the machine then gives an "abstract" reciprocity map (Theorem 7.3.8), not yet known to be related to Artin reciprocity except for cyclotomic extensions. We also establish the norm limitation theorem (Theorem 7.3.10).

The existence theorem and local-global compatibility

Our next step is to prove the adelic existence theorem (Theorem 6.4.2). As in the local setting, having the reciprocity law (even only in abstract form, and even without any compatibility with the Artin map) and the norm limitation theorem in hand allows us to reduce to showing that every open subgroup of C_K of finite index contains a norm group (Theorem 7.4.8). This can be done after enlarging K, so we can get into the realm of Kummer theory; this is closely related to the algebraic proof of the Second Inequality mentioned above.

We then turn around and use the existence theorem to deduce that for every finite abelian extension of the completion of a number field at some place is

itself the completion of a finite extension of the number field (Theorem 7.5.9). This will allow us to show, making careful use of cyclotomic extensions, that the "abstract" global reciprocity map restricts to the usual reciprocity map from local class field theory (Proposition 7.5.7). This will finally imply Proposition 6.4.5, thus yielding the adelic reciprocity map (and also showing that it coincides with the abstract reciprocity map).

Another approach via Brauer groups

We will also briefly sketch the approach taken in [36], in which one uses Galois cohomology in place of abstract class field theory. Specifically, one first checks that $H^2(\mathrm{Gal}(L/K), C_L)$ is cyclic of order $[L:K]$ in certain "unramified" (i.e., cyclotomic) cases; as in the local case, one can then deduce this result in general by induction on degree. Using Tate's theorem (Theorem 4.1.14), one gets a reciprocity map

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} = H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^0(\mathrm{Gal}(L/K), C_K / \mathrm{Norm}_{L/K} C_L)$$

which again can be reconciled with local reciprocity to get the Artin reciprocity map (Proposition 7.6.17). This approach will also yield some additional information, notably a description of the Brauer group of a number field (Theorem 7.6.10).

6.6 Adelic Fourier analysis after Tate

Reference. The original source is [4], XV; note that the "valuation vectors" used therein are our adèles, as per Remark 6.0.1. For a modern (and much less terse) treatment, see [42].

As an aside, we describe another classic use of adèles in algebraic number theory: the derivation of the analytic continuation and functional equation of Dedekind zeta functions and Dirichlet L-functions via Fourier analysis on the adèles, as described by Tate in his PhD thesis. This is meant merely as a guide to the latter, so we omit essentially all proofs.

Additive characters

Lemma 6.6.1 *Let K be a number field and let v be a place of K. Then the dual group $(K_v^+)^\vee$ of continuous characters from K_v^+ to $\{z \in \mathbb{C} : |z| = 1\}$ is a locally compact topological group. Moreover, for any nontrivial element $X \in (K_v^+)^\vee$, the map*

$$K_v^+ \to X, \qquad \eta \mapsto (\xi \mapsto X(\eta\xi))$$

defines a continuous isomorphism $K_v^+ \to (K_v^+)^\vee$.

Proof. See [4], XV, Lemma 2.2.1. ∎

Remark 6.6.2 To choose a character X as in Lemma 6.6.1, we may precompose with a trace map to reduce to the case $K = \mathbb{Q}$. In that case, for $v = \infty$ we may take X to be the character $t \mapsto e^{-2\pi i t}$; for $v = p$, we may take it to be $t \mapsto e^{-2\pi i \lambda(t)}$ where $\lambda(t) \in \mathbb{Z}_{(p)}$ is congruent to t modulo $\mathbb{Z}_p$.

This discussion globalizes directly to the adèles, as long as we are careful about normalization.

Theorem 6.6.3 *Let K be a number field. For each place v of K, let X_v be a nontrivial additive character on K_v^+ as in Remark 6.6.2, and define the additive*

character X on $\mathbb{A}_K^+$ via

$$X(\alpha) = \prod_v X_v(\alpha_v).$$

Then the dual group $(\mathbb{A}_K^+)^\vee$ is a locally compact topological group, and the map

$$\alpha \mapsto (\beta \mapsto X(\alpha\beta))$$

defines a continuous isomorphism $\mathbb{A}_K^+ \to (\mathbb{A}_K^+)^\vee$.

Proof. See [4], XV, Theorem 4.1.1. ■

Fourier inversion

Theorem 6.6.4 Local Fourier inversion. *Let K be a number field and let v be a place of K. Fix a Haar measure on K_v^+ and a nontrivial character $X \in (K_v^+)^\vee$. For $f \in L_1(K_v^+)$, define the* ***Fourier transform***

$$\hat{f}(\eta) = \int f(\xi)X(\eta\xi)\,d\xi.$$

If $\hat{f} \in L_1(K_v^+)$ also, then

$$f(\xi) = c\int \hat{f}(\eta)X(-\eta\xi)\,d\eta = c\widehat{\hat{f}}(-\xi)$$

for some $c > 0$ which depends only on the Haar measure and the character X. In particular, these can be normalized so that $c = 1$.

Proof. See [4], XV, Theorem 2.2.2. ■

Theorem 6.6.5 Global Fourier inversion. *Let K be a number field, fix a Haar measure on $\mathbb{A}_K$, and define the additive character X on $\mathbb{A}_K^+$ as in Theorem 6.6.3. For $f \in L_1(\mathbb{A}_K^+)$, define the* ***Fourier transform***

$$\hat{f}(\eta) = \int f(\xi)X(\eta\xi)\,d\xi.$$

If $\hat{(f)} \in L_1(K_v^+)$ also, then

$$f(\xi) = c\int \hat{f}(\eta)X(-\eta\xi)\,d\eta = c\widehat{\hat{f}}(-\xi)$$

for some $c > 0$ which depends only on the Haar measure and the character X. In particular, these can be normalized so that $c = 1$.

Proof. See [4], XV, Theorem 4.1.2. ■

Remark 6.6.6 Crucially, there is also a version of the **Poisson summation formula** in this context. In classical Fourier analysis, this involves summing a function and its Fourier transform over the lattice $\mathbb{Z}$ in $\mathbb{R}$. In the adelic setup, the "lattice" is the subgroup K of $\mathbb{A}_K$, and the result can also be viewed as an analogue of the Riemann-Roch theorem in complex geometry! See [4], XV, Theorem 4.2.1.

The space of quasi-characters

Definition 6.6.7 Let K be a number field. By a **quasi-character** on the idèle class group C_K, we will mean any continuous homomorphism from this group into $\mathbb{C}^*$. By contrast, a **character** is required to map into the unit circle.

For each quasi-character c, there exists a unique real number s such that $|c(\alpha)| = |\alpha|^s$ for all $\alpha \in I_K$ (where $|\alpha|$ is defined as in Definition 6.2.7). We call s the **exponent** of c.

The space of quasicharacters on C_K contains a distinguished copy of $\mathbb{C}$: each complex number s corresponds to the character $\alpha \mapsto |\alpha|^s$. The exponent of this character is precisely the real part of s. ◊

Remark 6.6.8 The adelic zeta function of K will be a function on the space of quasi-characters. Its restriction to the distinguished copy of $\mathbb{C}$ will give the usual zeta function. If we take the translate of this copy of $\mathbb{C}$ by some other quasi-character, we will end up computing the L-function associated to some Hecke character. The idea of the adelic setup is to package all of these Hecke L-functions together into a single object, which can be studied by an adelic analogue of the classical proof of analytic continuation for the Riemann zeta function. More on this below.

Zeta functions and L-functions

The classical approach to deriving the analytic continuation and functional equation for a Dedekind zeta function, or for Dirichlet L-functions, is to interpret via an integral representation (technically, as a **Mellin transform** of a theta series). The functional equation then follows from Poisson summation. Something similar is possible in the adelic situation, with the additional advantage of admitting a "local-global compatibility".

Theorem 6.6.9 *For suitable functions $f : \mathbb{A}_K \to \mathbb{C}$, define the associated **zeta function** as the following function of quasicharacters on C_K with exponent greater than 1:*

$$\zeta(f, c) = \int f(\alpha)c(\alpha)\, d\alpha.$$

This function is single-valued and holomorphic except at the points corresponding to $s = 0$ and $s = 1$ where it has simple poles with residues $-\kappa f(0)$ and $\kappa \hat{f}(0)$, respectively, where

$$\kappa = 2^{r_1}(2\pi)^{r_2}\frac{hR}{\sqrt{|\Delta_K|}\omega_K}$$

(with r_1 the number of real places, r_2 the number of complex places, h the class number, R the unit regulator, Δ_K the discriminant, and ω_K the order of the group of roots of unity). Moreover, we have the functional equation

$$\zeta(f, c) = \zeta(\hat{f}, \hat{c})$$

where $\hat{c}(\alpha) = \alpha c(\alpha)^{-1}$ (so in particular $s \mapsto 1 - s$).

Proof. See [4], XV, Theorem 4.4.1. ■

Remark 6.6.10 Theorem 6.6.9 looks a lot like what we are expecting except for the presence of the mysterious test function f. To get back to more classical statements like Theorem 2.4.2 and Theorem 2.4.5, one must choose f so that one can evaluate $\hat{f}$ and have it come out to be something similar to f. See the very end of [4], XV for further discussion.

Chapter 7

The main results

We finally embark on the proof of the main results of global class field theory, via the adelic reformulation (Section 6.4) and specifically the outline from Section 6.5.

7.1 Cohomology of the idèles I: the "First Inequality"

Reference. [36] VII.2-VII.4; [37] VI.3, but see below. See also this blog post by Akhil Mathew[1].

By analogy with local class field theory, we want to prove that for L/K a cyclic extension of number fields and C_K, C_L the respective idèle class groups of K and L,

$$H^1(\mathrm{Gal}(L/K), C_L) = 1, \qquad H^2(\mathrm{Gal}(L/K), C_L) = \mathbb{Z}/[L:K]\mathbb{Z}.$$

Our first step is to calculate the Herbrand quotient.

Theorem 7.1.1 *For L/K a cyclic extension of number fields,*

$$h(C_L) = [L:K].$$

Proof. This will follow by combining Corollary 7.1.5, Definition 7.1.9, and Lemma 7.1.10. ∎

This will end up reducing to a study of lattices in a real vector space, much as in the proof of Dirichlet's units theorem (Corollary 6.2.11).

From Theorem 7.1.1, we will deduce the so-called "First Inequality".

Theorem 7.1.2 First Inequality. *For L/K a cyclic extension of number fields,*

$$\#H^0_T(\mathrm{Gal}(L/K), C_L) \geq [L:K].$$

Proof. Apply Theorem 7.1.1 and remember that $\#H^1_T(\mathrm{Gal}(L/K), C_L) \geq 1$. ∎

The "Second Inequality" will be the reverse, which will be a bit more subtle (see Theorem 7.2.10).

[1] `amathew.wordpress.com/2010/05/30/the-first-inequality-cohomology-of-the-idele-classes/`

Some basic observations

Definition 7.1.3 Let L/K be a Galois extension of number fields with Galois group G. (We do not yet need G to be cyclic.) For any finite set S of places of K containing all infinite places, write $I_{L,S}$ to mean the group $I_{L,T}$ where T denotes the set of places of L lying over some place in S. Similarly, write $\mathfrak{o}_{L,S}$ to mean $\mathfrak{o}_{L,T}$.

Note that each $I_{L,S}$ is stable under the action of G and that I_L is the direct limit of the $I_{L,S}$ over all S. Moreover, by Corollary 6.2.10, for S sufficiently large we have

$$I_L = I_{L,S} L^*.$$

$\Diamond$

Proposition 7.1.4 *Let L/K be a Galois extension of number fields with Galois group G. For each $i > 0$,*

$$H^i(G, I_L) = \bigoplus_v H^i(G_w, L_w^*),$$

where v runs over places of K and w denotes a single place of L above v. Similarly, for each i,

$$H_T^i(G, I_L) = \bigoplus_v H_T^i(G_w, L_w^*).$$

Proof. View I_L as the direct limit of the $I_{L,S}$ over all finite sets S of places of K containing all infinite places and all ramified places; then $H^i(G, I_L)$ is the direct limit of the $H^i(G, I_{L,S})$. The latter is the product of $H^i(G, \prod_{w|v} L_w^*)$ over all $v \in S$ and $H^i(G, \prod_{w|v} \mathfrak{o}_{L_w}^*)$ over all $v \notin S$, but the latter is trivial because $v \notin S$ cannot ramify. By Shapiro's lemma (Lemma 3.2.3), $H^i(G, \prod_{w|v} L_w^*) = H^i(G_w, L_w^*)$, so we have what we want. The argument for Tate groups is analogous. ■

Corollary 7.1.5 *Let L/K be a Galois extension of number fields with Galois group G. Then*

$$H^1(G, I_L) = 0, \qquad H^2(G, I_L) = \bigoplus_v \frac{1}{[L_w : K_v]} \mathbb{Z}/\mathbb{Z}.$$

Proof. This follows by combining Proposition 7.1.4, the computation of cohomology of local fields (Lemma 1.2.3 and Proposition 4.2.1), and the equality

$$H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) \cong H_T^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) = \mathbb{R}^*/\mathbb{R}^+ \cong \mathbb{Z}/2\mathbb{Z}.$$

■

Remark 7.1.6 Sanity check. The case $i = 0$ of Proposition 7.1.4 asserts something that is evidently true: an idèle in I_K is a norm from I_L if and only if each component is a norm.

Remark 7.1.7 If S contains all infinite places and all ramified places, then

$$\mathrm{Norm}_{L/K} I_{L,S} = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_{K_v}^*$$

where U_v is open in K_v^*. The group on the right is open in I_K, so $\mathrm{Norm}_{L/K} I_K$ is open.

By quotienting down to C_K, we see that $\mathrm{Norm}_{L/K} C_K$ is open. In fact, the snake lemma on the diagram

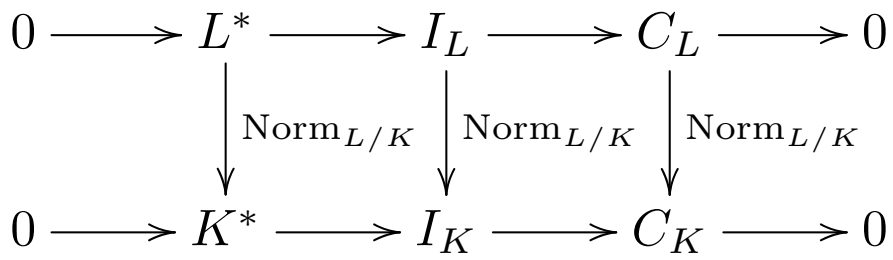

Figure 7.1.8

implies that the quotient $I_K/(K^* \times \mathrm{Norm}_{L/K} I_L)$ is isomorphic to $C_K/\mathrm{Norm}_{L/K} C_L$.

Cohomology of the units: first steps

Definition 7.1.9 Let L/K be a cyclic extension of number fields with Galois group G. Apply Corollary 6.2.10 to choose a finite set S of places of K so that $I_L = I_{L,S}L^*$. From the exact sequence

$$1 \to \mathfrak{o}_{L,S}^* \to I_{L,S} \to I_{L,S}/\mathfrak{o}_{L,S}^* = C_L \to 1$$

we have an equality of Herbrand quotients

$$h(C_L) = h(I_{L,S})/h(\mathfrak{o}_{L,S}^*).$$

By Corollary 7.1.5,

$$h(I_{L,S}) = \prod_{v \in S} \# H_T^0(G_v, L_w^*) = \prod_{v \in S} [L_w : K_v].$$

(Since G is abelian, we write G_v instead of G_w.) To get $h(C_L) = [L : K]$, it will thus suffice to establish Lemma 7.1.10 below. ◊

Lemma 7.1.10 *Let L/K be a cyclic extension of number fields. Let S be a finite set of places of K containing all infinite places. Then*

$$h(\mathfrak{o}_{L,S}^*) = \frac{1}{[L : K]} \prod_{v \in S} [L_w : K_v].$$

Proof. See the calculations in Definition 7.1.11 and Definition 7.1.13, plus Lemma 7.1.14. ■

Cohomology of the units: a computation with S-units

At this point, we have reduced the computation of the Herbrand quotient $h(I_L)$, and by extension the First Inequality, to the computation of $h(\mathfrak{o}_{L,S}^*)$ for a suitable set S of places of K. We treat this point next, using similar ideas to the proof of Dirichlet's units theorem (Corollary 6.2.11).

Definition 7.1.11 Let L/K be a cyclic extension of number fields with Galois group G. Let S be a finite set of places of K containing all infinite places, and let T be the set of places of L lying above places of S. Let V be the real vector space consisting of one copy of $\mathbb{R}$ for each place in T. Define the map $\mathfrak{o}_{L,S}^* \to V$ by

$$\alpha \to \prod_{w \in T} \log |\alpha|_w$$

with normalizations as in Definition 6.1.10. By the product formula (Proposition 6.1.11) and Dirichlet's units theorem (Corollary 6.2.11), the kernel of this map consists of roots of unity, and the image M is a lattice in the trace-zero hyperplane H of V. Since G acts compatibly on $\mathfrak{o}_{L,S}^*$ and V (the latter by permuting the factors), it also acts on M. ◊

Remark 7.1.12 Caveat. At this point, we deviate from [37] due to an error therein. Namely, Lemma VI.3.4 is only proved assuming that G acts transitively on the coordinates of V, but in Definition 7.1.11 this is not the case: G permutes the places above any given place v of K but those are separate orbits. So we'll follow [36] instead.

Definition 7.1.13 Continuing from Definition 7.1.11, we can write down two natural lattices in V. One of them is the lattice generated by M together with the all-ones vector, on which G acts trivially. As a G-module, the Herbrand quotient of that lattice is $h(M)h(\mathbb{Z}) = [L : K]h(M)$. The other is the lattice M' in which, in the given coordinate system, each element has integral coordinates. To compute its Herbrand quotient, notice that the projection of this lattice onto the coordinates corresponding to the places $w \in T$ above some $v \in S$ form a copy of $\mathrm{Ind}_{G_v}^G \mathbb{Z}$. Thus

$$h(G, M') = \prod_{v \in S} h(G, \mathrm{Ind}_{G_v}^G \mathbb{Z}) = \prod_{v \in S} h(G_v, \mathbb{Z}) = \prod_{v \in S} \#G_v = \prod_{v \in S} [L_w : K_v].$$

◊

To sum up, the calculations from Definition 7.1.11 and Definition 7.1.13 reduce Lemma 7.1.10 to the following statement (Lemma 7.1.14).

Herbrand quotients of real lattices

We conclude the proof of the First Inequality with the following statement.

Lemma 7.1.14 *Let V be a real vector space on which a finite cyclic group G acts linearly, and let L_1 and L_2 be G-stable lattices in V for which at least one of $h(L_1)$ and $h(L_2)$ is defined. Then $h(L_1) = h(L_2)$ (and both are defined).*

Proof. Note that $L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$ are $\mathbb{Q}[G]$-modules which become isomorphic to V, and hence to each other, after tensoring over $\mathbb{Q}$ with $\mathbb{R}$. By Lemma 7.1.15, this implies that $L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as $\mathbb{Q}[G]$-modules.
From this isomorphism, we see that as a $\mathbb{Z}[G]$-module, L_1 is isomorphic to some sublattice of L_2. Since a lattice has the same Herbrand quotient as any sublattice (the quotient is finite, so its Herbrand quotient is 1), that means $h(L_1) = h(L_2)$. ■

Lemma 7.1.15 *Let F/E be an extension of infinite fields. Let G be a finite group. Let V_1 and V_2 be two right $E[G]$-modules which are finite-dimensional as E-vector spaces. If $V_1 \otimes_E F$ and $V_2 \otimes_E F$ are isomorphic as $F[G]$-modules, then V_1 and V_2 are isomorphic.*

Proof. By hypothesis, the F-vector space

$$W_F = \mathrm{Hom}_F(V_1 \otimes_E F, V_2 \otimes_E F),$$

on which G acts by the formula $T^g(x) = T(x^{g^{-1}})^g$, contains an invariant vector which, as a linear transformation, is invertible. Now W_F can also be written as

$$W \otimes_E F, \qquad W = \mathrm{Hom}_E(V_1, V_2).$$

The fact that W_F has an invariant vector says that a certain set of linear equations has a nonzero solution over F, namely the equations that express the fact that the action of G leaves the vector invariant. But those equations have coefficients in E, so

$$W^G \otimes_E F = W_F^G;$$

in particular, the space of invariant vectors in W is also nonzero.
It remains to check that some element of W^G corresponds to a map $V_1 \to V_2$ which is actually an isomorphism; for this, we argue as in Exercise 3. Fix an isomorphism of vector spaces between $V_2 \otimes_E F$ and $V_1 \otimes_E F$ (which need not respect the G-action). By composing each element of W with this isomorphism and taking the determinant, we get a well-defined polynomial function on W, which we can restrict to W^G. By hypothesis, this function is not identically zero on W_F^G, so (because E is infinite) it cannot be identically zero on W^G either. ■

Splitting of primes

As a consequence of the First Inequality, we record the following fact which was previously stated as a consequence of the Chebotaryov density theorem (Theorem 2.4.11), but which will be needed logically earlier in the arguments. (See [37], Corollary VI.3.8 for more details.)

Corollary 7.1.16 *For any nontrivial extension L/K of number fields, there are infinitely many primes of K which do not split completely in L.*

Proof. Suppose first that L/K is cyclic. Suppose that all but finitely many primes split completely; we can then take a finite set S of places which contains all of them as well as all of the infinite places and all of the ramified places. For each $v \in S$, the group $U_v = \mathrm{Norm}_{L_w/K_v} L_w^*$ is open of finite index in K_v^*. For any $\alpha \in I_K$, using the approximation theorem (Proposition 6.1.17) we can then find $\beta \in K^*$ such that $(\alpha/\beta)_v \in U_v$ for all $v \in S$. For each place $v \notin S$, we have $L_w = K_v$, so $\alpha/\beta \in \mathrm{Norm}_{L/K} I_L$. We deduce that the class of α in C_L is a norm; that is, $C_K = \mathrm{Norm}_{L/K} C_L$, whereas Theorem 7.1.2 asserts that $H_T^0(\mathrm{Gal}(L/K), C_L) \geq [L : K]$, contradiction.
In the general case, let M be the Galois closure of L/K; then a prime of K splits completely in L if and only if it splits completely in M. Since $\mathrm{Gal}(M/K)$ is a nontrivial finite group, it contains a cyclic subgroup; let N be the fixed field of this subgroup. By the previous paragraph, there are infinitely many prime ideals of N which do not split completely in M, proving the original result. ■

Exercises

1. Let K be a number field. Let $L_1, \ldots, L_r$ be cyclic extensions of K of the same prime degree p such that $L_i \cap L_j = K$ for $i \neq j$. Using the First Inequality (Theorem 7.1.2), prove that there are infinitely many primes of K which split completely in $L_2, \ldots, L_r$ but not in L_1.

7.2 Cohomology of the idèles II: the "Second Inequality"

Reference. [36] VII.5; [37] VI.4. See also this blog post by Akhil Mathew[1].

[1] amathew.wordpress.com/2010/06/05/the-algebraic-proof-of-the-second-inequality-i/

In Section 7.1, we proved that for L/K a cyclic extension of number fields, the Herbrand quotient $h(C_L)$ of the idèle class group of L is equal to $[L:K]$ (Theorem 7.1.1) and deduced that $\#H_T^0(\mathrm{Gal}(L/K), C_L) \geq [L:K]$ (the "First Inequality"; Theorem 7.1.2). This time we'll prove the reverse inequality, and even a somewhat stronger statement (see Theorem 7.2.10 below).

For this step, we have no local analogue to draw upon: the corresponding assertion in local class field theory is covered by Theorem 90 (Lemma 1.2.3). Unfortunately, there seems to be no direct approach to computing either $H_T^{-1}(\mathrm{Gal}(L/K), C_L)$ or $H^1(\mathrm{Gal}(L/K), C_L)$, so some alternate strategy is needed.

We take an analytic approach motivated by the proof of Dirichlet's theorem on primes in arithmetic progressions; see Lemma 7.2.7. There is also an algebraic approach, but we prefer to postpone discussing it until we are ready to tackle the existence theorem, as these two topics share similar ideas; see Theorem 7.4.14.

Back to ideals

For the analytic proof, we need to recast the Second Inequality back into classical, ideal-theoretic language. In this argument, there is no need to assume that L/K is cyclic.

Definition 7.2.1 Let L/K be a finite Galois extension and $\mathfrak{m}$ a formal product of places of K. As in Definition 2.2.3, let $J_K^{\mathfrak{m}}$ be the group of fractional ideals of K coprime to $\mathfrak{m}$; similarly, let $J_L^{\mathfrak{m}}$ be the group of fractional ideals of L coprime to $\mathfrak{m}$.

Let $I_K^{\mathfrak{m}}$ be the subset of $\alpha \in I_K$ such that:

1. for each finite prime $\mathfrak{p}$ of K, $\alpha_v \equiv 1 \pmod{\mathfrak{p}^e}$ where e is the exponent of $\mathfrak{p}$ in $\mathfrak{m}$;
2. for each real place v in $\mathfrak{m}$, $\alpha_v > 0$.

Define $I_L^{\mathfrak{m}}$ similarly.

Let $P_K^{\mathfrak{m}}$ be the subgroup of $J_K^{\mathfrak{m}}$ consisting of principal ideals admitting a generator $\alpha \in K^* \cap I_L^{\mathfrak{m}}$; define $P_L^{\mathfrak{m}}$ similarly. In this notation,

$$\mathrm{Cl}^{\mathfrak{m}}(K) = J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}, \qquad \mathrm{Cl}^{\mathfrak{m}}(L) = J_L^{\mathfrak{m}}/P_L^{\mathfrak{m}}.$$

The homomorphism $I_K \to J_K$ from Definition 6.2.5 restricts to a homomorphism $I_K^{\mathfrak{m}} \to J_K^{\mathfrak{m}}$, which in turn induces a surjective homomorphism $I_K^{\mathfrak{m}}/(K^* \cap I_K^{\mathfrak{m}}) \to \mathrm{Cl}^{\mathfrak{m}}(K)$. On the other hand, as indicated in Remark 6.2.6, we have $K^* I_K^{\mathfrak{m}} = I_K$ and hence $I_K^{\mathfrak{m}}/(K^* \cap I_K^{\mathfrak{m}}) \cong C_K$, yielding a surjection $C_K \to \mathrm{Cl}^{\mathfrak{m}}(K)$. ◊

Lemma 7.2.2 *With notation as in Definition 7.2.1, the composition*

$$C_K/\operatorname{Norm}_{L/K} C_L \cong I_K^{\mathfrak{m}}/(K^* \operatorname{Norm}_{L/K} I_L^{\mathfrak{m}}) \to J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \operatorname{Norm}_{L/K} J_L^{\mathfrak{m}}$$

is an isomorphism for some $\mathfrak{m}$.

Proof. The map in question is surjective because $I_K^{\mathfrak{m}} \to J_K^{\mathfrak{m}}$ is; we thus need to check injectivity for suitable $\mathfrak{m}$. Let S be the set of finite places of K which ramify in L. For each $v \in S$, apply local class field theory (see Theorem 4.1.5) to see that for w a place of L above v, the image of $\mathrm{Norm}_{L_w/K_v} L_w^*$ is an open subgroup U_v of K_v^* of finite index. We may then choose $\mathfrak{m}$ to include every real place and each place in S, and to ensure that for each $v \in S$, $(I_K^{\mathfrak{m}})_v \subseteq U_v$.

We now prove the claim for such a choice of $\mathfrak{m}$. Given an element of $I_K^{\mathfrak{m}}$ whose image in $J_K^{\mathfrak{m}}$ belongs to $P_K^{\mathfrak{m}} \operatorname{Norm}_{L/K} J_L^{\mathfrak{m}}$, we can factor it as an element of $K^* \cap I_K^{\mathfrak{m}}$ times an element of $\operatorname{Norm}_{L/K} I_L^{\mathfrak{m}}$ times an element $\alpha \in I_K^{\mathfrak{m}}$ such that for each finite place v, $\alpha_v \in \mathfrak{o}_{K_v}^*$. We see that $\alpha \in \operatorname{Norm}_{L/K} I_L^{\mathfrak{m}}$ by looking separately at real places (which are okay because these places appear in $\mathfrak{m}$), complex places (which are okay for trivial reasons), finite places in S (which are okay by our choice of $\mathfrak{m}$), and finite places not in S (which are okay because these places are unramified in L). ■

With Lemma 7.2.2 in hand, we can reduce the Second Inequality to proving that

$$[J_K^{\mathfrak{m}} : P_K^{\mathfrak{m}} \operatorname{Norm}_{L/K} J_L^{\mathfrak{m}}] \leq [L : K].$$

A special case of Chebotaryov density

We will need a special case of the Chebotaryov density theorem, which fortunately we can prove without already having all of class field theory. We use the notion of **Dirichlet density** for sets of prime ideals in a number field; see Definition 2.4.8 and the remainder of the discussion in Section 2.4.

Proposition 7.2.3 *Let L be a finite extension of K and let M/K be its Galois closure. Then the set S of prime ideals of K that split completely in L has Dirichlet density $1/[M : K]$ (in the sense of Definition 2.4.8).*

Proof. A prime of K splits completely in L if and only if it splits completely in M, so we may assume $L = M$ is Galois. Recall that the set T of unramfied primes $\mathfrak{q}$ of L of absolute degree 1 has Dirichlet density 1 (see Exercise 1 and Exercise 2); each such prime lies over an unramified prime $\mathfrak{p}$ of K of absolute degree 1 which splits completely in L.
The set T having Dirichlet density 1 means that

$$\sum_{\mathfrak{q} \in T} \frac{1}{\operatorname{Norm}(\mathfrak{q})^s} \sim \frac{1}{s-1} \qquad s \searrow 1$$

(s approaching 1 from above, that is). If we group the primes in T by which prime of S they lie over, then we get

$$[L : K] \sum_{\mathfrak{p} \in T} \frac{1}{\operatorname{Norm}(\mathfrak{p})^s} \sim \frac{1}{s-1}.$$

That is, the Dirichlet density of S is $1/[L : K]$. ■

Example 7.2.4 For $L/\mathbb{Q}$ a quadratic extension, Proposition 7.2.3 states that the set of prime ideals of $\mathbb{Q}$ that split completely in L has Dirichlet density $1/2$. As this splitting is governed by a congruence condition thanks to quadratic reciprocity, this assertion also follows from Dirichlet's theorem on primes in arithmetic progressions. □

This gives the following result about splitting of primes, which may be of independent interest.

Lemma 7.2.5 *With notation as in Definition 7.2.1, for any subgroup H of $J_K^{\mathfrak{m}}$ of finite index containing $P_K^{\mathfrak{m}}$, the set of primes in H has Dirichlet density equal to either 0 or $1/[J_K^{\mathfrak{m}} : H]$.*

Proof. For $\chi : J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to \mathbb{C}^*$ a character, we defined in Definition 2.4.4 the

L-function

$$L(s,\chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p}) \operatorname{Norm}(\mathfrak{p})^{-s}}.$$

By Theorem 2.4.2,

$$\log L(s,1) \sim \log \zeta_K(s) \sim \log \frac{1}{s-1} \qquad s \searrow 1,$$

while if χ is not the trivial character, by Theorem 2.4.5, $L(s,\chi)$ is holomorphic at $s = 1$. If $L(s,\chi) = (s-1)^{m(\chi)} g(s)$ where g is holomorphic and nonvanishing at $s = 1$, then $m(\chi) \geq 0$, and

$$\log L(s,\chi) \sim m(\chi) \log(s-1) = -m(\chi) \log \frac{1}{s-1}.$$

By discrete Fourier analysis (or equivalently orthogonality of characters),

$$\sum_{\chi : J_K^{\mathfrak{m}}/H \to \mathbb{C}^*} \log L(s,\chi) \sim [J_K^{\mathfrak{m}} : H] \sum_{\mathfrak{p} \in H} \frac{1}{\operatorname{Norm}(\mathfrak{p})^{-s}}.$$

We conclude that the set of primes in H has Dirichlet density

$$\frac{1 - \sum_{\chi \neq 1} m(\chi)}{[J_K^{\mathfrak{m}} : H]};$$

this is $1/[J_K^{\mathfrak{m}} : H]$ if the $m(\chi)$ are all zero and 0 otherwise. ■

Remark 7.2.6 Using Theorem 2.4.7 one can see that in the proof of Lemma 7.2.5, we must have $m(\chi) = 0$ for all $\chi \neq 1$; consequently, the set of primes in H cannot in fact have density 0. However, we will not need this refinement for the proof of the Second Inequality.

From the proof of Lemma 7.2.5, we see incidentally that at most one of the $m(\chi)$ can be nonzero, in which case it equals 1. This already implies that $m(\chi) = 0$ when χ is of order greater than 2, as in this case χ is distinct from its complex conjugate $\overline{\chi}$ but $m(\chi) = m(\overline{\chi})$.

The Second Inequality

We are now ready to prove the Second Inequality.

Lemma 7.2.7 *With notation as in Definition 7.2.1, we have*

$$[J_K^{\mathfrak{m}} : P_K^{\mathfrak{m}} \operatorname{Norm}_{L/K} J_L^{\mathfrak{m}}] \leq [L : K].$$

Proof. Define the group $H = P_K^{\mathfrak{m}} \operatorname{Norm}_{L/K} J_L^{\mathfrak{m}} \subseteq J_K^{\mathfrak{m}}$. The group H includes every prime of K that splits completely, since such a prime is the norm of any prime of L lying over it. Thus on one hand, by Proposition 7.2.3 the set of primes in H has Dirichlet density at least $1/[L : K]$. On the other hand, by Lemma 7.2.5 the same set has density either zero or $1/[J_K^{\mathfrak{m}} : H]$. We conclude that $[J_K^{\mathfrak{m}} : H] \leq [L : K]$, as desired. ■

Corollary 7.2.8 *Let L/K be a Galois extension of number fields. Then*

$$\#H_T^0(\operatorname{Gal}(L/K), C_L) \leq [L : K].$$

Proof. This follows from Lemma 7.2.7 by translating back into the language of idèles using Lemma 7.2.2. ■

Remark 7.2.9 We do not consider Corollary 7.2.8 to be a component of the Second Inequality because it is not needed in order to verify the class field axiom (and we will not reproduce it in the algebraic approach). In fact, once we complete the proofs of the reciprocity law (Theorem 6.4.1) and the norm limitation theorem (Theorem 6.4.3), Corollary 7.2.8 will also follow from those two statements together.

On the other hand, if one wants to avoid abstract class field theory, then it is helpful to have Corollary 7.2.8 in hand. See Remark 7.6.19.

Theorem 7.2.10 Second Inequality. *Let L/K be a Galois extension of number fields. Then:*

1. *the group $H^1(\mathrm{Gal}(L/K), C_L)$ is trivial;*
2. *the group $H^2(\mathrm{Gal}(L/K), C_L)$ is finite of order at most $[L:K]$.*

Proof. For L/K cyclic, combining Corollary 7.2.8 with the periodicity of Tate groups (Theorem 3.4.1) shows that $\#H^2(\mathrm{Gal}(L/K), C_L) \leq [L:K]$. Combining with the First Inequality (Theorem 7.1.2) yields that $H^1(\mathrm{Gal}(L/K), C_L)$ is trivial and $\#H^2(\mathrm{Gal}(L/K), C_L) = [L:K]$.
For L/K solvable, we may proceed by induction on $[L:K]$. If $[L:K]$ is not cyclic, choose an intermediate subextension K'/K . By the induction hypothesis, $H^1(\mathrm{Gal}(L/K'), C_{K'})$ vanishes, so we may apply the inflation-restriction exact sequence (Corollary 4.2.16) to see that for $i = 1, 2$,

$$0 \to H^i(\mathrm{Gal}(K'/K), C_{K'}) \stackrel{\mathrm{Inf}}{\to} H^i(\mathrm{Gal}(L/K), C_L) \stackrel{\mathrm{Res}}{\to} H^i(\mathrm{Gal}(L/K'), C_L)$$

is exact. This allows us to complete the induction.
For L/K general, put $G = \mathrm{Gal}(L/K)$, let p be a prime, and let G_p be a Sylow p-subgroup of G. Then for any $i > 0$, $H^i(G, C_L)$ is killed by the order of G and

$$\mathrm{Res} : H^i(G, C_L) \to H^i(G_p, C_L)$$

is injective on p-primary components (both by the relationship between restriction and corestriction, from Example 3.2.22). Since G_p is solvable, we may deduce both assertions from the solvable case. ■

Aside: the Hasse norm theorem

We record a byproduct of the Second Inequality (not needed in what follows).

Theorem 7.2.11 Hasse norm theorem. *Let L/K be a cyclic extension of number fields. Then an element $x \in K^*$ belongs to $\mathrm{Norm}_{L/K} L^*$ if and only if for each (finite or infinite) place v of K, for some (and hence every) place w of L lying over K, $x \in \mathrm{Norm}_{L_w/K_v} L_w^*$.*

Proof. By the Second Inequality (Theorem 7.2.10), $H_T^{-1}(G, C_L) = 1$. This implies that $H_T^0(G, L^*) \to H_T^0(G, I_L)$ is injective. Now if $x \in K^*$ belongs to $\mathrm{Norm}_{L_w/K_v} L_w^*$. then it defines the zero class in $H_T^0(G, I_L)$, so by the previous logic it must also define the zero class in $H_T^0(G, L^*)$; this proves the claim. ■

Remark 7.2.12 The conclusion of Theorem 7.2.11 fails completely if L/K is abelian but not cyclic. See Exercise 1.

Remark 7.2.13 Another related fact is the **Grunwald-Wang theorem**. It was originally announced (and published) in an incorrect form by Grunwald [16], who asserted that for K a number field and n a positive integer, an element $x \in K^*$ is an n-th power if and only if it is an n-th power in K_v for all but

finitely many places v of K.

It was then shown by Wang [53] that this statement fails in the following way: the element 16 is an 8th power in K_v for any place v not lying above 2 (see Exercise 2) but need not be an 8th power in K.

Finally, Wang [55] established a corrected version of the theorem, which shows that the original statement is "nearly" true. For example, it holds as written whenever n is odd.

The Albert-Brauer-Hasse-Noether theorem

We record another byproduct of the Second Inequality, called the **Albert-Brauer-Hasse-Noether theorem**.

Theorem 7.2.14 Albert-Brauer-Hasse-Noether theorem. *For any number field K, the map*

$$H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) \to \bigoplus_v H^2(\mathrm{Gal}(\overline{K_v}/K_v), \overline{K_v}^*)$$

is injective, where the sum runs over places v of K.

Proof. This follows from Theorem 7.2.10 via the exact sequence

$$1 = H^1(\mathrm{Gal}(L/K), C_L) \to H^2(\mathrm{Gal}(L/K), L^*) \to \bigoplus_v H^2(\mathrm{Gal}(L_w/K_v), L_w^*)$$

for any Galois extension L/K, where w denotes some place of L above K. ■

Exercises

1. Show that the Hasse norm theorem (Theorem 7.2.11) fails for $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. (This example is due to Serre and Tate.)

Hint. Prove that every square in L is a local norm, but 5^2 is not a global norm.

2. Show that in any field K of characteristic not equal to 2, 16 is an 8th power in K if and only if one of $-1, 2, -2$ is a square in K. Then deduce that for K a number field, 16 is an 8th power in K_v for any place v not lying above 2, even though it is not always an 8th power in K.

3. Put $K = \mathbb{Q}(\sqrt{7})$. Show that 16 is an 8th power in every completion of K, but not in K itself.

4. Let K be a number field and choose $a, b, c \in K^*$. Prove that the equation $ax^2 + by^2 + c^2 = 0$ has a solution with $x, y, z \in K$ not all zero if and only if for each place v of K, there exists a solution with $x, y, z \in K_v$ not all zero. (This is a special case of the **Hasse-Minkowski theorem**.)

Hint. The equation has a solution in K if and only if $-c$ is a norm from $K(\sqrt{-b/a})$ to K.

7.3 An "abstract" reciprocity map

Reference. [36] VII.5; [37] VI.4, but only loosely.

We next manufacture a canonical isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to C_K / \mathrm{Norm}_{L/K} C_L$ for any finite extension L/K of number fields, where C_K and C_L are the corresponding idèle class groups (Theorem 7.3.8). However, we won't yet know it agrees with our proposed reciprocity map, which is the product of the local

reciprocity maps. We'll come back to this point after we establish the existence theorem (see Section 7.5).

Abstract unit groups and the class field axiom

We will be applying abstract class field theory with $k = \mathbb{Q}$ and $\overline{k} = \overline{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$. We first specify the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module A which will give rise to abstract unit groups.

Definition 7.3.1 Set $A = \bigcup_K C_K$; by Corollary 6.3.7, $A_K = C_K$ for every number field K. Our earlier calculations (Theorem 7.1.2, Theorem 7.2.10) imply that the class field axiom is satisfied: for L/K a cyclic extension of number fields,

$$\#H_T^0(\mathrm{Gal}(L/K), C_L) = [L : K], \qquad \#H_T^1(\mathrm{Gal}(L/K), C_L) = 1.$$

$\Diamond$

Remark 7.3.2 In Definition 7.3.1, it will follow from the reciprocity law that the group $H_T^0(\mathrm{Gal}(L/K), C_L)$ is cyclic. However, the class field axiom does not require advance knowledge of this.

Cyclotomic extensions and abstract ramification theory

The cyclotomic extensions of a number field play a role in class field theory analogous to the role played by the unramified extensions in local class field theory. This makes it essential to make an explicit study of them for use in proving the main results. However, we will not need the Kronecker-Weber theorem (Theorem 1.1.2); instead, we will recover it as part of the reciprocity law.

We first make a distinction which is of marginal significance in the totality of number theory, but is critical for our use of the machinery of abstract class field theory.

Definition 7.3.3 The extension $\bigcup_n \mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ obtained by adjoining all roots of unity has Galois group $\widehat{\mathbb{Z}}^* = \prod_p \mathbb{Z}_p^*$. That group has a lot of torsion, since each $\mathbb{Z}_p^*$ contains a torsion subgroup of order $p-1$ (or 2, if $p = 2$).

If we take the fixed field for the torsion subgroup of $\mathbb{Z}^*$, we get a slightly smaller extension, which I'll call the **small cyclotomic extension** of $\mathbb{Q}$ and denote $\mathbb{Q}^{\mathrm{smcy}}$. Its Galois group is isomorphic to $\prod_p \mathbb{Z}_p = \widehat{\mathbb{Z}}$, but *not canonically so*.

For K a number field, define $K^{\mathrm{smcy}} = K\mathbb{Q}^{\mathrm{smcy}}$. Then $\mathrm{Gal}(K^{\mathrm{smcy}}/K) \cong \widehat{\mathbb{Z}}$ as well, even if K contains some extra roots of unity. $\Diamond$

With this definition in hand, we can set up the homomorphism d needed to define abstract ramification theory for the base field $k = \mathbb{Q}$.

Definition 7.3.4 Choose an isomorphism of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q})$ with $\widehat{\mathbb{Z}}$; our results are not going to depend on the choice (see Remark 7.3.11). That gives a continuous surjection

$$d : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}};$$

recall that this means we are going to regard $\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q}$ as the "maximal unramified extension" of $\mathbb{Q}$.

As in the general setup, for any finite extension L/K of number fields, we define the **abstract ramification index** $e_{L/K}$ and the **abstract inertia**

degree $f_{L/K}$ by setting

$$f_{L/K} = [L \cap \mathbb{Q}^{\text{smcy}} : K \cap \mathbb{Q}^{\text{smcy}}], \qquad e_{L/K} = \frac{[L:K]}{f_{L/K}}.$$

◊

An abstract henselian valuation

To complete the setup of abstract class field theory, we need an **abstract henselian valuation** $v : C_{\mathbb{Q}} \to \widehat{\mathbb{Z}}$ with respect to d. Recall from Definition 5.1.8 that this means:

1. $v(C_{\mathbb{Q}})$ is a subgroup Z of $\widehat{\mathbb{Z}}$ containing $\mathbb{Z}$ with $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$ for all positive integers n;
2. $v(\text{Norm}_{K/\mathbb{Q}} C_K) = f_{K/\mathbb{Q}} Z$ for all finite extensions $K/\mathbb{Q}$.

Definition 7.3.5 To define the map v, we write

$$I_{\mathbb{Q}} = \mathbb{Q}^* \times \mathbb{R}^+ \times \widehat{\mathbb{Z}}^*$$

as in Remark 6.2.12. We then define v as the projection onto the third factor followed by the projection

$$\widehat{\mathbb{Z}}^* \cong \text{Gal}(\mathbb{Q}^{\text{cyc}}/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}^{\text{smcy}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}.$$

The first condition of Definition 5.1.8 holds by construction. We will check the second condition using Artin reciprocity for cyclotomic extensions. ◊

Lemma 7.3.6 *The map v defined in Definition 7.3.5 is a henselian valuation in the sense of Definition 5.1.8 (with respect to the map d from Definition 7.3.4).*

Proof. Since we already know from Definition 7.3.5 that v factors through $C_{\mathbb{Q}}$ and surjects onto $\widehat{\mathbb{Z}}$, it suffices to check that for every number field K, $v(\text{Norm}_{K/\mathbb{Q}} I_K) = f_{K/\mathbb{Q}}\widehat{\mathbb{Z}}$. We may establish this by checking that the map

$$I_K \overset{\text{Norm}_{K/\mathbb{Q}}}{\to} I_{\mathbb{Q}} \to \text{Gal}(\mathbb{Q}^{\text{cyc}}/\mathbb{Q})$$

has image $\text{Gal}(K^{\text{cyc}}/K) \subseteq \text{Gal}(\mathbb{Q}^{\text{cyc}}/\mathbb{Q})$, as then we get the desired condition by projecting from $\text{Gal}(\mathbb{Q}^{\text{cyc}}/\mathbb{Q})$ to $\text{Gal}(\mathbb{Q}^{\text{smcy}}/\mathbb{Q})$. Note that for $K = \mathbb{Q}$, this follows from Artin reciprocity for cyclotomic extensions (Definition 1.1.7).
In one direction, the fact that I_K maps into $\text{Gal}(K^{\text{cyc}}/K)$ is a corollary of local reciprocity (Theorem 4.1.2) plus Artin reciprocity for cyclotomic extensions as used above.
In the other direction, the same logic shows that for each positive integer n, the image of I_K in $\text{Gal}(K(\zeta_n)/K)$ equals the image of the classical Artin map for $K(\zeta_n)/K$; it will thus suffice to check that these maps are surjective. It is convenient to deduce this from the First Inequality; see Proposition 7.3.7 below. ■

Here is the consequence of the First Inequality used in the proof of Lemma 7.3.6.

Proposition 7.3.7 *For L/K an abelian extension of number fields, the Artin map always surjects onto* $\text{Gal}(L/K)$.

Proof. Let H be the image of the Artin map; the fixed field M of H has the property that all but finitely many primes of K split completely in M. We've already seen that this contradicts the First Inequality unless $M = K$

(Corollary 7.1.16). ■

Consequences of abstract CFT

We now apply abstract class field theory to obtain an "abstract adelic reciprocity law".

Theorem 7.3.8 Abstract adelic reciprocity law. *For every Galois extension L/K of number fields, we obtain an isomorphism*

$$r'_{L/K} : C_K / \operatorname{Norm}_{L/K} C_L \xrightarrow{\sim} \operatorname{Gal}(L/K)^{\mathrm{ab}}.$$

Proof. The hypotheses of abstract class field theory are satisfied by taking $k = \mathbb{Q}$ $\overline{k} = \overline{\mathbb{Q}}$; $A = \bigcup_K C_K$ as in Definition 7.3.1 (using Theorem 7.1.2 and Theorem 7.2.10 to verify the class field axiom); $d : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}$ as in Definition 7.3.4; and $v : C_{\mathbb{Q}} \to \widehat{\mathbb{Z}}$ as in Definition 7.3.5 (using Lemma 7.3.6). We may thus apply Theorem 5.3.9 to conclude. ■

Definition 7.3.9 By Proposition 5.2.7, the maps $r'_{L/K}$ from Theorem 7.3.8 fit together to give a map $r'_K : C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$; but we do not yet know that this coincides with the product of the local reciprocity maps, so we cannot yet recover Artin reciprocity. However, we can at least deduce the norm limitation theorem (Theorem 6.4.3). See also Remark 7.3.11 below. ◊

Theorem 7.3.10 Norm limitation theorem. *If L/K is a finite extension of number fields and $M = L \cap K^{\mathrm{ab}}$, then* $\operatorname{Norm}_{L/K} C_L = \operatorname{Norm}_{M/K} C_M$.

Proof. Apply Corollary 5.3.11. ■

Remark 7.3.11 Although we do not have a complete description of the isomorphism $r'_{L/K}$ coming from abstract class field theory, we do know one specific fact about this map: for "unramified" extensions L/K (i.e., $L \subseteq K^{\mathrm{smcy}}$), the "Frobenius" in $\operatorname{Gal}(L/K)$ maps to a "uniformizer" in C_K. That is, the element of $\operatorname{Gal}(L/K)$ coming from the element of $\operatorname{Gal}(K^{\mathrm{smcy}}/K)$ which maps to 1 under d_K corresponds via reciprocity to the element of C_K which maps to 1 under v_K.

The broader point here is that the definitions of both d and v involve the *same* artificial choice of an isomorphism $\operatorname{Gal}(\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}$, which thus does not affect the reciprocity map. Compare Remark 5.1.11 and Exercise 4.

7.4 The existence theorem

Reference. [36] VII.6, VII.9, [37] VI.4, VI.6.

With the "abstract" reciprocity theorem in hand, we now prove the existence theorem in its idelic formulation (see Theorem 6.4.2). Modulo the pending reconciliation of Artin reciprocity with abstract reciprocity (see Proposition 7.5.7), this will imply the classical version of the existence theorem: every generalized ideal class group of a number field is identified by Artin reciprocity with the Galois group of a suitable abelian extension (Theorem 2.2.8).

As in the proof of the local existence theorem (Theorem 4.3.11), having access to the (abstract) reciprocity law and the norm limitation theorem reduces the task of proving the existence theorem to the "topological" assertion that every open subgroup of C_L of finite index contains a norm subgroup. For this, we can essentially rerun the Kummer-theoretic argument from the local case.

We then give the closely related algebraic proof of the Second Inequality (Theorem 7.2.10).

A base case for the existence theorem

As in the proof of the local existence theorem (Theorem 4.3.11), the key to the proof of Theorem 7.4.8 is showing that for any given number field K, we can find finite extensions L/K for which the groups $\mathrm{Norm}_{L/K} C_L$ can be made arbitrarily small. In preparation for an inductive proof, we establish a key base case using Kummer theory.

Lemma 7.4.1 *Let K be a number field containing a primitive p-th root of unity for some prime p. Let U be an open subgroup of C_K of index p. Then for some finite set S of places of K containing the infinite places and all places above p, $I_K = K^* I_{K,S}$ and the preimage of U in $I_{K,S}$ contains*

$$W_S = \prod_{v \in S} (K_v^*)^p \times \prod_{v \notin S} \mathfrak{o}_{K_v}^*.$$

Proof. Let J be the preimage of U under the projection $I_K \to C_K$, so that J is open in I_K of finite index. Then J contains a subgroup of the form

$$V = \prod_{v \in S} \{1\} \times \prod_{v \notin S} \mathfrak{o}_{K_v}^*$$

for some finite set S of places of K containing the infinite places, which by Corollary 6.2.10 we may choose large enough so that $K^* I_{K,S} = I_K$. The group J must also contain I_K^p, and hence W_S. ∎

We continue with a lemma that allows to detect whether certain elements of a number field are p-th powers based on whether this happens locally. This amounts to a carefully chosen special case of the Grunwald-Wang theorem (Remark 7.2.13).

Lemma 7.4.2 *With notation as in Lemma 7.4.1,*

$$W_S \cap K^* = (\mathfrak{o}_{K,S}^*)^p.$$

Proof. It is clear that

$$(\mathfrak{o}_{K,S}^*)^p \subseteq W_S \cap K^*.$$

To prove the reverse inclusion, note that for any $y \in W_S \cap K^*$, if we set $L = K(y^{1/p})$, then every place $v \in S$ is split in L and every place $v \notin S$ is unramified in L, yielding

$$\mathrm{Norm}_{L/K} I_{L,S} = I_{K,S}.$$

Since $I_K = K^* I_{K,S}$, this implies $\mathrm{Norm}_{L/K} C_L = C_K$. By the First Inequality (Theorem 7.1.2), this implies $L = K$ and so $y \in (K^*)^p$. ∎

This will in turn enable us to compute the norm group for a certain compositum of Kummer extensions.

Lemma 7.4.3 *With notation as in Lemma 7.4.1, put $s = \#S$ and*

$$L = K(u^{1/p} : u \in \mathfrak{o}_{K,S}^*).$$

Then $[L : K] = p^s$ and

$$\mathrm{Norm}_{L/K} C_L = K^* W_S / K^* \subset C_K.$$

Proof. By Corollary 6.2.11 and the assumption that K contains a primitive p-th root of unity, the group $\mathfrak{o}_{K,S}^*/(\mathfrak{o}_{K,S}^*)^p$ is finite of order p^s, yielding $[L : K] = p^s$.

By local reciprocity (Lemma 4.3.8), we have $K^*W_S/K^* \subseteq \mathrm{Norm}_{L/K} C_L$; to prove equality, it will suffice to check that these groups have the same index in C_K.
Consider now the exact sequence

$$1 \to \frac{\mathfrak{o}_{K,S}^*}{\mathfrak{o}_{K,S}^* \cap W_S} \to \frac{I_{K,S}}{W_S} \to \frac{C_K}{K^*W_S/K^*} \to 1.$$

By Lemma 7.4.2, the group on the left has order $[\mathfrak{o}_{K,S}^* : (\mathfrak{o}_{K,S}^*)^p] = p^s$. By Lemma 7.4.4, the group in the middle has order p^{2s}. Thus using the abstract global reciprocity isomorphism (Theorem 7.3.8), we obtain

$$[C_K : K^*W_S/K^*] = p^s = [L : K] = [C_K : \mathrm{Norm}_{L/K} C_L],$$

as desired. ■

Here is the local calculation used in the proof of Lemma 7.4.3.

Lemma 7.4.4 *For K a number field, v a place of K, and p a prime such that $\zeta_p \in K$,*

$$[K_v^* : (K_v^*)^p] = \frac{p^2}{|p|_v}.$$

Proof. We separate cases as follows.

1. If v is a real place, then $p = 2$, $p^2/|p|_v = 2$, and
$$K_v^*/(K_v^*)^p = \mathbb{R}^*/(\mathbb{R}^*)^2 = \mathbb{R}^*/\mathbb{R}^+ \cong \mathbb{Z}/2\mathbb{Z}.$$
2. If v is a complex place, then $p^2/|p|_v = 1$ according to our conventions (Definition 6.1.10), and $K_v^*/(K_v^*)^p$ is trivial because $\mathbb{C}^*$ is p-divisible.
3. If v is a finite place not lying above p, then $p^2/|p|_v = p^2$ and $K_v^*/(K_v^*)^p$ is generated by ζ_p and a uniformizer of K_v.
4. If v is a finite place above p, then $|p|_v = p^{-n}$ for some positive integer n, so $p^2/|p|_v = p^{n+2}$. Since $K_v^* \cong \mathfrak{o}_{K_v}^* \times \mathbb{Z}$, it suffices to check that $[\mathfrak{o}_{K_v}^* : (\mathfrak{o}_{K_v}^*)^p] = p^{n+1}$. For this, see Exercise 1.

■

We finally put everything together to get a key special case of the existence theorem.

Lemma 7.4.5 *Let K be a number field containing a primitive p-th root of unity for some prime p. Let U be an open subgroup of C_K of index p. Then there exists a finite extension L of K such that* $\mathrm{Norm}_{L/K} C_L \subseteq U$.

Proof. This now follows from Lemma 7.4.1 and Lemma 7.4.3. which by Corollary 6.2.10 we may choose large enough so that $K^*I_{K,S} = I_K$. ■

Proof of the existence theorem

Building on the base case offered by Lemma 7.4.5, we now finish the proof of the existence theorem.

Lemma 7.4.6 *Let K be a number field. Let U be an open subgroup of C_K of some prime index p. Then there exists a finite extension L of K such that* $\mathrm{Norm}_{L/K} C_L \subseteq U$.

Proof. Take $K' = K(\zeta_p)$. Let U' be the inverse image of U in $C_{K'}$. By Theorem 7.3.8, $[C_K : \mathrm{Norm}_{K'/K} C_{K'}] = [K' : K]$ is coprime to p; consequently, $[C_{K'} : U'] = p$. By Lemma 7.4.5, there exists a finite extension L/K' such that $\mathrm{Norm}_{L/K'} C_L \subseteq U'$; then $\mathrm{Norm}_{L/K} C_L \subseteq \mathrm{Norm}_{K'/K} U' \subseteq U$. ■

Lemma 7.4.7 *Let K be a number field. Let U be an open subgroup of C_K of finite index. Then there exists a finite extension L of K such that $\mathrm{Norm}_{L/K} C_L \subseteq U$.*

Proof. We proceed by induction on the index $[C_K : U]$, with Lemma 7.4.6 as the base case. Otherwise, choose an intermediate subgroup V between U and C_K. By the induction hypothesis, V contains $N = \mathrm{Norm}_{L/K} C_L$ for some finite extension L of K. Then

$$[N : (U \cap N)] = [UN : U] \leq [V : U].$$

Let W be the subgroup of C_L consisting of those x whose norms lie in U. Then

$$[C_L : W] \leq [N : U \cap N] \leq [V : U],$$

so by the induction hypothesis W contains $\mathrm{Norm}_{M/L} C_M$ for some finite extension M/L. Thus U contains $\mathrm{Norm}_{M/K} C_M$, as desired. ■

Theorem 7.4.8 Adelic existence theorem. *For K a number field, the finite abelian extensions L/K are in bijection with the open subgroups of C_K of finite index via the map $L \mapsto \mathrm{Norm}_{L/K} C_L$.*

Proof. For any finite abelian extension L/K, $\mathrm{Norm}_{L/K} C_L$ is a subgroup of C_K which is open (by Remark 7.1.7) of index $[L : K]$ (by Theorem 7.3.8). Moreover, by Corollary 5.3.13, the correspondence $L \mapsto \mathrm{Norm}_{L/K} C_L$ is injective.
Conversely, let U be an open subgroup of C_K of finite index. By Lemma 7.4.7, there exists a finite extension L_1/K such that $\mathrm{Norm}_{L_1/K} C_{L_1} \subseteq U$. By the adelic norm limitation theorem (Theorem 6.4.3), we also have $\mathrm{Norm}_{L_1/K} C_{L_1} = \mathrm{Norm}_{L_2/K} C_{L_2} \subseteq U$ for L_2/K the maximal abelian subextension of L_1/K. By Theorem 7.3.8 again, we have an isomorphism $\mathrm{Gal}(L_2/K) \cong C_K/\mathrm{Norm}_{L_2/K} C_{L_2}$, via which the subgroup $U/\mathrm{Norm}_{L_2/K} C_{L_2}$ corresponds to a subgroup H of $\mathrm{Gal}(L_2/K)$. Taking L to be the fixed field of H, we deduce that $\mathrm{Norm}_{L/K} C_L = U$ as desired. ■

Remark 7.4.9 As with the proof of the local existence theorem, the proof of Theorem 7.4.8 is constructive in principle but not in practice: it involves constructing some extension much larger than the desired abelian extension, then invoking the norm limitation theorem to get down to an abelian extension. We remind the reader that there is no easy fix known for this (Remark 2.2.10).

An algebraic approach to the Second Inequality

Drawing inspiration from the calculation of norm groups given in Lemma 7.4.3, we now explain how to use similar ideas to give an algebraic proof of the Second Inequality. Again, the key case is where L/K is a cyclic extension of number fields of prime degree p and $\zeta_p \in K$. To modify the calculation from Lemma 7.4.3 to compute the norm group of a single Kummer extension, we use a second set of places.

Lemma 7.4.10 *Let K be a number field containing ζ_p for some prime p. Let L/K be a cyclic extension of number fields of degree p. We can then choose the following.*

1. *A finite set S of s places of K containing all infinite places, all places that ramify in L, and all places above p, for which $I_K = I_{K,S}K^*$.*

2. *A second set T of $s-1$ places of K disjoint from S, such that $\mathfrak{o}_{K,S}^* \to \prod_{v\in T} K_v^*/(K_v^*)^p$ is surjective with kernel Δ and $L = K(\Delta^{1/p})$.*

Proof. By Kummer theory (Theorem 1.2.6), we can choose a finite set S of places of K containing all infinite places, all places that ramify in L, and all places above p so that $L = K(\Delta^{1/p})$ for $\Delta = \mathfrak{o}_{K,S}^* \cap (L^*)^p$. This remains true after enlarging S, so by Corollary 6.2.10 we can further ensure that $I_K = I_{K,S}K^*$. Put $N = K((\mathfrak{o}_{K,S}^*)^{1/p})$. By Kummer theory again

$$\mathrm{Gal}(N/K) \cong \mathrm{Hom}(\mathfrak{o}_{K,S}^*/(\mathfrak{o}_{K,S}^*)^p, \mathbb{Z}/p\mathbb{Z}).$$

By Corollary 6.2.11, $\mathfrak{o}_{K,S}^*/(\mathfrak{o}_{K,S}^*)^p \cong (\mathbb{Z}/p\mathbb{Z})^s$. Choose generators $g_1, \dots, g_{s-1}$ of $\mathrm{Gal}(N/L)$; these correspond in $\mathrm{Hom}(\mathfrak{o}_{K,S}^*/(\mathfrak{o}_{K,S}^*)^p, \mathbb{Z}/p\mathbb{Z})$ to a set of homomorphisms whose common kernel is precisely $\Delta/(\mathfrak{o}_{K,S}^*)^p$. We thus need to find, for each g_i, a place v_i such that the kernel of g_i is the same as the kernel of $\mathfrak{o}_{K,S}^* \to K_{v_i}^*/(K_{v_i}^*)^p$; we can then take $T = \{v_1, \dots, v_{s-1}\}$.
Let N_i be the fixed field of g_i; by Corollary 7.1.16 (which we deduced from the First Inequality), there are infinitely many primes of N_i that do not split in N. So we can choose a place w_i of each N_i such that their restrictions v_i to K are distinct, not contained in S, and don't divide p.
We claim N_i is the maximal subextension of N/K in which v_i splits completely (i.e., the **decomposition field** of v_i). On one hand, v_i does not split completely in N, so the decomposition field is no larger than N_i. On the other hand, the decomposition field is the fixed field of the decomposition group, which has exponent p and is cyclic (since v_i does not ramify in N). Thus it must have index p in N, so must be N_i itself.
Thus $L = \bigcap N_i$ is the maximal subextension of N in which all of the v_i split completely. We conclude that for $x \in \mathfrak{o}_{K,S}^*$, x belongs to Δ iff $K_{v_i}(x^{1/p}) = K_{v_i}$ for all i, which occurs iff $x \in K_{v_i}^p$. That is, Δ is precisely the kernel of the map $\mathfrak{o}_{K,S}^* \to \prod_i K_{v_i}^*/(K_{v_i}^*)^p$. This proves the claim. ∎

We have the following modified version of Lemma 7.4.2.

Lemma 7.4.11 *With notation as in Lemma 7.4.10, write*

$$W_{S,T} = \prod_{v\in S} (K_v^*)^p \times \prod_{v\in T} K_v^* \times \prod_{v\notin S\cup T} \mathfrak{o}_{K_v}^*.$$

Then

$$W_{S,T} \cap K^* = (\mathfrak{o}_{K,S\cup T}^*)^p.$$

Proof. It is again clear that

$$(\mathfrak{o}_{K,S\cup T}^*)^p \subseteq W_{S,T} \cap K^*.$$

To prove the reverse inclusion, it will again suffice to prove that $y \in W_{S,T} \cap K^*$, if we set $L = K(y^{1/p})$, then $\mathrm{Norm}_{L/K} C_L = C_K$; namely, Theorem 7.1.2 will then imply $L = K$ and so $y \in (K^*)^p$.
Since $\mathfrak{o}_{K,S}^* \to \prod_{v\in T} \mathfrak{o}_{K_v}^*/(\mathfrak{o}_{K_v}^*)^p$ is surjective, any element of $I_{K,S\cup bigT}$ can be written as the product of an element of $\mathfrak{o}_{K,S}^*$ with an element of $I_{K,S\cup T}$ which is a p-th power at each place of T. In particular, by Lemma 4.3.8 such an element is a norm from L at each place of T; we can now reprise the proof of Lemma 7.4.2, skipping over the places in T, to deduce that we have a norm from L. ∎

Lemma 7.4.12 *With notation as in Lemma 7.4.10 and Lemma 7.4.11, $K^*W_{S,T}/K^*$ is contained in $\mathrm{Norm}_{L/K} C_L$ and has index p in C_K. Consequently, the Second Inequality holds for L/K.*

Proof. By Lemma 7.4.11, we have an exact sequence

$$1 \to \frac{\mathfrak{o}^*_{K,S\cup T}}{(\mathfrak{o}^*_{K,S\cup T})^p} \to \frac{I_{K,S\cup T}}{W_{S,T}} \to \frac{C_K}{K^*W_{S,T}/K^*} \to 1,$$

with which we may compute as in Lemma 7.4.3: the left group has order $p^{\#(S\cup T)} = p^{2s-1}$ by Corollary 6.2.11 while the middle group has order p^{2s} by Lemma 7.4.4, so

$$[C_K : K^*W_{S,T}/K^*] = p.$$

Meanwhile, we can check by local reciprocity that $\mathrm{Norm}_{L/K} I_{L,S} = I_{K,S}$ (compare the proof of Lemma 7.4.11).

- For $v \in S$, elements of $(K_v^*)^p$ are norms from any abelian extension of K_v of exponent p (by Lemma 4.3.8).
- For $v \in T$, v splits in L and so $L_w = K_v$.
- For $v \notin S \cup T$, v is unramified in L and so $\mathrm{Norm}_{L_w/K_v} \mathfrak{o}^*_{L_w} = \mathfrak{o}^*_{K_v}$.

Dence $K^*W_{S,T} \subseteq \mathrm{Norm}_{L/K} C_L$, completing the proof. ∎

Lemma 7.4.13 *Let L/K be a cyclic extension of number fields of prime degree p and let $K' = K(\zeta_p), L' = L(\zeta_p)$. Then the map*

$$H^0_T(\mathrm{Gal}(L/K), C_L) \to H^0_T(\mathrm{Gal}(L'/K'), C_{L'})$$

induced by the inclusion $C_L \to C_{L'}$ is injective.

Proof. For $x \in C_K$, $\mathrm{Norm}_{L/K}(x) = x^p$; this implies that both groups in question are killed by p. In particular, multiplication by $d = [K' : K]$, which divides $p-1$, is an isomorphism on these groups.
Suppose $x \in C_K$ maps to the identity in $H^0_T(\mathrm{Gal}(L'/K'), C_{L'})$. We can then choose a representative of class of x in $H^0_T(\mathrm{Gal}(L/K), C_L)$ of the form y^d; then y also maps to the identity in $H^0_T(\mathrm{Gal}(L'/K'), C_{L'})$. That is, $y = \mathrm{Norm}_{L'/K'}(z')$ for some $z' \in C_{L'}$, and

$$y^d = \mathrm{Norm}_{K'/K}(y) = \mathrm{Norm}_{L'/K}(z') \in \mathrm{Norm}_{L/K} C_L.$$

Thus $x \in \mathrm{Norm}_{L/K} C_L$, as needed. ∎

Theorem 7.4.14 Second Inequality (algebraic proof). *Let L/K be a Galois extension of number fields with Galois group G. Then:*

1. *the group $H^1(G, C_L)$ is trivial;*
2. *the group $H^2(G, C_L)$ is finite of order at most $[L : K]$.*

Proof. As in the proof of Theorem 7.2.10, we use an induction argument to reduce to proving that for L/K cyclic,

$$H^0_T(\mathrm{Gal}(L/K), C_L) \leq [L : K].$$

In fact, the same induction (considering H^2 in place of H^0_T) allows us to further reduce to the case where $[L : K] = p$ is prime.
Let $K' = K(\zeta_p)$ and $L' = L(\zeta_p)$; then K' and L are linearly disjoint over K (since their degrees are coprime), so $[L' : K'] = [L : K] = p$ and the Galois

groups of L/K and L'/K' are canonically isomorphic. By Lemma 7.4.12 and Lemma 7.4.13,

$$\#H^0_T(\mathrm{Gal}(L/K), C_L) \leq \#H^0_T(\mathrm{Gal}(L'/K'), C_{L'}) \leq [L' : K'] = p$$

as desired. ■

Exercises

1. Complete the proof of Lemma 7.4.4 by showing that if $|p|_v = p^{-n}$ for some positive integer n, then $[\mathfrak{o}^*_{K_v} : (\mathfrak{o}^*_{K_v})^p] = p^{n+1}$. (Remember that K is a number field containing a primitive p-th root of unity.)

Hint. Using the logarithm map, we obtain an isomorphism $\mathfrak{o}^*_{K_v}/\mu_{K_v} \cong \mathbb{Z}_p^n$ (even when $p = 2$). See [37], Proposition II.5.7 for details.

2. Let K be a number field. Prove that for every positive integer n, C_K^n is the intersection of the norm groups $\mathrm{Norm}_{L/K} C_L$ over all abelian extensions L/K of exponent n.

7.5 Local-global compatibility

Reference. [37] VI.5.

Let L/K be a Galois extension of number fields. So far, we've used abstract class field theory to construct reciprocity isomorphisms and to establish the adelic form of the existence theorem (Theorem 7.4.8).

It remains to verify that the "abstract" reciprocity map coincides with the product of the local reciprocity maps (Definition 6.4.4). As noted earlier, this is enough to recover the classical Artin reciprocity law (Proposition 6.4.7); this will finally complete the proof of all of the statements originally asserted in Chapter 2).

Compatibility for cyclotomic extensions

Definition 7.5.1 Let L/K be a Galois extension of number fields. Let

$$r_{L/K} : I_K \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

be the product of the local reciprocity maps Definition 6.4.4. Meanwhile, let

$$r'_{L/K} : I_K \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

be the map obtained by inverting the isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to C_K/\mathrm{Norm}_{L/K} C_L$ given by Theorem 7.3.8. ◊

As a base case for our work, we need to know that $r_{L/K} = r'_{L/K}$ when L is contained in a small cyclotomic extension. Note that this is very similar to the proof that the map v is an abstract henselian valuation (Lemma 7.3.6).

Lemma 7.5.2 *With notation as in Definition 7.5.1, suppose that $L \subset K^{\mathrm{smcy}}$. Then $r_{L/K} = r'_{L/K}$.*

Proof. In the setting of abstract class field theory, L/K is viewed as an "unramified" extension. Consequently, the reciprocity map $r'_{L/K} : C_K/\mathrm{Norm}_{L/K} C_L \to \mathrm{Gal}(L/K)$ is described completely by Lemma 5.3.1: it is given by composing the valuation map $v_K : C_K \to \widehat{\mathbb{Z}}$ with the inverse of the map

$d_K : \mathrm{Gal}(K^{\mathrm{smcy}}/K) \cong \widehat{\mathbb{Z}}$, then projecting from $\mathrm{Gal}(K^{\mathrm{smcy}}/K)$ to $\mathrm{Gal}(L/K)$. (Note that as per Remark 7.3.11, this does not depend on the artificial choice of the isomorphism d_K, because v_K is defined using the same choice.) Consequently, in this case we end up with the usual Artin map for a cyclotomic extension (Definition 1.1.7), which is compatible with local reciprocity by direct calculation (Example 4.1.4). ■

For the purposes of illustration, we sketch an alternate approach to that calculation in terms of Lubin-Tate formal groups. This approach has the benefit that it does not depend on global reciprocity, and so can be adapted more easily to extensions which are not cyclotomic.

Lemma 7.5.3 *Via the identifications* $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$ *with* $(\mathbb{Z}/p^m\mathbb{Z})^*$*, we have*

$$r_{\mathbb{Q}_\ell(\zeta_{p^m})/\mathbb{Q}_\ell}(a) = \begin{cases} \mathrm{sign}(a) & \ell = \infty \\ \ell^{v_\ell}(a) & \ell \neq \infty, p \\ u^{-1} & \ell = p. \end{cases}$$

Proof. This is straightforward for $\ell = \infty$. For $\ell \neq \infty, p$, we have an unramified extension of local fields, where we know the local reciprocity map takes a uniformizer to a Frobenius. In this case the latter is simply ℓ.
The hard work is in the case $\ell = p$. For that computation one uses what amounts to a very special case of the Lubin-Tate construction of explicit class field theory for local fields, using formal groups. Put $K = \mathbb{Q}_p$, $\zeta = \zeta_{p^m}$ and $L = \mathbb{Q}_p(\zeta)$.
Suppose without loss of generality that u is a positive integer, and let $\sigma \in \mathrm{Gal}(L/K)$ be the automorphism corresponding to u^{-1}. Since L/K is totally ramified at p, we have $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}})$, and we can view σ as an element of $\mathrm{Gal}(L^{\mathrm{unr}}/K)$. Let $\phi_L \in \mathrm{Gal}(L^{\mathrm{unr}}/L)$ denote the Frobenius, and put $\tau = \sigma\phi_L$. Then τ restricts to the Frobenius in $\mathrm{Gal}(K^{\mathrm{unr}}/K)$ and to σ in $\mathrm{Gal}(L/K)$. As per Definition 5.2.1, we may compute $r_{L/K}^{-1}(\sigma)$ as $\mathrm{Norm}_{M/K}\, \pi_M$, where M is the fixed field of τ and π_M is a uniformizer. We want that norm to be u times a norm from L to K, i.e.,

$$r_{L/K}^{-1}(\sigma) \in u\,\mathrm{Norm}_{L/K}\, L^*.$$

Define the polynomial

$$e(x) = x^p + upx$$

and put

$$P(x) = e^{(n-1)}(x)^{p-1} + pu,$$

where $e^{(k+1)}(x) = e(e^{(k)}(u))$. Then $P(x)$ satisfies Eisenstein's criterion, so its splitting field over $\mathbb{Q}_p$ is totally ramified, any root of P is a uniformizer, and the norm of said uniformizer is $(-1)^{[L:K]}pu \in \mathrm{Norm}_{L/K}\, L^*$, since $\mathrm{Norm}_{L/K}(\zeta - 1) = (-1)^{[L:K]}(p)$.
The punch line is that the splitting field of $P(x)$ is precisely M! Here is where the Lubin-Tate construction comes to the rescue... and where I will stop this sketch. See [37] V.2, V.4 and/or [36] I.3. ■

Compatibility for general extensions

Lemma 7.5.4 *With notation as in Definition 7.5.1, suppose that* $L \cap K^{\mathrm{smcy}} = K$*. Then* $r_{L/K} = r'_{L/K}$*.*

Proof. In the setting of abstract class field theory, L/K is viewed as a "totally ramified" extension. Consequently, we may set notation as in the proof of Lemma 5.3.2, then apply Proposition 5.2.7 to obtain a commutative diagram

$$\begin{array}{ccc} C_M/\operatorname{Norm}_{N/M} C_N & \xrightarrow{r'_{N/M}} & \operatorname{Gal}(N/M) \\ \downarrow{\scriptstyle \operatorname{Norm}_{M/K}} & & \downarrow \\ C_K/\operatorname{Norm}_{L/K} C_L & \xrightarrow{r'_{L/K}} & \operatorname{Gal}(L/K) \end{array}$$

Figure 7.5.5

in which the horizontal arrows are isomorphisms (Theorem 7.3.8) and the right vertical arrow is an isomorphism, as then is the left vertical arrow. We also have a corresponding diagram on the local side:

$$\begin{array}{ccc} I_M & \xrightarrow{r_{N/M}} & \operatorname{Gal}(N/M) \\ \downarrow{\scriptstyle \operatorname{Norm}_{M/K}} & & \downarrow \\ I_K & \xrightarrow{r_{L/K}} & \operatorname{Gal}(L/K) \end{array}$$

Figure 7.5.6

This means that we can reduce checking the compatibility for L/K to the corresponding statement for the "unramified" extension N/M, to which Lemma 7.5.2 applies. ■

At last, we obtain the desired compatibility of reciprocity maps, and with it the completion of the proofs from global class field theory. Hooray! (See Remark 7.6.18 for another approach.)

Proposition 7.5.7 *For any Galois extension L/K of number fields, $r_{L/K} = r'_{L/K}$; that is, the abstract reciprocity map coincides with the product of the local reciprocity maps.*

Proof. By the norm limitation theorem (Theorem 7.3.10), we may assume that L/K is abelian. By Proposition 5.2.7, we may check the comparison of maps after replacing L with a larger abelian extension of K.
We may split the exact sequence

$$1 \to \operatorname{Gal}(K^{\mathrm{ab}}/K^{\mathrm{smcy}}) \to \operatorname{Gal}(K^{\mathrm{ab}}/K) \to \operatorname{Gal}(K^{\mathrm{smcy}}/K) \cong \widehat{\mathbb{Z}} \to 1$$

by choosing an element of $\operatorname{Gal}(K^{\mathrm{ab}}/K)$ lifting the generator $1 \in \widehat{\mathbb{Z}}$. Using this, we can split K^{ab} as the compositum of K^{smcy} and an abelian extension which is linearly disjoint from K^{smcy}. Using the previous paragraph, we can split some finite extension of L as the compositum of linearly disjoint cyclic extensions, one contained in K^{smcy} and the others linearly disjoint from K^{smcy}. Applying Lemma 7.5.2 to the first extension and Lemma 7.5.4 to the others, we deduce the desired compatibility for abelian extensions. ■

Remark 7.5.8 It's worth repeating that only now do we know that the product $r_{L/K}$ of the local reciprocity maps kills principal idèles (Proposition 6.4.5). That fact, which relates local behavior for different primes in a highly global fashion, is the basis of various **higher reciprocity laws**. See [36], Chapter

VIII for details.

Globalization of local abelian extensions

As a complement to Proposition 7.5.7, we show that every local abelian extension is the completion of a global abelian extension. Over $\mathbb{Q}$, this holds because the local Kronecker-Weber theorem (Theorem 1.3.4) and the Kronecker-Weber theorem (Theorem 1.1.2) are expressed in terms of the same family of extensions of $\mathbb{Q}$, namely the cyclotomic extensions; however, in the general case we must take a less explicit approach.

Theorem 7.5.9 *Let K be a number field, let v a place of K, and let M a finite abelian extension of K_v. Then there exists a finite abelian extension L of K such that for any place w of L above v, L_w contains M. (This conclusion can be formally improved; see Exercise 1.)*

Proof. We can quickly dispatch the cases where v is infinite: if v is complex there is nothing to prove, and if v is real then we may take $L = K(\sqrt{-1})$. So assume hereafter that v is finite.
By the existence theorem (Theorem 7.4.8) plus local-to-global compatibility (Proposition 7.5.7), it suffices to produce an open subgroup V of C_K of finite index such that the preimage of V under $K_v^* \to C_K$ is contained in $N = \mathrm{Norm}_{M/K_v} M^*$. Let S be the set of infinite places and let $T = S \cup \{v\}$. By Corollary 6.2.11, $\mathfrak{o}_{K,T}^*$ is a finitely generated abelian group and $G = \mathfrak{o}_{K,T}^* \cap N$ is a subgroup of $\mathfrak{o}_{K,T}^*$ of finite index.
Pick a finite place $u \notin T$. The image of $\mathfrak{o}_{K,T}^*$ in K_u^* is a finitely generated subgroup of $\mathfrak{o}_{K_u}^*$. Hence we can choose a sufficiently small neighborhood U of the identity in $\mathfrak{o}_{K_u}^*$ so as to ensure that $U \cap \mathfrak{o}_{K,T}^* \subseteq G$.
Now put

$$W = N \times U \times \prod_{w \in S} K_w^* \times \prod_{w \notin S \cup \{u,v\}} \mathfrak{o}_K^*, \qquad V = K^* W / K^*.$$

If $\alpha_v \in K_v^*$ maps into U, then there exists $\beta \in K^*$ such that $\alpha_v \beta \in W$. On one hand, this implies that $\alpha_v \beta_v \in N$. On the other hand, it implies that $\beta \in \mathfrak{o}_{K,T}^*$ and $\beta_u \in U$, so $\beta \in G$ and so $\beta_v \in N$. Thus $\alpha_v \in N$, as desired. ∎

Exercises

1. Prove that Theorem 7.5.9 can be formally promoted to the conclusion that $L_w = M$.

Hint. Since L/K is abelian, the kernel of the map $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(M/K_v)$ is normal in $\mathrm{Gal}(L/K)$; take its fixed field.

7.6 Brauer groups and the reciprocity map

Reference. [36] IV (for the general theory of Brauer groups); VII.7 and VII.8 (for the application to reciprocity). For the general theory, see also [24], Chapter 4.

We discuss Brauer groups of fields, especially number fields. On one hand these can be used to give an alternate construction of the global reciprocity map, not based on abstract class field theory; on the other hand, they carry important information from class field theory which is useful in numerous applications.

In this lecture, we reprise a bit of shorthand from Section 4.2, writing $H^i(L/K)$ to mean $H^i(\mathrm{Gal}(L/K), L^*)$.

The Brauer group of a field

Definition 7.6.1 Recall from Definition 4.1.15 that we have defined the **Brauer group** of a field K as the group

$$\mathrm{Br}(K) = H^2(\overline{K}/K) = \varinjlim_{L/K} H^2(L/K)$$

where L runs over finite Galois extensions of K and the transition maps in the direct limit are inflation maps. By Lemma 1.2.3 and Proposition 4.2.14, these maps are all injective, so the direct limit is actually a union. ◊

This definition of Brauer groups is not the original one; we give that next.

Lemma 7.6.2 *For any field K, there is a natural bijection between $\mathrm{Br}(K)$ and the isomorphism classes of division algebras which are finite-dimensional K-algebras with center K.*

Proof. See [36], Corollary IV.3.16; [46], Chapter X, Proposition 9; or [24], Theorem 8.11. ■

Example 7.6.3 For K an algebraically closed field, every division algebra which is finite dimensional over K is trivial. Namely, if D is such an algebra, then for each $x \in D$, multiplication by x defines a K-linear endomorphism of D, which necessarily has at least one eigenvalue $y \in K$. Then $x - y$ is an element of D which cannot be invertible (since multiplication by this element is a K-linear endomorphism of D with 0 as an eigenvalue), so it must be zero; hence $x \in K$. □

Example 7.6.4 For K a finite field, $\mathrm{Br}(K)$ is trivial. In the classical interpretation, this is Wedderburn's theorem that every finite division algebra is commutative. In the cohomological interpretation, it follows from Proposition 4.2.4 via the periodicity of Tate groups Theorem 3.4.1. □

Remark 7.6.5 While Lemma 7.6.2 only characterizes the Brauer group as a set, the original construction of Brauer included the group structure. Namely, for any two central simple algebras D_1, D_2 over K, we have an isomorphism of K-algebras

$$D_1 \otimes_K D_2 \cong M_n(D)$$

for some positive integer n and some division algebra D with center K, and D is the product of D_1 and D_2 in $\mathrm{Br}(K)$ (in particular, it is characterized by this construction up to isomorphism).

In this construction, the identity element in $\mathrm{Br}(K)$ is K viewed as a division algebra with itself as the center. The inverse element of a division algebra D is the **opposite algebra** in which multiplication is reversed.

Remark 7.6.6 The property of a field K of characteristic 0 having trivial Brauer group is useful in the theory of finite group representations: for such a field, any K-valued character of a finite group arises from a representation defined over K. (This follows from **Schur's lemma**: the character in question appears within some irreducible K-linear representation, whose endomorphism ring is a division algebra; the triviality of the Brauer group forces this to split without any base extension.)

By contrast, for $G = \{\pm 1, \pm i, \pm j, \pm k\}$ the unit quaternion group, the standard 2-dimensional representation of G has a $\mathbb{Q}$-valued character but cannot be realized as a representation over $\mathbb{Q}$. In other words, this representation has nontrivial **Schur index**.

Remark 7.6.7 One can also associate Brauer groups to arbitrary rings and even to schemes in algebraic geometry, by replacing division algebras (or more precisely, central simple algebras) with **Azumaya algebras** and Galois cohomology with **étale cohomology**. See [15].

The Brauer group of a number field

We state the formula for the Brauer group of a number field, and prove it modulo one key step.

Lemma 7.6.8 *Let L/K be a cyclic extension of number fields of degree n. Then there is a commutative diagram as in Figure 7.6.9 in which the vertical arrows are isomorphisms.*

$$\begin{array}{ccccc} K^*/\operatorname{Norm}_{L/K} L^* & \longrightarrow & I_K/\operatorname{Norm}_{L/K} I_L & \xrightarrow{r_{L/K}} & \operatorname{Gal}(L/K) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(L/K) & \longrightarrow & \bigoplus_v H^2(L_w/K_v) & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \end{array}$$

Figure 7.6.9

Proof. The left square comes from applying Theorem 3.4.1 to the morphism $L^* \to I_L$ of $\mathrm{Gal}(L/K)$-modules. Since $r_{L/K}$ is defined in terms of local reciprocity maps, the right square comes from Lemma 4.2.21. ■

Theorem 7.6.10 *For any number field K, the group $\mathrm{Br}(K)$ fits into an exact sequence of the form*

$$0 \to \mathrm{Br}(K) \to \mathrm{Br}(\mathbb{A}_K) = \bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$$

in which

$$\mathrm{Br}(K_v) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{for } v \text{ finite} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{for } v \text{ real} \\ 0 & \text{for } v \text{ complex} \end{cases}$$

and the map on the right is summation.

Proof. The map $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$ is the injection from Theorem 7.2.14. The value of $\mathrm{Br}(K_v)$ for v finite is given by Lemma 4.2.21. For v complex, it is evident that $\mathrm{Br}(K_v) = 0$. For v real, by Theorem 3.4.1 we have

$$\begin{aligned} \mathrm{Br}(\mathbb{R}) &= H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) \\ &\cong H_T^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) \\ &\cong \mathbb{R}^*/\operatorname{Norm}_{\mathbb{C}/\mathbb{R}} \mathbb{C}^* = \mathbb{R}^*/\mathbb{R}^+ \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}. \end{aligned}$$

Since the values of $\mathrm{Br}(K_v)$ are the ones given, the surjectivity of the map $\bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ is evident.
It remains to establish exactness at the middle of the sequence. For any finite Galois extension L/K, we have the exact sequence

$$H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/K), I_L) \to H^2(\mathrm{Gal}(L/K), C_L).$$

If L/K is cyclic, then by reciprocity (Theorem 7.3.8), the top row of the commutative diagram in Lemma 7.6.8 is exact, as then is the bottom row.

Consequently, we could conclude the proof if we knew that every class in $\mathrm{Br}(K)$ is the image of a class in $H^2(\mathrm{Gal}(L/K), L^*)$ for some finite *cyclic* extension L of K. In fact, something even stronger is true; see Proposition 7.6.13. ■

Definition 7.6.11 For K a number field and $\alpha \in \mathrm{Br}(K)$, the image of α in $\mathrm{Br}(K_v)$ is often called the **local invariant** of α at v. The exact sequence appearing in Theorem 7.6.10 is sometimes called the **fundamental exact sequence** associated to K; it can be viewed as another source of "reciprocity" in class field theory. For example, applying the fundamental exact sequence to a quaternion algebra over $\mathbb{Q}$ (see Exercise 5) gives rise to Hilbert's reformulation of the law of quadratic reciprocity using **Hilbert symbols**.

The fundamental exact sequence also plays a key role in various applications of Brauer groups in number theory. One of these is the detection of obstructions to the existence of rational points on algebraic varieties over number fields, called **Brauer-Manin obstructions**. This construction is based on the following observation: for X an algebraic variety over a number field K, each class in $\mathrm{Br}(X)$ gives rise to a commutative diagram

$$\begin{array}{ccccccccc} & & X(K) & \longrightarrow & X(\mathbb{A}_K) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \mathrm{Br}(\mathbb{A}_K) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

Figure 7.6.12

in which the vertical maps are evaluation maps and the bottom row is the fundamental exact sequence. ◊

All Brauer classes are (cyclic) cyclotomic

Recall that in the cohomological approach to local class field theory, the crucial computation was that of the Brauer groups of local fields, which involved first studying unramified extensions and then transferring the knowledge to general extensions (see the proof of Proposition 4.2.18). The missing step in Theorem 7.6.10 is of a very similar nature, except that we have to vary the extension based on the class.

Proposition 7.6.13 *Let L/K be a Galois extension of number fields. Then for any element x of $H^2(L/K)$, there exist a cyclic cyclotomic extension M of K and an element y of $H^2(M/K)$ such that x and y map to the same element of $H^2(ML/K)$.*

Proof. By Theorem 7.2.14, any class in $H^2(L/K)$ is determined by its images in $H^2(L_w/K_v)$ for all places v in K (where w denotes any place of L above v), with only finitely many of these being nonzero. Moreover, a class in $H^2(L_w/K_v)$ of some order m is killed by replacing K_v by any extension of degree m (by Remark 4.2.22 and Proposition 4.2.23; see also [36], Theorem III.2.1). It thus suffices to find a cyclic cyclotomic extension for which, for some fixed finite set of finite places S of K, the degrees $[L_w : K_v]$ for all $v \in S$ are conveniently large; for this, see Exercise 1. (Compare also [36], Proposition VII.7.2.) ■

Remark 7.6.14 By Proposition 7.6.13, the field $\mathbb{Q}^{\mathrm{ab}}$ has trivial Brauer group. Since in addition every complex character of a finite group has values in $\mathbb{Q}^{\mathrm{ab}}$, it follows that every irreducible complex representation of a finite group can be

realized over $\mathbb{Q}^{\mathrm{ab}}$; for a more direct proof of this, see [45], Chapter 12, Theorem 24.

Local-global compatibility via Brauer groups

To conclude, we turn things around and show that Proposition 7.6.13 can be used to recover local-global compatibility for the reciprocity map (Proposition 6.4.5). This makes no use of abstract class field theory, although it does use the same inputs (notably the First and Second Inequality).

Proposition 7.6.15 *Let K be a number field and put $L = K(\zeta_n)$. Then $r_{L/K} : I_K \to \mathrm{Gal}(L/K)$ maps all principal idèles to the identity.*

Proof. For $K = \mathbb{Q}$, this follows from the explicit description of the Artin map given in Definition 1.1.7 (or from Lemma 7.5.3). In general, we have a commutative diagram

$$\begin{array}{ccc} I_L & \longrightarrow & \mathrm{Gal}(L_w(\zeta_n)/L_w) \\ \downarrow{\scriptstyle \mathrm{Norm}_{L_w/\mathbb{Q}_p}} & & \downarrow \\ I_{\mathbb{Q}} & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \end{array}$$

Figure 7.6.16

and we know the bottom row kills principal idèles and the right column is injective. Thus the top row kills principal idèles too. ■

Proposition 7.6.17 *For any cyclic extension L/K of number fields, the map $r_{L/K} : I_K \to \mathrm{Gal}(L/K)$ kills principal idèles.*

Proof. To begin with, Proposition 7.6.15 implies that $r_{L/K}$ kills principal idèles whenever L/K is a cyclotomic extension, and Lemma 7.6.8 implies that in this case the composite $H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$ along the bottom row of Figure 7.6.9 vanishes. By Proposition 7.6.13, the same then holds for any cyclic extension L/K. By Lemma 7.6.8 again, the composition along the top row of Figure 7.6.9 vanishes, proving the claim. ■

Remark 7.6.18 Let L/K be a cyclic extension of number fields. At this point, $r_{L/K}$ kills both principal idèles (by Proposition 6.4.5) and norms (since it does so locally), so it induces a map $C_K/\operatorname{Norm}_{L/K} C_L \to \mathrm{Gal}(L/K)$. By the surjectivity of the Artin map, as deduced from the First Inequality (Proposition 7.3.7), this map is surjective; by comparing orders using the Second Inequality (Theorem 7.2.10), we see that the map is also an isomorphism. This establishes local-global compatibility (Proposition 6.4.5) for cyclic extensions, from which it directly follows also for abelian extensions. Hooray again!

Remark 7.6.19 Note that for a cyclic extension L/K of number fields, Remark 7.6.18 establishes not just local-global compatbility, but the entire reciprocity isomorphism

$$C_K/\operatorname{Norm}_{L/K} C_L \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

without use of abstract class field theory. One can say the same for an abelian extension: in this case, local reciprocity (Theorem 4.1.2) and Remark 7.6.18 together imply that we have a well-defined map. Using the cyclic case, we may see that this map is surjective; by Corollary 7.2.8 (a side effect of our proof of the Second Inequality), the map is forced to be an isomorphism.

It is less clear how to recover the norm limitation theorem, which is needed to prove the existence theorem. The difficulty is that if L/K is not abelian and M/K is its maximal abelian subextension, then the maximal abelian subextension of a completion of L can be strictly larger than the corresponding completion of M; so we cannot simply apply the local norm limitation theorem. Instead, one first uses the fundamental exact sequence (Theorem 7.6.10, whose proof depended on reciprocity only for cyclic extensions) to argue that C_L satisfies the hypotheses of Tate's theorem (Theorem 4.3.1), which yields an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \cong H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^0(\mathrm{Gal}(L/K), C_L) = C_K / \mathrm{Norm}_{L/K}\, C_L.$$

By comparing with the construction of the local reciprocity map, we see that the inverse of this isomorphism is exactly $r_{L/K}$, which yields the norm limitation theorem. See [36], Theorem VIII.4.8 for more details.

Exercises

1. Let K be a number field, let S be a finite set of finite places of K, and let m be a positive integer. Prove that there exists a subextension L of K^{smcy}/K (which is necessarily cyclic) such that for all $v \in S$, for some place w of L above K, $[L_w : K_v]$ is divisible by m.

Hint. See [36], Lemma VII.7.3.

2. Let D be a quaternion algebra over a field K (see Exercise 5). Prove the following statements directly (without using Lemma 7.6.2).

(a) D is isomorphic to its opposite algebra.

(b) There is an isomorphism $D \otimes_K D \cong M_4(K)$ of K-algebras. Consequently, if D is not split, then it represents an element of $\mathrm{Br}(K)$ of order 2.

Appendix A

Parting thoughts

Class field theory encompasses a vast expanse of mathematics, so it's worth concluding by taking stock of what we've seen and what we haven't. First, a reminder of the main topics we have covered.

- The Kronecker-Weber theorem: the maximal abelian extension of $\mathbb{Q}$ is generated by roots of unity (Theorem 1.1.2).
- The Artin reciprocity law for an abelian extension of a number field (Theorem 2.2.6).
- The existence theorem classifying abelian extensions of number fields in terms of generalized ideal class groups (Theorem 2.2.8).
- The Chebotaryov density theorem, describing the distribution over primes of a number field of various splitting behaviors in an extension field (Theorem 2.4.11).
- Some group cohomology "nuts and bolts", including the periodicity of Tate cohomology for a cyclic group (Theorem 3.4.1) and Tate's theorem (Theorem 4.3.1).
- The local reciprocity law (Theorem 4.1.2), the local existence theorem (Theorem 4.1.5), and the norm limitation theorem (Theorem 4.1.7).
- The Artin-Tate framework of abstract class field theory, including the abstract reciprocity law (Theorem 5.3.9) and the abstract norm limitation theorem (Corollary 5.3.11).
- Adèles, idèles, and the idelic formulations of the reciprocity law (Theorem 6.4.1) and the existence theorem (Theorem 6.4.2).
- Computations of group cohomology in the local case (multiplicative group; Proposition 4.2.1) and the global case (idèle class group; Theorem 7.1.2, Theorem 7.2.10).

We also gave brief summaries of Brauer groups of number fields (Section 7.6) and of adelic Fourier analysis (Section 6.6).

Now, some things that we haven't covered. When this course was first taught, these topics were assigned as final projects to individual students in the course.

- The Lubin-Tate construction of explicit class field theory for local fields (see [4], IV).

- More details about zeta functions and L-functions, including the class number formula and the distribution of norms in ideal classes.
- Another application of group cohomology: to computing ranks of elliptic curves via **Selmer groups** (see [51], X).
- Orders in number fields, and the notion of a **ring class field**.
- An analogue of the Kronecker-Weber theorem over the function field $\mathbb{F}_q(t)$, and even over its extensions (see [19]).
- Explicit class field theory for imaginary quadratic fields, via elliptic curves with complex multiplication (see [4], XIII; [10]).
- Quadratic forms over number fields and the Hasse-Minkowski theorem (see [44]).
- Artin (nonabelian) L-series, the basis of "nonabelian class field theory."

Some additional topics for further reading would include the following.

- Duality in Galois cohomology, including Tate local duality and Poitou-Tate global duality (see [17]).
- The Golod-Shafarevich inequality and the class field tower problem (see [4], IX).
- Class field theory for function fields (see [47]) and its use to produce curves over finite fields with unusually many points (see manypoints.org[1] and the forthcoming [50]).
- Application of Artin reciprocity to cubic, quartic, and higher reciprocity (see [36]).
- Algorithmic class field theory (see [8], [9]).
- Clausen's K-theoretic approach to Artin reciprocity (see [7]).
- Higher-dimensional class field theory (see [28]).
- Brauer-Manin obstructions to the existence of rational points on algebraic varieties (see [41], Chapter 8).

And finally, some ruminations about where number theory has gone since the mid-20th century, expanding upon Remark 6.2.13. In its cleanest form, class field theory describes a correspondence between one-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$, for K a number field, and certain representations of $\mathrm{GL}_1(\mathbb{A}_K)$, otherwise known as the group of idèles. But what about the nonabelian extensions of K, or equivalently the higher-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$?

Building on work of many authors, Langlands has proposed that for every n, there should be a correspondence between n-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$ and representations of $\mathrm{GL}_n(\mathbb{A}_K)$. This correspondence is the heart of the so-called **Langlands Program**, an unbelievably deep web of statements which has driven much of the mathematical establishment for the last few decades. For example, for $n = 2$, this correspondence includes on one hand the 2-dimensional Galois representations coming from elliptic curves, and on the other hand representations of $\mathrm{GL}_2(\mathbb{A}_K)$ corresponding to modular forms

[1] `manypoints.org`

(see [12] for the reinterpretation of the classical theory of modular forms in this language). In particular, it includes the **modularity of elliptic curves**, proved by Breuil, Conrad, Diamond, and Taylor [2] following on the celebrated work of Wiles [57] and Taylor-Wiles [52] on Fermat's Last Theorem.

Various analogues of the Langlands correspondence have been worked out: for local fields by Harris and Taylor [18], with subsequent simplifications by Henniart [20] and Scholze [43]; and for function fields by L. Lafforgue [29], building on the case $n = 2$ which was treated by Drinfeld. Moreover, one can pin things down better by replacing GL_n with a more general algebraic group; in the function fields, this case is addressed by V. Lafforgue [30]. The work of Waldspurger [54] of Laumon and Ngô [34] on the Langlands fundamental lemma is also part of this story.

Recently, some intriguing links have emerged between the Langlands program and some duality theories appearing in mathematical physics, leading to fruitful transfers of ideas in both directions. See [27] for the starting point.

This discussion could continue *ad infinitum*, so I had to make an arbitrary decision to stop somewhere, and this is that point. Thanks for reading!

Bibliography

[**1**] E. Artin and J. Tate, *Class Field Theory*, AMS Chelsea Publishing, Providence, RI, (2009).

[**2**] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", Journal of the American Mathematical Society **14** (2001), 843--939.

[**3**] B. Cais, B. Bhatt, A. Caraiani, K.S. Kedlaya, P. Scholze, and J. Weinstein, *Perfectoid Spaces: Lectures from the 2017 Arizona Winter School*, American Mathematical Society, (2019).

[**4**] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, (1967).

[**5**] J.-L. Chabert, "From Pólya fields to Pólya groups, I: Galois extensions", Journal of Number Theory **203** (2019), 360–375.

[**6**] C. Chevalley, "La théorie du corps de classes", Annals of Mathematics **41** (1940), 394–418.

[**7**] D. Clausen, "A K-theoretic approach to Artin maps", arXiv:1703.07842v2, (2017).

[**8**] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin, (1993).

[**9**] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics 193, Springer-Verlag, New York, (2000).

[**10**] D.A. Cox, *Primes of the Form* $x^2 + ny^2$, second edition, John Wiley & Sons, Hoboken, NJ, (2013).

[**11**] A. Fröhlich and M.J. Taylor, *Algebraic Number Theory*, Cambridge University Press, (1991).

[**12**] S. Gelbart, *Automorphic Forms on Adèle Groups*, Annals of Mathematics Studies 83, Princeton University Press, Princeton, NJ, (1975).

[**13**] G. Gras, *Class Field Theory: From Theory to Practice*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, (2003).

[**14**] A. Grothendieck, "Sur quelques points d'algèbre homologique", Tôhoku Mathematical Journal **9** (1957), 119–221.

[**15**] A. Grothendieck, "Le groupe de Brauer I, II, III", in *Dix Exposés sur la Cohomologie des Schémas*, North-Holland, Amsterdam, (1968).

[**16**] W. Grunwald, "Ein allgemeiner Existenzsatz für algebraische Zahlkörper", Journal für die reine und angewandte Mathematik **169** (1933), 103–107.

[**17**] D. Harari, *Galois Cohomology and Class Field Theory*, Universitext,

Springer, Cham, (2020).

[18] M. Harris and R. Taylor, *The Geometry and Cohomology of Some Simple Shimura Varieties*, with an appendix by Vladimir G. Berkovich, Annals of Mathematics Studies 151, Princeton University Press, Princeton, NJ, (2001).

[19] D. Hayes, "A brief introduction to Drinfeld modules", in *The Arithmetic of Function Fields (Columbus, OH, 1991)*, de Gruyter, Berlin, (1992), 1–32.

[20] G. Henniart, "Une preuve simple des conjectures de Langlands pour GL(n) sur un corps p-adique", Inventiones Mathematicae **139** (2000), 439–455.

[21] D. Hilbert, *The Theory of Algebraic Number Fields*, Springer-Verlag, Berlin, (1998).

[22] D.F. Holt, "An interpretation of the cohomology groups $H_n(G, M)$", J. Algebra **60** (1979), no. 2, 307–320.

[23] I.M. Isaacs, *Character Theory of Finite Groups*, American Mathematical Society, Providence, RI, (2006).

[24] N. Jacobson, *Basic Algebra, II*, W. H. Freeman, San Francisco, (1980).

[25] G. Janusz, *Algebraic Number Fields*, American Mathematical Society, (1996).

[26] F. Jarvis, *Algebraic Number Fields*, Springer, Cham, (2014).

[27] A. Kapustin and E. Witten, "Electric-magnetic duality and the geometric Langlands program", Communications in Number Theory and Physics **1** (2007), 1–236.

[28] K. Kato, "A generalization of local class field theory by using K-groups, I", Proceedings of the Japan Academy, Series A, Mathematical Sciences **53** (1977), 140–143.

[29] L. Lafforgue, "Chtoucas de Drinfeld et correspondance de Langlands", Inventiones Mathematicae **147** (2002), 1–241.

[30] V. Lafforgue, "Chtoucas pour les groupes réductifs et paramétrisation de Langlands globale", Journal of the American Mathematical Society **31** (2018), 719–891.

[31] J.C. Lagarias and A.M. Odlyzko, "Effective versions of the Chebotarev density theorem", in *Algebraic Number Fields: L-Functions and Galois Representations*, Academic Press, London, (1977), 409–464.

[32] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics 211, Springer-Verlag, New York, (2002).

[33] S. Lang, *Algebraic Number Theory*, second edition, Graduate Texts in Mathematics 110, Springer-Verlag, New York, (1994).

[34] G. Laumon and B.C. Ngô, "Le lemme fondamental pour les groupes unitaires", Annals of Mathematics **168** (2008) 477–573.

[35] A. Leriche, "About the embedding of a number field in a Pólya field", Journal of Number Theory **145** (2014), 210–229.

[36] J. Milne, *Class Field Theory*, version 4.04, http://jmilne.org/math/CourseNotes/cft.html.

[37] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, (1999).

[38] J. Neukirch, *Class Field Theory, the Bonn Lectures*, Springer, Heidelberg,

(2013).

[39] N. Nikolov and D. Segal, "On finitely generated profinite groups, I: strong completeness and uniform bounds", Annals of Mathematics **165** (2007), 171--238.

[40] E. Noether, "Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper", Mathematische Annalen 108 (1933), 411–419.

[41] B. Poonen, *Rational Points on Varieties*, Graduate Studies in Mathematics 186, American Mathematical Society, Providence, RI, (2017).

[42] D. Ramakrishnan and R.J. Valenza, *Fourier Analysis on Number Fields*, Graduate Texts in Mathematics 186, Springer, New York, (1999).

[43] P. Scholze, "The local Langlands correspondence for GL_n over p-adic fields", Inventiones Mathematicae 192 (2013), 663–715.

[44] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York-Heidelberg, (1973).

[45] J.-P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics 42, Springer-Verlag, New York, (1977).

[46] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, New York-Berlin, (1979).

[47] J.-P. Serre, *Algebraic Groups and Class Fields*, Graduate Texts in Mathematics 117, Springer-Verlag, New York, (1988).

[48] J.-P. Serre, *Galois Cohomology*, corrected reprint of the 1997 English edition, Springer-Verlag, Berlin, (2002).

[49] J.-P. Serre, *Lectures on* $N_X(p)$, CRC Press, Boca Raton, FL, (2012).

[50] J.-P. Serre, *Rational Points on Curves over Finite Fields*, with contributions by Everett Howe, Joseph Oesterlé, and Christophe Ritzenthaler, Documents Mathématiques, Société Mathématique de France, (2020).

[51] J. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics 106, Springer, Dordrecht, (2009).

[52] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras", Annals of Mathematics **141** (1995), 553–572.

[53] S. Wang, "A counter-example to Grunwald's theorem", Annals of Mathematics **49** (1948) 1008–1009.

[54] J.-L. Waldspurger, "Sur les intégrales orbitales tordues pour les groupes linéaires: un lemme fondamental", Canadian Journal of Mathematics **43** (1991), 852–896.

[55] S. Wang, "On Grunwald's theorem", Annals of Mathematics **51** (1950), 471–484.

[56] L. Washington, *Introduction to Cyclotomic Fields*, second edition, Graduate Texts in Mathematics 83, Springer-Verlag, New York, (1997).

[57] A. Wiles, "Modular elliptic curves and Fermat's Last Theorem", Annals of Mathematics **141** (1995), 443–551.

[58] H. Zantema, "Integer valued polynomials over a number field", Manuscripta Mathematica **40** (1982), 155–203.