Notes on class field theory (updated 17 Mar 2017)

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
E-mail address: kedlaya@ucsd.edu

Contents

Preface

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 Chebotarev 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 *Algebraic Number Theory*; 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, Janusz, Lang) 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; as a result, I decided to prepare a corrected version of the notes. In so doing, I made a conscious decision to suppress any temptation to modify the presentation with the benefit of hindsight, or to fill in additional material to make the text more self-contained. This decision, while largely dictated by lack of time and energy, was justified by the belief that the informality of the original notes contributed to their readibility. In other words, this 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 Neukirch, the main source of inspiration was Milne's lecture notes on algebraic number theory (see `http://jmilne.org/math/CourseNotes/cft.html`, version 3.10; note that a more recent version is available, but we have not verified that all references remain valid). These two sources are referenced simply as "Neukirch" and "Milne," with additional references described more explicitly as they occur. 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.

This document is not yet in a final state. Consequently, corrections and comments are welcome. Thanks to Zonglin Jiang, Justin Lacini, and Zongze Liu for their feedback on previous drafts.

Part 1

Trailer: Abelian extensions of the rationals

CHAPTER 1

The Kronecker-Weber theorem

Reference. Our approach follows Washington, *Introduction to Cyclotomic Fields*, Chapter 14. A variety of other methods can be found in other texts.

Abelian extensions of $\mathbb{Q}$.

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 provide 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.

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, there are no other examples!

THEOREM 1.1 (Kronecker-Weber). *If $K/\mathbb{Q}$ is a finite abelian extension, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some positive integer n.*

For example, every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic field, a fact known to Gauss.

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 this theorem in the next few lectures. Our approach will be to deduce it from a local analogue (see Theorem 3.1).

THEOREM 1.2 (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.*

Before proceeding, it is worth noting explicitly a nice property of abelian extensions that we will exploit below. 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. 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 exercises) unless $r - p \equiv 0 \pmod{m}$. Thus F_p must be equal to the image of p under the map $(\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(K/\mathbb{Q})$.

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.

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. (See for instance Neukirch III.2.)

THEOREM 1.3 (Minkowski). *There are no nontrivial extensions of $\mathbb{Q}$ which are unramified everywhere.*

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

PROOF OF THEOREM 1.1. For each prime p over which K ramifies, pick a prime $\mathfrak{p}$ of K over p; by local Kronecker-Weber (Theorem 1.2), $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{n_p})$ 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.)

We will prove that $K \subseteq \mathbb{Q}(\zeta_n)$, by proving that $K(\zeta_n) = \mathbb{Q}(\zeta_n)$. Write $L = K(\zeta_n)$ and let I_p be the inertia group of p in L. If we let U be the maximal

unramified subextension of $L_{\mathfrak{q}}$ over $\mathbb{Q}_p$ for some prime $\mathfrak{q}$ over p, then $L_{\mathfrak{q}} = U(\zeta_{p^{e_p}})$ and $I_p \cong \mathrm{Gal}(L_{\mathfrak{q}}/U) \cong (\mathbb{Z}/p^{e_p}\mathbb{Z})^*$. Let I be the group generated by all of the I_p; then

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

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) For $m \in \mathbb{Z}$ not a perfect square, determine the conductor of $\mathbb{Q}(\sqrt{m})$. (Hint: first consider the case where $|m|$ is prime.)
(2) Recover the law of quadratic reciprocity from the Artin reciprocity law, using the fact that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ has conductor p.
(3) 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 $(1 - xx)^m - 1$ modulo a prime divisor of n.)
(4) Prove that if m is not a prime power, $1 - \zeta_m$ is a unit in $\mathbb{Z}[\zeta_m]$.

CHAPTER 2

Kummer theory

Reference. Serre, *Local Fields*, Chapter X; Neukirch section IV.3; or just about any advanced algebra text (e.g., Lang's *Algebra*). The last lemma is from Washington, *Introduction to Cyclotomic Fields*, Chapter 14.

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

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!

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 in this chapter was first applied somewhat later by Hilbert in his *Zahlbericht*, a summary of algebraic number theory as of the end of the 19th century.

THEOREM 2.1. *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.*

Before describing the proof of Theorem 2.1, let me introduce some terminology which marks the tip of the iceberg of group cohomology, which we will see more of later.

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

The somewhat unusual common name for this result exists because in the special case where G is cyclic, this statement occurs as Theorem (Satz) 90 in Hilbert's *Zahlbericht*. The general case first appears in Emmy Noether's 1933 paper on the principal ideal theorem (Theorem 6.1), where Noether attributes it to Andreas Speiser.

PROOF. Let f be a function of the form described above. By the linear independence of automorphisms (see exercises), 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 $H^1(G, L^*)$. □

PROOF OF KUMMER'S THEOREM. On one hand, if $\alpha \in K^*$ is such that $\alpha^{1/d} \notin K$ for any proper divisor d of n, then the polynomial $x^n - \alpha$ is irreducible over K, and every automorphism must have the form $\alpha \mapsto \alpha\zeta_n^r$ for some $r \in \mathbb{Z}/n\mathbb{Z}$. Thus $\mathrm{Gal}(K(\alpha^{1/n})/K) \cong \mathbb{Z}/n\mathbb{Z}$.

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. □

Another way to state Kummer's theorem 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 easily.) Another way is in terms of the absolute Galois group of K. 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 2.3 (Kummer reformulated). *The Kummer pairing induces an isomorphism*

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

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 homomorphisms of $\mathrm{Gal}(\overline{K}/K)/H$ to $\mathbb{Z}/d\mathbb{Z}$, so one of them must equal f. Thus surjectivity follows. □

But what about $\mathbb{Z}/n\mathbb{Z}$-extensions of a field that does not contains ζ_n? These are harder to describe, and indeed describing such extensions of $\mathbb{Q}$ is the heart of this course. There is one thing one can say: 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.

LEMMA 2.4. *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*

$$a^g/a^{\omega(g)} \in (L^*)^n \qquad \forall g \in \mathrm{Gal}(L/K). \tag{1}$$

Note that $\omega(g)$ is only defined up to adding a multiple of n, so $a^{\omega(g)}$ is only defined up to an n-th power, i.e., modulo $(L^*)^n$. (In fact, we will only use one of the implications: if M/K is Galois and abelian, then (1) holds. However, we include both implications for completeness.)

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) 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

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

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. □

Exercises.

(1) Prove the linear independence of automorphisms: if $g_1, \ldots, g_n$ are distinct automorphisms of L over K, then there do not exist $x_1, \ldots, x_n \in L$ such that $x_1 y^{g_1} + \cdots + x_n y^{g_n} = 0$ for all $y \in L$. (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 Theorem 90: 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 Lang, *Algebra*), there exists $\alpha \in L$ whose conjugates form a basis of L as a K-vector space.)

(3) Prove the following extension of Theorem 90 (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.)

CHAPTER 3

The local Kronecker-Weber theorem

Reference. Washington, *Introduction to Cyclotomic Fields*, Chapter 14.

We now prove the local Kronecker-Weber theorem (Theorem 1.2), modulo some steps which will be left as exercises. As shown previously, this will imply the original Kronecker-Weber theorem.

THEOREM 3.1 (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.*

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 first recall the following facts from the theory of local fields (e.g., see Neukirch II.7).

LEMMA 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.*

LEMMA 3.3. *Let L/K be a totally and tamely ramified extension of finite extensions of $\mathbb{Q}_p$ of degree e. (Recall that tamely ramified means that p does not divide e.) Then there exists a generator π of the maximal ideal of the valuation ring of K such that $L = K(\pi^{1/e})$.*

We also recall one similarly easy but possible less familiar fact, whose proof we leave as an exercise.

LEMMA 3.4. *The fields $\mathbb{Q}_p((-p)^{1/(p-1)})$ and $\mathbb{Q}_p(\zeta_p)$ are equal.*

We now proceed to the proof of the local Kronecker-Weber theorem.

Case 1: $q \neq p$.

Let L be the maximal unramified subextension of K. By Lemma 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 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 $\pi = -pu$ 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 $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$.

For $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ 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 $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ 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 $K \subseteq L((-p)^{1/e}, u^{1/e})$ 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 $\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$ by Lemma 3.4. Putting it all together,

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

Case 2: $q = p \neq 2$**.**

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 $(\mathbb{Z}/p\mathbb{Z})^3$. It thus suffices to prove the following lemma.

LEMMA 3.5. *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 2.4,

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

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 exercises). 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

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

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. □

Case 3: $p = q = 2$. This case is similar to the previous case, 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.

Exercises.

(1) Prove Lemma 3.4. (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 3.5) 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 $(1 + x)^{1/p}$.)
(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 $n > 0$.
(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 $(\mathbb{Z}/4\mathbb{Z})^3$.
(5) Prove that there is no extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$. (Hint: use Kummer theory.)
(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 $\mathbb{Z}/4\mathbb{Z}$.)

Part 2

The statements of class field theory

CHAPTER 4

The Hilbert class field

Reference. Milne, Introduction; Neukirch, VI.6.

Recall that the field $\mathbb{Q}$ has no extensions which are everywhere unramified (Theorem 1.3). This is quite definitely not true of other number fields; we begin with an example illustrating this.

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.

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. Caution: until further notice, the phrase "L/K is unramified" will 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. (Get used to this. The real and complex embeddings of a number field will be treated like primes consistently throughout this text.)

THEOREM 4.1. *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.*

In fact, there is a canonical isomorphism, given by the Artin reciprocity law. We'll see this a bit later. The field L is called the *Hilbert class field* of K.

Warning: there can be infinite unramified *nonabelian* extensions. In fact, Golod and Shafarevich used unramified abelian extensions to construct these! Namely, starting from a number field $K = K_0$, let K_1 be the Hilbert class field of K_0, let K_2 be the Hilbert class field of K_1, and so on. Then K_i is an unramified but not necessarily abelian extension of K_0, and for a suitable choice of K_0, $[K_i : K_0]$ can be unbounded. (See Cassels-Frohlich for more discussion.)

Exercises.

(1) Let K be an imaginary quadratic extension of $\mathbb{Q}$ in which t finite primes ramify. Asuming Theorem 4.1, 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 4.1 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 the next chapter.
(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.)

CHAPTER 5

Generalized ideal class groups and the Artin reciprocity law

Reference. Milne V.1; Neukirch VI.6.

An example (continued from the previous chapter).

Before proceeding to generalized ideal class groups, we continue a bit with the example from the previous chapter to illustrate what is about to happen. Let $K = \mathbb{Q}(\sqrt{-5})$ and let $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$; recall that L/K is unramified everywhere.

THEOREM 5.1. *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). □

Bonus aside: for any ideal $\mathfrak{a}$ of $\mathfrak{o}_K$, $\mathfrak{a}\mathfrak{o}_L$ is principal. (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 "capitulation" theorem; we'll come back to this a bit later.

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.

Recall that the ideal class group of K is defined as the group of fractional ideals modulo the subgroup 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 $I_K^{\mathfrak{m}}$ be the group of fractional ideals of K which are coprime to each finite place of K occurring in $\mathfrak{m}$. Let $P_K^{\mathfrak{m}} \subseteq I_K^{\mathfrak{m}}$ 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 $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. A quotient of a ray class group is called a *generalized ideal class group*.

The Artin reciprocity law.

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

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

(Aside: 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.) Then the following miracle occurs.

THEOREM 5.2 (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 above homomorphism.*

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

Define the *conductor* of L/K to be the smallest formal product $\mathfrak{m}$ for which the conclusion of the Artin reciprocity law 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 $I_K/I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is an isomorphism.

THEOREM 5.3 (Existence of ray class fields). *Every formal product $\mathfrak{m}$ has a ray class field.*

For example, 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 $\mathbb{Q}(\zeta_m)$.

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.

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) with notation as in (a), $\mathrm{Frob}_{M/L}(\mathfrak{q}) = \mathrm{Frob}_{M/K}(\mathfrak{p})^{f(\mathfrak{q}/\mathfrak{p})}$, 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 Milne V.1. Make sure you understand its proof!) Then use that formula 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 $\mathbb{Q}(\sqrt{D})$.

(3) Show that the homomorphism $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective. You may assume the following fact: if L/K is an extension of number fields (with $L \neq K$), there exists a prime of K which does not split completely in L.

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

CHAPTER 6

The principal ideal theorem

Reference. Milne, section V.3 (but you won't find the proofs I've omitted there either); Neukirch, section VI.7 (see also IV.5); Lang, *Algebraic Number Theory*, section XI.5.

For a change, we're going to prove something, if only assuming the Artin reciprocity law which we haven't proved. Or rather, we're going to sketch a proof that you will 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 in the old days the word "capitulate" meant "to become principal". Etymology left to the reader.)

THEOREM 6.1 (Principal ideal theorem). *Let L be the Hilbert class field of the number field K. Then every ideal of K becomes principal in L.*

(Warning: this does not mean that L has class number 1!) Example: 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.

The idea is that given Artin reciprocity, this reduces to a question in group theory. Namely, 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 $I_L \to \mathrm{Gal}(M/L)$ is trivial. So what we need is to find a map V such that

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

commutes, then show that V is the zero map. (The horizontal arrows are the Artin maps.)

Regarding the relationship between K, L and M:

(a) M is Galois over K (because its image under any element of $\mathrm{Gal}(\overline{K}/K)$ is still an abelian extension of L unramified at all finite and infinite places, and so is contained in M) and unramified everywhere (since M/L and L/K are unramified);

(b) L is the maximal subextension of M/K which is abelian over K (since any abelian subextension is unramified over K, and so is contained in L).

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 (b) implies that $\mathrm{Gal}(M/L)$ is the commutator subgroup of $\mathrm{Gal}(M/K)$ and $\mathrm{Gal}(M/K)^{\mathrm{ab}} = \mathrm{Gal}(L/K)$.

Before returning to the principal ideal theorem, we need to do a bit of group theory. Let G be a finite group and H a subgroup (but not necessarily normal!). Let $g_1, \dots, g_n$ be left coset representatives of H in G: that is, $G = g_1 H \cup \dots \cup g_n H$. 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. In particular, it induces a map $V : G \to H^{\mathrm{ab}}$.

THEOREM 6.2. *The map $V : G \to H^{\mathrm{ab}}$ is a homomorphism, 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).*

The map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is called the *transfer map* (in German, "Verlagerung", hence the V).

Now let's return to that diagram:

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

and show that the transfer map V does actually make this diagram commute; it's enough to check this when we stick a prime $\mathfrak{p}$ of K in at the top left. For consistency of notation, put $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. 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 set of automorphisms mapping $\mathfrak{r}$ to itself) and let $g \in G_{\mathfrak{r}}$ be the Frobenius of $\mathfrak{r}$. (Note: 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 $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ 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 $G_{\mathfrak{r}} \tau_i H = \tau_i H \cup g \tau_i H \cup \dots \cup g^{m-1} \tau_i H$ 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 6.3. *If $L \cap \mathfrak{r}^{\tau_i} = \mathfrak{q}_i$, then $\mathrm{Frob}_{M/L}(\mathfrak{q}_i) = \prod_{j=0}^{m-1} \phi(g g_{ij})^{-1} g g_{ij}$.*

Thus the principal ideal theorem now follows from the following fact.

THEOREM 6.4. *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.*

Exercises.

(1) Prove Theorem 6.2. (Hint: one approach to proving independence from choices is to change one g_i at a time. Also, notice that $\phi(g g_1), \dots, \phi(g g_n)$ are a permutation of $g_1, \dots, g_n$.)
(2) Prove Lemma 6.3. (Hint: see Neukirch, Proposition IV.5.9.)

(3) With notation as in Theorem 6.2, let $\mathbb{Z}[G]$ be the group algebra of G (formal linear combinations $\sum_{g\in G} n_g[g]$ with $n_g \in \mathbb{Z}$, multiplied by putting $[g][h] = [gh]$) and let I_G be the ideal of sums $\sum n_g[g]$ with $\sum n_g = 0$ (called the *augmentation ideal*; see Chapter 10). 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

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

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

(4) With notation as in the previous exercise, prove that the following diagram commutes:

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

where S is given by $S(x) = x([g_1] + \cdots + [g_n])$.

(5) Prove Theorem 6.4. (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 Neukirch, Theorem VI.7.6.)

CHAPTER 7

Zeta functions and the Chebotarev density theorem

Reference. Lang, *Algebraic Number Theory*, Chapter VIII for starters; see also Milne, Chapter VI and Neukirch, Chapter VII. For advanced reading, see Tate's thesis (last chapter of Cassels-Frohlich), but wait until we introduce the adeles.

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.

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 in the sum $\mathfrak{a}$ runs over the nonzero ideals of $\mathfrak{o}_K$.

A fundamental fact about the zeta function is the following. We omit the proof.

THEOREM 7.1. *The function $\zeta_K(s)$ extends to a meromorphic function on $\mathbb{C}$ whose only pole is a simple pole at $s = 1$ of residue 1.*

The case $K = \mathbb{Q}$ is of course the famous Riemann zeta function. 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 $1/2$.

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

$$L(s, \chi_{\mathfrak{m}}) = \prod_{\mathfrak{p} \not| \mathfrak{m}} (1 - \chi(\mathfrak{p}) \mathrm{Norm}(\mathfrak{p})^{-s})^{-1} = \sum_{(\mathfrak{a}, \mathfrak{m}) = 1} \chi(\mathfrak{a}) \mathrm{Norm}(\mathfrak{a})^{-s}.$$

Then we have another basic fact whose proof we also omit.

THEOREM 7.2. *If $\chi_{\mathfrak{m}}$ is not trivial, then $L(s, \chi_{\mathfrak{m}})$ extends to an analytic function on $\mathbb{C}$.*

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 $s = 1$.

THEOREM 7.3. *If $\chi_{\mathfrak{m}}$ is not the trivial character, then $L(1, \chi_{\mathfrak{m}}) \neq 0$.*

This is already a nontrivial, but important result over $\mathbb{Q}$. It implies Dirichlet's famous theorem that there are infinitely many primes in arithmetic progression, by implying that for any nontrivial $\chi_{\mathfrak{m}}$, $\sum_{\mathfrak{p}} \chi(\mathfrak{p}) \mathrm{Norm}(\mathfrak{p})^{-s}$ remains bounded as

$s \to \infty$. In fact, we say that a set of primes S in a number field K has Dirichlet density d if

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

Then the fact implies that the Dirichlet density of the set of primes congruent to a modulo m (assuming a is coprime to m) is $1/\phi(m)$.

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 $1/\#\,\mathrm{Cl}^{\mathfrak{m}}(K)$. (Proof: see exercises.)

Finally, we point out a result of class field theory that also applies to nonabelian extensions. Recall that if L/K is any Galois extension of number fields with Galois group G, $\mathfrak{p}$ is a prime of K, and $\mathfrak{q}$ is a prime above $\mathfrak{p}$ which is unramified, then there is a well-defined Frobenius associated to $\mathfrak{q}$ (it's the element g of the decomposition group $G_{\mathfrak{q}}$ such that $x^g \equiv x^{\#(\mathfrak{o}_K/\mathfrak{p})} \pmod{\mathfrak{q}}$); but as a function of $\mathfrak{p}$, this Frobenius is only well-defined up to conjugation in G.

THEOREM 7.4 (Chebotarev Density Theorem). *Let L/K be an arbitrary 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 $g \in \mathrm{Gal}(L/K') \subset G$ has Dirichlet density $1/f$. The same is true if we restrict to primes of absolute degree 1 (see exercises).

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 $\#G/\#Z$. □

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 Theorems 7.1, 7.2, and 7.3, prove that the set of primes of K lying in any specified class of the ray class group of conductor $\mathfrak{m}$ is $1/\#\,\mathrm{Cl}^{\mathfrak{m}}(K)$. (Hint: combine the quantities $\sum_{\mathfrak{p}} \chi(\mathfrak{p}) \mathrm{Norm}(\mathfrak{p})^{-s}$ to cancel out all but one class.)

Part 3

Cohomology of groups

CHAPTER 8

Cohomology of finite groups I: abstract nonsense

Reference. Milne, II.1. See Serre, *Galois Cohomology* for a much more general presentation. (We will generalize ourselves from finite to profinite groups a bit later on.) Warning: 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!

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!

Let G be a finite group and A an abelian group (itself not necessarily finite) with a right G-action, also known as a G-module. I'll write the G-action as a superscript, 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., $\phi(m^g) = \phi(m)^g$. (For those keeping score, the category of G-modules is an abelian category.)

We would like to define some invariants of the pair (G, A) that we can use to get information about G and A. We will use the general methodology of homological algebra to do this. Before doing so, though, we need a few lemmas about G-modules.

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.

LEMMA 8.1. *Every G-module can be embedded into some injective G-module. (That is, the category of G-modules has enough injectives.)*

PROOF. Exercise. □

In particular, any G-module M admits an *injective resolution*: a complex

$$0 \to M \to I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} I_2 \xrightarrow{d_2} \dots$$

(that is, $d_{i+1} \circ d_i = 0$ for all i) in which each I_i is injective and the complex itself is *exact*: $\operatorname{im} d_i = \ker d_{i+1}$. (To wit, embed M into I_0, embed I_0/M into I_1, et cetera.)

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

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

The functor $M \to M^G$ from G-modules to abelian groups is left exact but not right exact: 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, but $M^G \to (M'')^G$ may not be exact. (Example: 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.)

This is the general situation addressed by homological algebra: it provides a canonical way to extend the truncated exact sequence $0 \to (M')^G \to M^G \to (M'')^G$. (Or if you prefer, it helps measure the failure of exactness of the G-invariants functor.) To do this, given M and an injective resolution as above, take G-invariants: the result

$$0 \to I_0^G \stackrel{d_0}{\to} I_1^G \stackrel{d_1}{\to} I_2^G \stackrel{d_2}{\to} \dots$$

is still a complex, but no longer exact. We turn this failure into success by defining the i-th cohomology group as the quotient

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

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 a injective resolution $0 \to N \to J_0 \to J_1 \to \cdots$, there exists a commutative diagram

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & M & \longrightarrow & I_0 & \xrightarrow{d_0} & I_1 & \xrightarrow{d_1} & I_2 & \xrightarrow{d_2} & \cdots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \\
0 & \longrightarrow & N & \longrightarrow & J_0 & \xrightarrow{d_0} & J_1 & \xrightarrow{d_1} & J_2 & \xrightarrow{d_2} & \cdots
\end{array}$$

and likewise after taking G-invariants, so we get maps $H^i(f) : H^i(G, M) \to H^i(G, N)$.

LEMMA 8.2. *The map $H^i(f)$ does not depend on the choice of the f_i (given the choices of injective resolutions).*

PROOF. This proof is a bit 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 $f_i = g_i \circ d_i + d_{i-1} \circ g_{i-1}$. (Such a set of maps is called a *homotopy*.) Details left as an exercise. (Warning: the diagonal arrows in the diagram below don't commute!)

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & M & \longrightarrow & I_0 & \xrightarrow{d_0} & I_1 & \xrightarrow{d_1} & I_2 & \xrightarrow{d_2} & \cdots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_0} & \swarrow{\scriptstyle g_0} & \downarrow{\scriptstyle f_1} & \swarrow{\scriptstyle g_1} & \downarrow{\scriptstyle f_2} & & \\
0 & \longrightarrow & N & \longrightarrow & J_0 & \xrightarrow{d_0} & J_1 & \xrightarrow{d_1} & J_2 & \xrightarrow{d_2} & \cdots
\end{array}$$

□

In particular, 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.

If you know any homological algebra, you'll recognize what comes next: given a short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules, there is a canonical

long exact sequence

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

where the δ_i are certain "connecting homomorphisms" (or "snake maps"). I won't punish you with the proof of this; if you've never seen it before, deduce it yourself from the Snake Lemma. (For the proof of the latter, engage in "diagram chasing", or see the movie *It's My Turn*. To define δ: 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. Then verify that the result is well-defined, et cetera.)

LEMMA 8.3 (Snake Lemma). *Given a commuting diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \\ 0 & \longrightarrow & N_0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & 0 \end{array}$$

in which the rows are exact, 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.

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 exercises.

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 8.1. (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 8.2, 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.)

(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 $0 \to M_0^G \to M_1^G \to \cdots$ 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!)

CHAPTER 9

Cohomology of finite groups II: concrete nonsense

Reference. Milne, 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.

Recall the last point (and the last exercise) from the last chapter: if

$$0 \to M \to M_0 \to M_1 \to \cdots$$

is an acyclic resolution of M (i.e., the sequence is exact, and $H^i(G, M_j) = 0$ for $i > 0$ and all j), then

$$H^i(G, M) = \ker(M_i^G \to M_{i+1}^G) / \operatorname{im}(M_{i-1}^G \to M_i^G).$$

Thus 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*. 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).

If H is a subgroup of G and M is an H-module, we define the *induced* G-module associated to M to be $\operatorname{Ind}_H^G M = M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. We may also identify $\operatorname{Ind}_H^G M$ with the set of functions $\phi : G \to M$ 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 9.1 (Shapiro's lemma). *If H is a subgroup of G and N is an H-module, then there is a canonical isomorphism $H^i(G, \operatorname{Ind}_H^G N) \to H^i(H, N)$. In particular, N is an acyclic H-module if and only if $\operatorname{Ind}_H^G(N)$ is an acyclic G-module.*

PROOF. The key points are:

(a) $(\operatorname{Ind}_H^G N)^G = N^H$, so there is an isomorphism for $i = 0$ (this is clearest from the description using functions);
(b) the functor Ind_H^G from H-modules to G-modules is exact (that is, $\mathbb{Z}[G]$ is flat over $\mathbb{Z}[H]$, which is easy to see because it in fact is free over $\mathbb{Z}[H]$);
(c) if I is an injective H-module, then $\operatorname{Ind}_H^G(I)$ is an injective G-module. This follows from the existence of a canonical isomorphism $\operatorname{Hom}_G(M, \operatorname{Ind}_H^G I) = \operatorname{Hom}_H(M, I)$, for which see Proposition 9.3 below.

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

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

To complete the previous argument, we need an important property of induced modules.

PROPOSITION 9.3. *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*

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

In other words, 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.

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 $M \to \mathrm{Ind}_H^G M$ and to a homomorphism $\mathrm{Ind}_H^G M \to M$. 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. Note that this second map doesn't depend on the choice of the representatives; for $g \in G$, we can use the coset representatives gg_i instead, so the equality

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

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 Chapter 10.)

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 $\phi : G \to N$, 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. □

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 9.3! Immediate consequence: 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. (But contrary to what you might expect, for fixed M, the groups $H^i(G, M)$ do not necessarily become zero for i large, even if M is finite! We'll see explicit examples next time.)

Another consequence is the following result. (The case $i = 1$ was an exercise earlier.)

THEOREM 9.4. *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. □

Now let's see an explicit way to compute group cohomology. Given a group G and a G-module M, define the G-modules N_i for $i \geq 0$ as the set of functions $\phi : G^{i+1} \to M$, 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 $N_i = \mathrm{Ind}_1^G N_{i,0}$ where $N_{i,0}$ is the subset of N_i consisting of functions for which $\phi(g_0, \ldots, g_i) = 0$ when $g_0 \neq e$.

Define the map $d_i : N_i \to N_{i+1}$ 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. Then one checks that the sequence

$$0 \to M \to N_0 \to N_1 \to \ldots$$

is exact. Since the N_i are induced, this is an acyclic resolution: thus the cohomology of the complex

$$0 \to N_0^G \to N_1^G \to \cdots$$

coincides with the cohomology groups $H^i(G, M)$. And now we have something we can actually compute! (Terminology: the elements of N_i^G in the kernel of d_i are called *(homogeneous) i-cochains*; the ones in the image of d_{i-1} are called *i-coboundaries*.)

Fun with H^1.

For example, we can give a very simple description of $H^1(G, M)$. Namely, a 1-cochain $\phi : G^2 \to M$ 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 coboundary of a 0-cochain $\psi : G \to M$ 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 Chapter 2.

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:

(a) for any $a \in A$, the map $M \to A$ given by $m \mapsto m(a)$ is a bijection;
(b) for $a \in A$, $g \in G$ and $m \in M$, $m(a)^g = m^g(a)$ (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 $\rho : G \to M$ given by $\rho(g) = a^g - a$, 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. (For example, 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: $m(a) = m + a$.)

This interpretation of H^1 appears prominently in the theory of elliptic curves: For example, if L is a finite extension of K and E is an elliptic curve over E, then $H^1(\mathrm{Gal}(L/K), E(\overline{K}))$ is the set of K-isomorphism classes of curves whose Jacobians are K-isomorphic to E (but which might not themselves be isomorphic to E by virtue of not having a K-rational point). For another example, $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(E))$ 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 $L = \mathbb{Q}(\sqrt{2})$.) See Silverman, *The Arithmetic of Elliptic Curves*, 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.

We can also give an explicit interpretation of $H^2(G, M)$ (see Milne, 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.) Namely, given the sequence, choose a map $s : G \to E$ (not a homomorphism) such that $s(g)$ maps to g under the map $E \to G$. Then the map $\phi : G^3 \to M$ 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 following diagram commute:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

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 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

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.

Let M be a G-module and M' a G'-module. Suppose we are given a homomorphism $\alpha : G' \to G$ of groups and a homomorphism $\beta : M \to M'$ 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 $H^i(G, M) \to H^i(G', M')$ (construct them on pairs of injective resolutions, then show that any two choices are homotopic).

The principal examples are as follows.

(a) 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 $\alpha : G \to G$ be the conjugation by some fixed h: $g \mapsto h^{-1}gh$, and let $\beta : M \to M$ be the map $m \mapsto m^h$. Then the induced homomorphisms $H^i(G, M) \to H^i(G, M)$ are all the identity map.

(b) 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*

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

Another way to get the same map: use the adjunction homomorphism $M \to \mathrm{Ind}_H^G M$ from Proposition 9.3 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 to get

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

(c) Take notation as in (a), but this time 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, give what are called the *corestriction homomorphisms*:

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

(d) 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 and K fields.)

(e) If H is 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*

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

The inflation and restriction maps will interact in an interesting way; see Proposition 13.7.

Exercises.

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

(2) The set $H^2(G, M)$ has the structure of an abelian group. Describe the corresponding structure on short exact sequences $0 \to M \to E \to G \to 0$.

(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.

(4) (Artin-Schreier) 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 10

Homology of finite groups

Reference. Milne, II.2; for cyclic groups, also Neukirch, IV.7 and Lang, *Algebraic Number Theory*, IX.1.

Caveat. The Galois cohomology groups used in Neukirch are not the ones we defined earlier. They are the Tate cohomology groups we are going to define below.

Homology.

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 details.)

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.

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 is the reverse notion to injective; but it's 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, e.g., $\mathbb{Z}[G]$ itself!

Given a projective resolution $\cdots \to P_1 \to P_0 \to M \to 0$ of a G-module M (an exact sequence in which the P_i are projective), take coinvariants to get a no longer exact 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

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

Also, you can replace the projective resolution by an acyclic resolution (where here M being acyclic means $H_i(G, M) = 0$ for $i > 0$) and get the same homology

groups. For example, induced modules are again acyclic (and the analogue of Shapiro's lemma holds, in part because any free $\mathbb{Z}[H]$-module induces to a free $\mathbb{Z}[G]$-module).

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 an earlier exercise (see Chapter 6), it was shown that the map $g \mapsto [g] - 1$ defines an isomorphism $G^{\text{ab}} \to I_G/I_G^2$.

The Tate groups.

We now "fit together" the long exact sequences of cohomology and homology to get a doubly infinite exact sequence. Define the map $\text{Norm}_G : M \to M$ by

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

(It looks like it should be called "trace", but in practice our modules M will be groups which are most naturally written multiplicatively, i.e., the nonzero elements of a field.) Then Norm_G induces a homomorphism

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

Now define

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

then I claim that for any short exact sequence $0 \to M' \to M \to M'' \to 0$, we get an 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. The only issue is exactness between $H_T^{-2}(G, M'')$ and $H_T^1(G, M')$ inclusive; this follows by diagram-chasing (as in the snake lemma) on the commutative diagram

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

with exact rows (noting that the diagram remains commutative with the dashed arrows added).

This construction is especially useful if M is induced, in which case $H_T^i(G, M) = 0$ for all i. (The T stands for Tate, who among many other things was an early pioneer in the use of Galois cohomology into algebraic number theory.)

Finite cyclic groups.

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

THEOREM 10.1. *Let G be a finite cyclic group and M a G-module. Then there is a canonical (up to the choice of a generator of G), functorial isomorphism $H_T^i(G, M) \to H_T^{i+2}(G, M)$ for all $i \in \mathbb{Z}$.*

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 $\operatorname{Ind}_1^G M$, 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

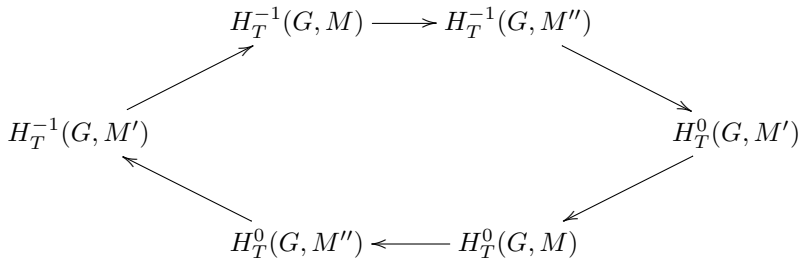
$$0 \to A \to B \to B/\operatorname{im}(f) \to 0$$
$$0 \to B/\ker(g) \to C \to D \to 0$$

to get

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

□

In particular, 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:



If the groups $H_T^i(G, M)$ are finite, we define the *Herbrand quotient*

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

Then from the exactness of the hexagon, if M', M, M'' all have Herbrand quotients, then

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

Moreover, if two of M', M, M'' have Herbrand quotients, 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.

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.

One special case is easy to work out: 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^{-1} and H^0.

Extended functoriality revisited.

The extended functoriality for cohomology groups has an analogue for homology and Tate groups, but under more restrictive conditions. 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. We would like to obtain canonical homomorphisms $H_i(G, M) \to H_i(G', M')$ and $H_T^i(G, M) \to H_T^i(G', M')$, 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. (Note that for Tate groups, we don't need any extra condition to get functoriality for $i \geq 0$.)

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) Show that $\mathrm{Res} : H_T^{-2}(G, \mathbb{Z}) \to H_T^{-2}(H, \mathbb{Z})$ corresponds to the transfer (Verlagerung) map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

CHAPTER 11

Profinite groups and infinite Galois theory

Reference. Neukirch, Sections IV.1 and IV.2.

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.

Recall the Galois correspondence for a finite extension: if L/K is Galois and $G = \mathrm{Gal}(L/K)$, then the (normal) subgroups H of G correspond to the (Galois) subextensions M of L, the correspondence in each direction being given by

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

To see what we have to be careful about, here's one example. 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.

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.

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 the exercises.

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!

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 11.1 (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*

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

For example, the Galois correspondence works 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. 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 $G/H_i \cong G_i$ and some other obvious compatibilities hold: let G be the set of families $\{g_i\}_{i\in I}$, where each g_i is in G_i and $f_{ij}(g_i) = g_j$.

For example, the group $\mathbb{Z}_p$ 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.)

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. Thus 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 11.2. *The group $H^i(G, M)$ is the direct limit of $H^i(G/H, M^H)$ using the inflation homomorphisms.*

That is, if $H_1 \subseteq H_2 \subseteq G$, you have the inflation homomorphism

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

so the groups $H^i(G/H, M^H)$ form a direct system, and $H^i(G, M)$ is the direct limit of these. (That is, you take the union of all of the $H^i(G/H, M^H)$, then you identify pairs that become the same somewhere down the line.)

Or if you prefer, you can compute these groups using continuous cochains: use continuous maps $G^{i+1} \to M$ that satisfy the same algebraic conditions as do the usual cochains. For example, $H^1(G, M)$ classifies continuous crossed homomorphisms modulo principal ones, et cetera.

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. (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) Neukirch exercise IV.2.4: a closed subgroup H of a profinite group G is called a *p-Sylow subgroup* of G if, for every open normal subgroup N of G, HN/N is a p-Sylow subgroup of G/N. Prove that:
   (a) For every prime p, there exists a p-Sylow subgroup of G.
   (b) Every subgroup of G, the quotient of which by any open normal subgroup is a p-group, is contained in a p-Sylow subgroup.
   (b) Every two p-Sylow subgroups of G are conjugate.

   You may use Sylow's theorem (that (a)-(c) hold for finite groups) without further comment. Warning: Sylow subgroups are usually not open.
(5) Neukirch exercise IV.2.4: Compute the p-Sylow subgroups of $\widehat{\mathbb{Z}}$, of $\mathbb{Z}_p^*$, and of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Part 4

Local class field theory

CHAPTER 12

Overview of local class field theory

Reference. Milne, I.1; Neukirch, V.1.

We will spend the next few chapters 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.)

The local reciprocity law.

The main theorem of local class field theory is the following. For K a local field, let K^{ab} be the maximal abelian extension of K.

THEOREM 12.1 (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:*

(a) *for any generator π of the maximal ideal of $\mathfrak{o}_K$ and any finite unramified extension L of K, $\phi_K(\pi)$ acts on L as the Frobenius automorphism;*
(b) *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.*

The map ϕ_K is variously called the *local reciprocity map* or the *norm residue symbol*. Using the local Kronecker-Weber theorem (Theorem 2), this can be explicitly verified for $K = \mathbb{Q}_p$ (see exercises).

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

THEOREM 12.2 (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 $U = \mathrm{Norm}_{L/K} L^*$.*

The condition "open" is only needed 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.

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. Which one?

THEOREM 12.3 (Norm limitation theorem). *Let M be the maximal abelian subextension of L/K. Then $\mathrm{Norm}_{L/K} L^* = \mathrm{Norm}_{M/K} M^*$.*

Aside: for each uniformizer (generator of the maximal ideal) 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 12.4. *For any finite Galois extension L/K of local fields with Galois group G, there is a canonical isomorphism $H_T^i(G, \mathbb{Z}) \to H_T^{i+2}(G, L^*)$.*

In fact, this map can be written in terms of the cup product in group cohomology, which we have not defined (and will not).

The local invariant map.

One way to deduce the local reciprocity law (the one we will carry out first) is to first prove the following.

THEOREM 12.5. *For any local field K, there exist canonical isomorphisms*

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

The first map is an inflation homomorphism; the second map in this theorem 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 this to prove Theorem 12.4 and hence the local reciprocity law and the norm limitation theorem, we employ the following theorem of Tate, which we will prove a bit later (see Theorem 14.1).

THEOREM 12.6. *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 $H^2(G, M)$.*

In general, for any field K, the group $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*)$ is called the *Brauer group* of K. It is an important invariant of K; it can be realized also in terms of certain noncommutative algebras over K (central simple algebras). I won't pursue this connection further, nor study many of the interesting properties and applications of Brauer groups.

Abstract class field theory.

Having derived local class field theory once, we will do it again a slightly different way. In the course of proving the above results, we will have calculated that if L/K is a cyclic extension of local fields, that

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

It turns out that this alone is enough number-theoretic input to prove local class field theory! More precisely, given a field K with $G = \mathrm{Gal}(\overline{K}/K)$, a continuous G-module A, a surjective continuous homomorphism $d : G \to \widehat{\mathbb{Z}}$, and a homomorphism $v : A^G \to \widehat{\mathbb{Z}}$ satisfying suitable conditions, we will show that for every finite extension L of K there is a canonical isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_L \to \mathrm{Norm}_{L/K} A_K$, where A_K and A_L denote the $\mathrm{Gal}(\overline{K}/K)$ and $\mathrm{Gal}(\overline{K}/L)$-invariants of A. In particular, these conditions will hold for K a local field, $A = \overline{K}^*$, d the map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{\mathrm{unr}}/K)$, and $v : \mathrm{Gal}(K^*) \to \mathbb{Z} \to \widehat{\mathbb{Z}}$ the valuation.

This is the precise sense in which we will use local class field theory as a model for global class field theory. After we complete local class field theory, our next goal will be to construct an analogous module A in the global case which is "complete enough" that its H_T^0 and H_T^{-1} will not be too big; the result will be the idele class group. (One main difference is that in the global case, the analogue of v will really take values in $\widehat{\mathbb{Z}}$, not just $\mathbb{Z}$.)

Exercises.

(1) For $K = \mathbb{Q}_p$, the local reciprocity map plus the local Kronecker-Weber theorem give a canonical map $\mathbb{Q}_p^* \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}}$. What is the map? From the answer, you should be able to turn things around and deduce local Kronecker-Weber from local reciprocity.

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

(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.)

(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 the previous exercise; 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. Give a direct proof of the following consequence of Theorem 12.5: if K is a local field, then any two quaternion algebras which are not split are isomorphic to each other.

CHAPTER 13

Cohomology of local fields: some computations

Reference. Milne, III.2 and III.3; Neukirch, 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.

We now make some computations of $H^i_T(L/K)$ for L/K a finite Galois extension of local fields. To begin with, recall that by "Theorem 90" (Lemma 2.2), $H^1(L/K) = 0$. Our goal in this chapter will be to supplement this fact with a computation of $H^2(L/K)$.

PROPOSITION 13.1. *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 $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subseteq \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z}$.*

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). For convenience, we write U_L for the unit group $\mathfrak{o}_L^*$.

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

PROPOSITION 13.2. *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 (exercise). 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 2.2. Thus $H^0_T(L/K)$ is trivial too, that is, $\mathrm{Norm}_{L/K} : L^* \to K^*$ is surjective. □

PROPOSITION 13.3. *For any finite unramified extension L/K of local fields, the map $\mathrm{Norm}_{L/K} : U_L \to U_K$ is surjective.*

PROOF. Say $u \in U_K$ is a unit. Pick $v_0 \in U_L$ such that in the residue fields, the norm of v_0 coincides with u. Thus $u/\mathrm{Norm}(v_0) \equiv 1 \pmod{\pi}$, where π is a uniformizer of K. Now we construct units $v_i \equiv 1 \pmod{\pi^i}$ such that $u_i = u/\mathrm{Norm}(v_0 \cdots v_i) \equiv 1 \pmod{\pi^{i+1}}$: 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 13.4. *For any finite unramified extensions L/K of local fields, then $H_T^i(\mathrm{Gal}(L/K), U_L) = 1$ for all $i \in \mathbb{Z}$.*

PROOF. Again, $\mathrm{Gal}(L/K)$ is cyclic, so by Theorem 10.1 we need only check this for $i = 0, 1$. For $i = 1$, the desired equality is Lemma 2.2; for $i = 0$, it is the previous proposition. □

Using the Herbrand quotient, we get $h(L^*) = h(U_L)h(L^*/U_L)$. The previous corollary says that $h(U_L) = 1$, and

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

Since $H_T^1(\mathrm{Gal}(L/K), L^*)$ is trivial, we conclude $H_T^0(\mathrm{Gal}(L/K), L^*)$ has order $[L : K]$. In fact, it is cyclic: the long exact sequence of Tate groups gives

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

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. Since $\mathbb{Q}$ is injective as an abelian group, it is also injective as a G-module for any group G (exercise). Thus we get an isomorphism $H_T^0(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^{-1}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$. 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

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

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

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

What's really going on here is that $H_T^0(\mathrm{Gal}(L/K), L^*)$ is a cyclic group generated by a uniformizer π (since every unit is a norm). Under the map $H_T^0(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$, 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, $H_T^1(L/K)$ is trivial by Lemma 2.2, so all there is to compute is $H_T^0(L/K)$. 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 13.5. *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 9.4, 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 13.6. *Let L/K be a finite Galois extension of local fields. Then there is an open, Galois-stable subgroup W of $U_L = \mathfrak{o}_L^*$ such that $H^i(\mathrm{Gal}(L/K), W) = 0$ for all $i > 0$.*

PROOF. Take V as in the previous lemma. 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 $W = \exp(V)$. □

Since the quotient U_L/W is finite, its Herbrand quotient is 1, so $h(U_L) = h(V) = 1$. So again we may conclude that $h(L^*) = h(U_L)h(\mathbb{Z}) = [L : K]$, and so $H_T^0(\mathrm{Gal}(L/K), L^*) = [L : K]$. However, we cannot yet check that $H_T^0(\mathrm{Gal}(L/K), L^*)$ is cyclic because the groups $H_T^1(\mathrm{Gal}(L/K), U_L)$ are not guaranteed to vanish; see the exercises.

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; see Milne, Remark II.1.35.

PROPOSITION 13.7 (Inflation-Restriction Exact Sequence). *Let G be a finite group, H a normal subgroup, and M a G-module. If $H^i(H, M) = 0$ for $i = 1, \ldots, r-1$, then*

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

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 9.3) that there is an injective homomorphism $M \to \mathrm{Ind}_1^G M$ of G-modules. Let N be the G-module which makes the sequence

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

exact. We construct a commutative diagram

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

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

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

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. □

By Lemma 2.2, we have the following.

COROLLARY 13.8. *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.

We now prove the following.

PROPOSITION 13.9. *For any finite Galois extension L/K of local fields, the group $H^2(\mathrm{Gal}(L/K), L^*)$ has order at most $[L : K]$.*

A key fact we need to recall is that any finite Galois extension of local fields is *solvable*: the maximal unramified extension is cyclic, the maximal tamely ramified extension is cyclic over that, and the rest is an extension of order a power of p, so its Galois group is automatically solvable. This lets us induct on $[L : K]$.

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, we can find a Galois subextension M/K. Now the exact sequence

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

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 $[L:K]$. Let M/K be an unramified extension of degree $[L:K]$. Then we have a diagram

$$\begin{array}{ccccccc} & & & & H^2(M/K) & & \\ & & & & \downarrow{\scriptstyle \mathrm{Inf}} & \searrow & \\ 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\mathrm{Inf}} & H^2(ML/K) & \xrightarrow{\mathrm{Res}} & H^2(ML/L) \end{array}$$

in which the bottom row is exact and the vertical arrows are injective, both by Corollary 13.8. It suffices to show that the diagonal arrow $H^2(M/K) \to H^2(ML/L)$ is the zero map; then we can push a generator of $H^2(M/K)$ down to $H^2(ML/K)$, then pull it back to $H^2(L/K)$ by exactness to get an element of order $[L:K]$.

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

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

in which the vertical arrows are isomorphisms. (Remember that extended functoriality for Tate groups starts in degree 0, yielding the first horizontal arrow.) 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. This composition is none other than the canonical map $K^*/\operatorname{Norm}_{M/K} M^* \to L^*/\operatorname{Norm}_{ML/L}(ML)^*$. 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.

Note. If L/K is a finite extension of degree n, then the map $\mathrm{Res} : H^2(K^{\mathrm{unr}}/K) \to H^2(L^{\mathrm{unr}}/L)$ translates, via the local reciprocity map, into a map from $\mathbb{Q}/\mathbb{Z}$ to itself. This map turns out to be multiplication by n (see Milne, Proposition II.2.7).

The local invariant map.

By staring again at the above argument, we can in fact prove that $H^2(\overline{K}/K) \cong \mathbb{Q}/\mathbb{Z}$. First of all, we have an injection $H^2(K^{\mathrm{unr}}/K) \to H^2(\overline{K}/K)$ by Corollary 13.8, 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 $H^2(K^{\mathrm{unr}}/K) \to H^2(\overline{K}/K)$. Since that's true for any M, we get that the map is indeed surjective, hence an isomorphism.

Next time, we'll use this map to obtain the local reciprocity map.

Exercises.

(1) Give an elementary proof (without cohomology) that the norm map from one finite field to another is always surjective.
(2) Give an example of a cyclic ramified extension L/K of local fields in which the groups $H^i_T(\mathrm{Gal}(L/K), U_L)$ are nontrivial.

CHAPTER 14

Local class field theory via Tate's theorem

Reference. Milne II.3, III.5.

For L/K a finite extension of local fields, we have now computed that $H^1(L/K) = 0$ (Lemma 2.2) and $H^2(L/K)$ is cyclic of order $[L:K]$ (Proposition 13.1). In this chapter, we 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 12.6).

THEOREM 14.1 (Tate). *Let G be a finite (solvable) 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 $H_T^i(G,\mathbb{Z}) \to H_T^{i+2}(G,M)$ 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 $\mathrm{Cor} \circ \mathrm{Res} = [G:H]$, $\mathrm{Res}(\gamma)$ 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 $\phi(e,e,e)$.) 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.)

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:

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

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 14.2 below to conclude that $H^i_T(G, M) = 0$ 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 10.1) to conclude that $H^i_T(G, \mathbb{Z}) \cong H^{i+2}_T(G, M)$. □

Note: we only need the results of this section for G solvable, because in our desired application G is the Galois group of a finite extension of local fields. But one can remove this restriction: see the note after this lemma.

LEMMA 14.2. *Let G be a finite (solvable) 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 $H^i_T(G, M) = 0$ for all $i \in \mathbb{Z}$.*

PROOF. For G cyclic, this follows by periodicity. 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, $H^i_T(H, M) = 0$ for all i. Thus by the inflation-restriction exact sequence (Proposition 13.7),

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

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 10.1), $H^i_T(G/H, M^H) = 0$ 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 $H^0_T(G, M)$, we have that $H^0_T(G/H, M^H) = 0$, so for any $x \in M^G$, there exists $y \in M^H$ such that $\mathrm{Norm}_{G/H}(y) = x$. Since $H^0_T(H, M) = 0$, 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 $H^0_T(G, M) = 0$, as desired.

So far so good, but we want to kill off the Tate groups with negative indices too, so we do a dimension shift. 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 $H^{i+1}_T(H', N) \cong H^i_T(H', M)$ for any subgroup H' of G. In particular, $H^1(H', N) = H^2(H', N) = 0$, so the above argument gives $H^i_T(G, N) = 0$ for $i \geq 0$. Now from $H^0_T(G, N) = 0$ we get $H^{-1}_T(G, M) = 0$; since the same argument applies to N, we also get $H^{-2}_T(G, M) = 0$ and so on. □

To go from the solvable case to the general case, one shows that the p-primary component of $H^i(G, M)$ injects into $H^i(G_p, M)$, where G_p is the p-Sylow subgroup. (Apply $\mathrm{Cor} \circ \mathrm{Res}$ from G to G_p; the result is multiplication by $[G : H]$ which is prime to p.)

The results of local class field theory.

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 14.1 with for $G = \mathrm{Gal}(L/K)$, $M = L^*$ to obtain isomorphisms $H_T^i(G, \mathbb{Z}) \to H_T^{i+2}(G, M)$, thus proving Theorem 12.4. This yields a canonical isomorphism

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

This establishes the existence of the local reciprocity map (Theorem 12.1; note that part (a) follows from the explicit computations in Chapter 13) and the norm limitation theorem (Theorem 12.3), modulo one subtlety: if M/K is another finite Galois extension containing L, we need to know that the diagram

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

commutes, so 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

$$\begin{array}{ccc} H_T^0(\mathrm{Gal}(M/K), M^*) & \longrightarrow & H_T^{-1}(\mathrm{Gal}(M/K), I_{\mathrm{Gal}(M/K)}) \\ \downarrow & & \downarrow \\ H_T^0(\mathrm{Gal}(L/K), L^*) & \longrightarrow & H_T^{-1}(\mathrm{Gal}(L/K), I_{\mathrm{Gal}(L/K)}) \end{array}$$

This appears to be a gap in Milne's presentation. To fix it, choose a 2-cocycle $\phi_M : \mathrm{Gal}(M/K)^3 \to M^*$ representing the preferred generator of $H^2(M/K)$; then the upper horizontal arrow is a connecting homomorphism for the exact sequence

$$1 \to M^* \to M^*[\phi_M] \to I_{\mathrm{Gal}(M/K)} \to 1.$$

The lower horizontal arrow arises similarly from the exact sequence

$$1 \to L^* \to L^*[\phi_L] \to I_{\mathrm{Gal}(L/K)} \to 1,$$

where ϕ_L represents a class whose inflation is $[G : H]$ times the class represented by ϕ_M. Further details omitted.

In any case, it remains to prove the local existence theorem (Theorem 12.2). We begin with a lemma, in which we take advantage of Kummer theory to establish an easy case of the existence theorem.

LEMMA 14.3. *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* $\operatorname{Norm}_{L/K} L^*$ *for every cyclic extension L of K of degree ℓ.*

The same statement holds even if ℓ is not prime (exercise) and can be interpreted in terms of the *Hilbert symbol*, whose properties generalize quadratic reciprocity to higher powers; see Milne, III.4.

PROOF. Let M be the compositum of all cyclic ℓ-extensions of K. The group $K^*/(K^*)^\ell$ is finite (exercise), and hence is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^n$ for some positive integer n. By Kummer theory (Theorem 2.3), we also have $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^n$.

By the local reciprocity law, $K^*/\operatorname{Norm}_{M/K} M^* \cong (\mathbb{Z}/\ell\mathbb{Z})^n$; 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. □

This allows to deduce a corollary of the existence theorem which is needed in its proof.

COROLLARY 14.4. *Let K be a local field. 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 $D_K \subseteq U_K$ by considering unramified extensions of K, so D_K is in particular a compact topological group. By Lemma 14.3, every element of D_K is an ℓ-th power in K for every prime ℓ; it remains to check that one can find an ℓ-th root which is also in D_K. This would then imply that D_K is a divisible subgroup of U_K, and hence the trivial group (see exercises).

For L/K a finite extension, it is true but not immediately clear that

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

that is, for $x \in D_K$, for each finite extension M of K, $x = \operatorname{Norm}_{M/K}(z)$ for some $z \in M$, but may not be apparent that the elements $y = \operatorname{Norm}_{M/L}(z)$ can be chosen to be equal. However, for a given M, the set of such y is a nonempty compact subset of U_L, and any finite intersection of these sets is nonempty (since it contains the set corresponding to the compositum of the corresponding fields), so the whole intersection is nonempty.

Let ℓ be a prime number 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 (it can contain at most ℓ elements) and nonempty: we have $x = \operatorname{Norm}_{L/K}(y)$ for some $y \in D_L$, so y has an ℓ-th root z in L and $\operatorname{Norm}_{L/K}(z) \in E(L)$. Again by the finite intersection property, we find an ℓ-th root of x in K belonging to D_K, completing the proof. □

Returning to the local existence theorem, let U be an open subgroup of K^* of finite index; we wish to find a finite abelian extension L of K such that $U = \operatorname{Norm}_{L/K} L^*$. We note first that by the local reciprocity law, 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 $\operatorname{Gal}(L/M)$ for some intermediate extension M/K having the desired effect. We note next that by the norm limitation theorem, it suffices to produce *any* finite extension L/K, not necessarily abelian, such that U contains $\operatorname{Norm}_{L/K} L^*$.

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

$$(\operatorname{Norm}_{L/K} L^*) \cap U_K \subseteq U \cap U_K.$$

Since U_K is compact, each open subgroup $(\operatorname{Norm}_{L/K} L^*) \cap U_K$ is also closed and hence compact. By Corollary 14.4, as L/K runs over all finite extensions of K, the intersection of the groups $(\operatorname{Norm}_{L/K} L^*) \cap U_K$ is trivial; in particular, the intersection of the compact subsets

$$((\operatorname{Norm}_{L/K} L^*) \cap U_K) \cap (U_K \setminus U)$$

of U_K is empty. By the finite intersection property (and taking a compositum), there exists a single L/K for which $(\mathrm{Norm}_{L/K} L^*) \cap U_K \subseteq U \cap U_K$; this completes the proof of Theorem 12.2.

Making things 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.

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. In general, one can at least do the following, imitating our proof that $H^2(L/K)$ is cyclic of order n. 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 $H_T^0(M/K) = K^*/\mathrm{Norm}_{M/K} M^*$, 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 10.1:

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

(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 $x \in H_T^0(M/K) = M^G/\mathrm{Norm}_G(M)$, 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 $i, j = 0, \dots, \#G - 1$. 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 $i, j = 0, \dots, \#G - 1$)

$$\begin{aligned}\psi_2(e, g^i, g^{i+j}) &= \psi_1(g^i, g^{i+j}) - \psi_1(e, g^{i+j}) + \psi_1(e, g^i) \\ &= x \otimes ([e] + \cdots + [g^{i-1}] + [g^i] + \cdots + [g^{i+j-1}] - [e] - \cdots - [g^{i+j-1}]) \\ &= \begin{cases} 0 & i + j < \#G \\ -x \otimes ([e] + \cdots + [g^{\#G-1}]) & i + j \geq \#G. \end{cases}\end{aligned}$$

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 $i + j \geq \#G$.

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 $\mathrm{Gal}(ML/K)$.

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 14.3 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.)

CHAPTER 15

Abstract class field theory

Reference. Neukirch, IV.4-IV.6. Remember that Neukirch's cohomology groups are all Tate groups, so he doesn't put the subscript "T" on them.

We now turn to an alternate method for deriving the main result of local class field theory, the local reciprocity law. This method, based on a presentation of Artin and Tate, makes it clear what the main cohomological inputs are in the local case, and gives an outline of how to proceed to global class field theory. (Warning: this method does not give information about the local invariant map.)

Caveat. We are going to work with the absolute Galois group of a field K, i.e., the Galois group of its algebraic closure. One could work with a smaller overfield as well. In fact, one can go further: one really is working with the Galois group and not the fields, so one can replace the Galois group by an arbitrary profinite group! This is what Neukirch does, but fortunately he softens the blow by "pretending" that his profinite group corresponds to a field and its extensions via the Galois correspondence. This means you can simply assume that his group G is the absolute Galois group of a field without getting confused.

Caveat. Certain words you thought you knew what they meant, such as "unramified", are going to be reassigned more abstract meanings. But these meanings will coincide with the correct definitions over a local field.

Abstract ramification theory.

Let k be a field, $\overline{k}$ a separable closure of k, and $G = \mathrm{Gal}(\overline{k}/k)$. 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 $\mathrm{Gal}(k^{\mathrm{unr}}/k) \cong \widehat{\mathbb{Z}}$.

We now make some constructions that, in our example, recover information about ramification of extensions of k. For starters, define the *inertia group* I_k as the kernel of d, and define the *maximal unramified extension* k^{unr} of k as the fixed field of I_k. More generally, for any field L between k and $\overline{k}$, put $G_L = \mathrm{Gal}(\overline{k}/L)$, put $I_L = G_L \cap I_k$ and let L^{unr} be the fixed field of I_L. We say an extension L/K is *unramified* if $L \subseteq K^{\mathrm{unr}}$. Note that this implies that G_L contains I_K, necessarily as a normal subgroup, and $G_L/I_K \subseteq G_K/I_K$ injects via d into $\widehat{\mathbb{Z}}$; thus G_L/I_K is abelian and any finite quotient of it is cyclic. In particular, G_K is Galois 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}.) If $K \neq k$, then d doesn't map G_K onto $\widehat{\mathbb{Z}}$, so it will be convenient to renormalize things. Put

$$d_K = \frac{1}{[\widehat{\mathbb{Z}} : d(G_K)]} d : G_K \to \widehat{\mathbb{Z}};$$

then d_K is surjective, and induces an isomorphism $d_K : \mathrm{Gal}(K^{\mathrm{unr}}/K) \to \widehat{\mathbb{Z}}$.

Given a finite extension L/K of fields between k and $\overline{k}$, 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: $e_{M/K} = e_{M/L}e_{L/K}$ and $f_{M/K} = f_{M/L}f_{L/K}$. 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 same is true 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.

Now suppose that, in addition to the field k and the map $d : G \to \widehat{\mathbb{Z}}$, we have a G-module A (written multiplicatively) and a homomorphism $v : A^G \to \widehat{\mathbb{Z}}$. We wish to write down conditions that will be satisfied in case k is a local field (with d as before, $A = \overline{k}^*$ and $v : k^* \to \mathbb{Z}$ the valuation of the local field), but which will in general give a notion of "valuation" on all of A.

Given k, $d : G \to \widehat{\mathbb{Z}}$, and the G-module A, write $A_K = A^{G_K} = A^{\mathrm{Gal}(K/k)}$ for any field K between k and $\overline{k}$. Also, recall that the norm map $\mathrm{Norm}_{L/K} : A_L \to A_K$ is given by $\mathrm{Norm}_{L/K}(a) = \prod_g a^g$, where g runs over a set of right coset representatives of G_K in G_L, at least when L is finite. (The norm doesn't make sense for an infinite extension, but it still makes sense to write $\mathrm{Norm}_{L/K} A_L$ to mean the intersection of $\mathrm{Norm}_{M/K} A_M$ over all finite subextensions M/K of L.)

A *henselian valuation* of A_k with respect to d is a homomorphism $v : A_k \to \widehat{\mathbb{Z}}$ such that:

(a) if $Z = \mathrm{im}(v)$, then Z contains $\mathbb{Z}$ and $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$ for all positive integers n;
(b) $v(\mathrm{Norm}_{K/k} A_K) = f_{K/k}Z$ for all finite extensions K of k.

This valuation immediately extends to a valuation $v_K : A_K \to Z$ for all fields K between k and $\overline{k}$, by setting

$$v_K = \frac{1}{f_{K/k}} \circ \mathrm{Norm}_{K/k}.$$

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, $v_K(\mathrm{Norm}_{L/K}(a)) = f_{L/K}v_L(a)$ for any $a \in A_L$.

For any field K between k and $\overline{k}$, define the *unit subgroup* U_K as the set of $u \in A_K$ with $v_k(u) = 0$. If K/k is finite, we say $\pi \in A_K$ is a *uniformizer* for K if $v_K(\pi) = 1$.

The reciprocity map: definition.

Warning. The multiplicativity of the reciprocity map is proven in Neukirch (Proposition IV.5.5), but I find this proof unreadable.

Now we bring in the key cohomological input. Suppose that for every *cyclic* extension L/K of finite extensions of k,

$$\#H^i_T(\mathrm{Gal}(L/K), A_L) = \begin{cases} [L : K] & i = 0 \\ 1 & i = -1. \end{cases}$$

In Neukirch, this assumption is called the *class field axiom*. (Note that it's not enough just to check cyclic extensions of k itself.) Then we will prove the following theorem.

THEOREM 15.1 (Reciprocity law). *For each finite Galois extension L/K of finite extensions of k, there is a canonical isomorphism $r_{L/K} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\operatorname{Norm}_{L/K} A_L$.*

Since we've already checked the class field axiom in the example where k is a local field and $A = \overline{k}^*$, this immediately recovers the local reciprocity law.

Before defining the reciprocity map, we verify a consequence of the class field axiom. (Notice the similarities between this argument and what we have done; essentially we are running the computation of the cohomology of an unramified extension of local fields in reverse!)

PROPOSITION 15.2. *For L/K an unramified extension of finite extensions of k (i.e., $e_{L/K} = 1$), the class field axiom implies that $H_T^i(\mathrm{Gal}(L/K), U_L) = 1$ for $i = 0, -1$. Moreover, $H_T^1(\mathrm{Gal}(L/K), A_L)$ is cyclic and is 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. Note that an unramified extension is always Galois and cyclic. Consider the short exact sequence $0 \to U_L \to A_L \to A_L/U_L \to 0$. Applying Herbrand quotients, we have $h(A_L) = h(U_L)h(A_L/U_L)$, where $h(A_L) = \#H_T^0(A_L)/\#H_T^{-1}(A_L)$ and so on. By the class field axiom, $h(A_K) = [L : K]$. Also, A_L/U_L is isomorphic to $Z = \mathrm{im}(v)$ with trivial group action, so $H_T^0(Z)$ is cyclic of order $[L : K]$ and $H_T^{-1}(Z)$ is trivial. (Recall that $H_T^0(Z) = Z/\operatorname{Norm}(Z)$ and $H_T^{-1}(Z) = \ker(\mathrm{Norm})$, since the action is trivial.) Otherwise put, the long exact sequence in Tate groups gives

$$1 = H_T^{-1}(A_L/U_L) \to H_T^0(U_L) \to H_T^0(A_L) \to H_T^0(A_L/U_L) \to H_T^1(U_L) \to H_T^1(A_L) = 1$$

and the two groups in the middle have the same order, so we just have to show that one of the outer groups is trivial, and then the middle map will be an isomorphism.

Thus it suffices to check that $H_T^1(U_L) = 1$, or equivalently $H_T^{-1}(U_L) = 1$. Here is where we use that L/K is unramified, not just cyclic. Recall that $H_T^{-1}(U_L)$ consists of elements u of U_L of norm 1, modulo those of the form v^σ/v for some $v \in U_L$, where σ is a generator of $\mathrm{Gal}(L/K)$. By hypothesis, $H_T^{-1}(A_L)$ is trivial, so any $u \in U_L$ of norm 1 can be written as w^σ/w for some $w \in A_L$. Now because L/K is unramified, there exists $x \in A_K$ such that $w/x \in U_L$. Now $u = v^\sigma/v$ for $v = w/x$, so u defines the trivial class in $H_T^{-1}(U_L)$, proving the claim. □

COROLLARY 15.3. *If L/K is unramified, then $U_K = \operatorname{Norm}_{L/K} U_L$. (Remember, this makes sense even if L/K is not finite!)*

We now define the reciprocity map $r : \mathrm{Gal}(L/K) \to A_K/\operatorname{Norm}_{L/K} A_L$; as a bonus, this definition will actually give an explicit recipe for computing the reciprocity map in local class field theory. For starters, 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 $g \in \mathrm{Gal}(L^{\mathrm{unr}}/K)$, let M be the fixed field of g (so that $e(M/K) = e((M \cap L)/K)$ and $f(M/K) = d_K(g)$), and set $r'(g) = \operatorname{Norm}_{M/K}(\pi_M)$ for some uniformizer π_M. This doesn't depend on the choice of uniformizer: if π'_M is another one, then $\pi_M/\pi'_M \in U_L$ belongs to $\operatorname{Norm}_{L^{\mathrm{unr}}/L} U_{L^{\mathrm{unr}}}$ by

Corollary 15.3, so $\mathrm{Norm}_{M/K}(\pi_M/\pi'_M)$ belongs to $\mathrm{Norm}_{L^{\mathrm{unr}}/K} U_{L^{\mathrm{unr}}} \subseteq \mathrm{Norm}_{L/K} U_L$. So at least r' is now a well-defined map, if not yet a semigroup homomorphism.

Let's make some other easy observations about this definition before doing the hard stuff. Note that 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. Also, if $g \in H$ is actually in $\mathrm{Gal}(L^{\mathrm{unr}}/L)$, then $r'(g) \in \mathrm{Norm}_{L/K} A_L$. In that case, M contains L, so $r'(g) = \mathrm{Norm}_{M/K}(\pi_M)$ can be rewritten as $\mathrm{Norm}_{L/K} \mathrm{Norm}_{M/L}(\pi_M)$, so is clearly a norm. That is, if r' were known to be multiplicative, it would induce a group homomorphism from $\mathrm{Gal}(L/K)$ to $A_K/\mathrm{Norm}_{L/K} A_L$.

Now for the hard part: we have to check that r' is multiplicative. 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 π_i be a uniformizer of M_i, and put $\rho_i = r(g_i) = \mathrm{Norm}_{M_i/K}(\pi_i)$. Again, we want $\rho_1\rho_2/\rho_3$ to be in $\mathrm{Norm}_{L^{\mathrm{unr}}/K} A_{L^{\mathrm{unr}}}$; what makes this hard is that the ρ_i all lie in different fields over K. At least one thing is clear: $v_K(\rho_i) = f(M_i/K) v_{M_i}(\pi_i) = f(M_i/K) = d_K(g_i)$, so $v_K(\rho_1\rho_2/\rho_3) = 0$.

To make progress, we have to push our problem into a single field. Choose $\phi \in \mathrm{Gal}(L^{\mathrm{unr}}/K)$ such that $d_K(\phi) = 1$, and put $d_i = d_K(g_i)$; then we can write $g_i = \phi^{d_i} h_i$ for some h_i with $d_K(h_i) = 0$, that is, $h_i \in \mathrm{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}})$. Put

$$\sigma_i = \pi_i \pi_i^{\phi} \cdots \pi_i^{\phi^{d_i - 1}};$$

then $\rho_i = \mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\sigma_i)$.

Proposition 15.4. *Let M be the fixed field of some $h \in \mathrm{Gal}(L^{\mathrm{unr}}/K)$ with $d_K(h) = n$ a positive integer, and suppose $\phi \in H$ satisfies $d_K(\phi) = 1$. Then for any $x \in A_M$,*

$$\mathrm{Norm}_{M/K}(x) = \mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(x x^{\phi} \cdots x^{\phi^{n-1}}).$$

Now put $u = \sigma_1\sigma_2/\sigma_3$; then $u \in U_{L^{\mathrm{unr}}}$ and $\mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(u) = \rho_1\rho_2/\rho_3$ is the thing we need to be in $\mathrm{Norm}_{L/K} U_L$. Let N be a finite unramified extension of L such that $u \in U_N$. Then $\mathrm{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(u) = \mathrm{Norm}_{N/N\cap K^{\mathrm{unr}}}(u)$, and by the lemma below, that implies that $u \in \mathrm{Norm}_{N/K} U_N$ and so $u \in \mathrm{Norm}_{L/K}(U_L)$.

Lemma 15.5. *If M/L and L/K are finite extensions with M/K Galois and L/K unramified, and $u \in U_M$ is such that $\mathrm{Norm}_{M/L}(u) \in U_K$, then $\mathrm{Norm}_{M/L}(u) \in \mathrm{Norm}_{M/K} U_L$.*

Proof. There is a noncohomological proof in Neukirch (Lemma IV.5.4), but I couldn't follow it, so here's a cohomological argument instead. If $v = \mathrm{Norm}_{M/L}(u) \in U_K$, then v represents an element of $H_T^0(\mathrm{Gal}(M/K), U_M) = U_K/\mathrm{Norm}_{M/K}(U_M)$ which maps to zero under the map $\mathrm{Res} : H_T^0(\mathrm{Gal}(M/K), U_M) \to H_T^0(\mathrm{Gal}(M/L), U_M)$. By the following lemma, v is then in the image of $\mathrm{Inf} : H_T^0(\mathrm{Gal}(L/K), U_L) \to H_T^0(\mathrm{Gal}(M/K), U_M)$; but the former space is zero by Corollary 15.3! Thus v is cohomologous to zero in $H_T^0(\mathrm{Gal}(M/K), U_M)$; that is, $v = \mathrm{Norm}_{M/K}(w)$ for some $w \in U_M$. □

This lemma is of course a variant of the inflation-restriction exact sequence; we get it from there by dimension shifting.

Lemma 15.6. *Let H be a normal subgroup of a finite group G and M a G-module. Then the sequence*

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

is exact.

PROOF. Choose N so that $0 \to N \to \operatorname{Ind}_1^G M \to M \to 0$ is exact (where again $\operatorname{Ind}_1^G M \to M$ is the map $m \otimes [g] \mapsto m^g$); then by the usual inflation-restriction exact sequence (Proposition 13.7),

$$0 \to H_T^1(G/H, N^H) \xrightarrow{\text{Inf}} H_T^1(G, N) \xrightarrow{\text{Res}} H_T^1(H, N)$$

is exact. Now $\operatorname{Ind}_1^G M$ is acyclic for G and for H, and $(\operatorname{Ind}_1^G M)^H$ is acyclic for G/H. Moreover, if we take H-invariants, we have an exact sequence

$$0 \to N^H \to (\operatorname{Ind}_1^G M)^H \to M^H \to 0;$$

namely, exactness on the right holds because any $m \in M^H$ lifts to $m \otimes [1] \in (\operatorname{Ind}_1^G M)^H$. Using long exact sequences, we may thus shift dimensions to deduce the desired result. □

Putting everything together, we have a semigroup homomorphism $r' : H \to A_K / \operatorname{Norm}_{L/K} A_L$ which kills $\operatorname{Gal}(L^{\text{unr}}/L)$. Thus r' induces a homomorphism $r = r_{L/K} : \operatorname{Gal}(L/K) \to A_K / \operatorname{Norm}_{L/K} A_L$. We call this the *reciprocity map*. Some straightforward functorialities are left to the reader, including the following.

PROPOSITION 15.7. *If L/K and L'/K' are finite Galois extensions such that $K \subseteq K'$ and $L \subseteq L'$, then the natural map $\operatorname{Gal}(L'/K')^{\text{ab}} \to \operatorname{Gal}(L/K)^{\text{ab}}$ is compatible via the reciprocity map with $\operatorname{Norm}_{K'/K} : A_{K'} \to A_K$. If moreover $K' \subseteq L$, then the natural map $A_K \to A_{K'}$ is compatible with the transfer map $\operatorname{Ver} : \operatorname{Gal}(L/K)^{\text{ab}} \to \operatorname{Gal}(L'/K')^{\text{ab}}$.*

Proof of the reciprocity law.

We continue to assume the class field axiom. Recall that we want the following result.

THEOREM 15.8 (Reciprocity law). *For each finite Galois extension L/K of finite extensions of k, there is a canonical isomorphism $r_{L/K} : \operatorname{Gal}(L/K)^{\text{ab}} \to A_K / \operatorname{Norm}_{L/K} A_L$.*

From the definition of r, it's easy enough to check this for L/K unramified.

PROPOSITION 15.9. *If L/K is finite unramified, the reciprocity map $r_{L/K}$ sends the Frobenius of $\operatorname{Gal}(L/K)$ to a uniformizer of K, and is an isomorphism.*

PROOF. The groups $\operatorname{Gal}(L/K)$ and $A_K / \operatorname{Norm}_{L/K}(A_L) = H_T^0(\operatorname{Gal}(L/K), A_L)$ are both cyclic of the same order $[L : K]$, the latter by the class field axiom. If $g \in \operatorname{Gal}(L/K)$ is the Frobenius, and $h \in \operatorname{Gal}(L^{\text{unr}}/K)$ lifts h, then the fixed field of h is just K itself, and from the definition of r', $r(g) = r'(h)$ is just a uniformizer of K. Since that uniformizer generates $H^0(\operatorname{Gal}(L/K), A_L)$, we conclude $r_{L/K}$ is an isomorphism. □

PROPOSITION 15.10. *If L/K is finite, cyclic and totally ramified (i.e., $f_{L/K} = 1$), then $r_{L/K}$ is an isomorphism.*

PROOF. Since $r_{L/K}$ maps between two groups of the same order by the H_T^0 clause of the class field axiom, it suffices to show that it is injective.

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 $\operatorname{Gal}(L/K) \times \operatorname{Gal}(K^{\text{unr}}/K)$.

Let g be a generator of the first factor and ϕ a generator of the second factor. Put $\tau = g\phi$, so that $d_K(\tau) = 1$, and let M be the fixed field of τ. Pick uniformizers pi_L and π_M of L and M, so that $r(g) = r'(\tau) = \operatorname{Norm}_{M/K}(\pi_M)$. Let N be the compositum of L and M.

Put $n = [L : K]$, and suppose $r(g^j) = \operatorname{Norm}_{M/K}(\pi_M^j)$ is the identity in $A_K/\operatorname{Norm}_{L/K} A_L$. Since $d_K(\tau) = 1$, we have $r(g) = \operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\pi_M)$. On the other hand (by Proposition 15.4 with $n = 0$!), $\operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\pi_L)$ is the identity in $A_K/\operatorname{Norm}_{L/K} A_L$. Thus we also have $r(g) = \operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(\pi_M/\pi_L)$.

Put $u = \pi_L^j/\pi_M^j \in U_N$. If $r(g^j)$ is in $\operatorname{Norm}_{L/K} A_L$, then there exists $v \in U_L$ such that $\operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(v) = \operatorname{Norm}_{L^{\mathrm{unr}}/K^{\mathrm{unr}}}(u)$. By the H_T^{-1} clause of the class field axiom, we can write u/v as a^g/a for some $a \in A_N$. Now

$$(\pi_L^j/v)^{g-1} = (\pi_L^j/v)^{\tau-1} = (\pi_M^j u/v)^{\tau-1} = (u/v)^{\tau-1} = (a^\tau/a)^{g-1}.$$

If we put $x = (\pi_L^j/v)(a/a^\tau)$, that means x is g-invariant, so it belongs to A_{N_0}, where $N_0 = N \cap K^{\mathrm{unr}}$. On one hand, that means $v_{N_0}(x) \in \widehat{\mathbb{Z}}$. On the other hand, we have $n v_{N_0}(x) = v_N(x) = j$. Thus j is a multiple of n, and r must be injective. □

Now we proceed to the proof of the reciprocity law. Any resemblance with the method used to calculate the local invariant map is not coincidental!

Proof of Theorem 15.8. For reference, we record the following commutative diagram, for L/K a finite extension and M an intermediate field:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(L/M) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle r_{L/M}} & & \downarrow{\scriptstyle r_{L/K}} & & \downarrow{\scriptstyle r_{M/K}} & & \\
 & & A_M/\operatorname{Norm}_{L/M} A_L & \xrightarrow{\operatorname{Norm}_{M/K}} & A_K/\operatorname{Norm}_{L/K} A_L & \longrightarrow & A_K/\operatorname{Norm}_{M/K} A_M & \longrightarrow & 1
\end{array}$$

in which the rows are exact. We're going to do a lot of diagram-chasing on this picture.

First suppose L/K is abelian; we induct on $[L : K]$. If L/K is cyclic of prime order, then either it is unramified or totally ramified, and we already know $r_{L/K}$ is an isomorphism in those cases. Otherwise, let M be a subextension of L/K. Then chasing the above diagram gives that $r_{L/K}$ is surjective. Now the diagram shows that the kernel of $r_{L/K}$ lies in the kernel of $\mathrm{Gal}(L/K) \to \mathrm{Gal}(N/K)$ for *every* proper subextension N of L/K. Since L/K is abelian, the intersection of these kernels is trivial. Thus $r_{L/K}$ is also injective, so is an isomorphism.

Next, suppose L/K is solvable; we again induct on $[L : K]$. If L is abelian, we are done. If not, let M be the maximal abelian subextension of L/K; by the same diagram chase as in the previous paragraph, $r_{L/K}$ is surjective. Also, we have a diagram

$$\begin{array}{ccc}
\mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{r_{L/K}} & A_K/\operatorname{Norm}_{L/K} A_L \\
\downarrow & & \downarrow \\
\mathrm{Gal}(M/K) & \xrightarrow{r_{M/K}} & A_K/\operatorname{Norm}_{M/K} A_M
\end{array}$$

in which the left vertical and bottom horizontal arrows are isomorphisms. Thus the composite $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\operatorname{Norm}_{M/K} A_M$ is an isomorphism, so $r_{L/K}$ must be injective. Again, we conclude $r_{L/K}$ is an isomorphism.

Finally, let L/K be not solvable. The same argument as in the previous paragraph shows that $r_{L/K}$ is injective. To show $r_{L/K}$ is surjective, let M be the fixed field of a p-Sylow subgroup of $\mathrm{Gal}(L/K)$. Then M/K need not be Galois, so the original diagram doesn't actually make sense. But the square on the left still commutes, and $r_{L/M}$ is an isomorphism by what we already know. If we can show the bottom arrow $\mathrm{Norm}_{M/K}$ surjects onto the p-Sylow subgroup S_p of $A_K/\mathrm{Norm}_{L/K} A_L$, then the same will be true of $r_{L/K}$. In fact, the inclusion $A_K \subseteq A_M$ induces a homomorphism $i : A_K/\mathrm{Norm}_{L/K} A_L \to A_M/\mathrm{Norm}_{L/M} A_L$ such that $\mathrm{Norm}_{M/K} \circ i$ is multiplication by $[M : K]$, which is not divisible by p, and so is an isomorphism on S_p. Thus $\mathrm{Norm}_{M/K}$ surjects onto S_p, as does $r_{L/K}$; since $r_{L/K}$ surjects onto each p-Sylow subgroup of $A_K/\mathrm{Norm}_{L/K} A_L$, it is in fact surjective. □

As a bonus byproduct of the proof, we get the following.

COROLLARY 15.11 (Norm limitation theorem). *If M is the maximal abelian subextension of the finite Galois extension L/K, then* $\mathrm{Norm}_{L/K} A_L = \mathrm{Norm}_{M/K} A_M$.

A look ahead.

What does this tell us about the global Artin reciprocity law? If L/K is a finite abelian extension of number fields, we are trying to prove that $\mathrm{Gal}(L/K)$ is canonically isomorphic to a generalized ideal class group of K. So we need to use for A something 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, 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".

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. But never mind about this; 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.)

Exercises.

(1) Prove Proposition 15.7.

Part 5

The adelic formulation

CHAPTER 16

Adèles and idèles

Reference. Milne, Section V.4; Neukirch, Section VI.1 and VI.2; Lang, *Algebraic Number Theory*, Chapter VII.

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.

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 "La théorie du corps de classes." 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.

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 $\mathfrak{p}$.

The adèles.

The basic idea is that we want some sort of "global completion" of a number field K. In fact, we already know one way to complete $\mathbb{Z}$, namely its profinite completion $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. But we really want something containing $\mathbb{Q}$. We define the *ring of finite adèles* $\mathbb{A}_{\mathbb{Q}}^{\text{fin}}$ 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.

For symmetry, we really should allow *all* places, not just the finite places. So we also define the *ring of adèles* over $\mathbb{Q}$ as $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \mathbb{A}_{\mathbb{Q}}^{\text{fin}}$. Then $\mathbb{A}_{\mathbb{Q}}$ is a locally compact topological ring with a canonical embedding $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$.

Now for a general number field K. The profinite completion $\widehat{\mathfrak{o}_K}$ is canonically isomorphic to $\prod_{\mathfrak{p}} \mathfrak{o}_{K_\mathfrak{p}}$, so we 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* $\prod_p{}' K_\mathfrak{p}$, where we only allow tuples (α_p) for which $\alpha_p \in \mathfrak{o}_{K_\mathfrak{p}}$ for almost all $\mathfrak{p}$.

The ring of adèles $\mathbb{A}_K$ is the product of $\mathbb{A}_K^{\text{fin}}$ with each archimedean completion. (That's one copy of $\mathbb{R}$ for each real embedding and one copy of $\mathbb{C}$ for each conjugate pair of complex embeddings.)

One has a natural norm on the ring of adèles, because one has a natural norm on each completion:

$$|(\alpha_v)_v| = \prod_v |\alpha_v|_v.$$

One should normalize these in the following way: for v real, take $|\cdot|_v$ to be the usual absolute value. For v complex, take $|\cdot|_v$ to be the *square* of the usual absolute value. (That means the result is not an absolute value, in that it doesn't satisfy the triangle inequality. Sorry.) For v nonarchimedean corresponding to a prime above p, normalize so that $|p|_v = p^{-1}$.

Again, there is a natural embedding of K into $\mathbb{A}_K$ because there is such an embedding for each completion. With the normalization as above, one has the product formula:

PROPOSITION 16.1. *If $\alpha \in K$, then $|\alpha| = 1$.*

In particular, K is *discrete* in $\mathbb{A}_K$ (the difference between two elements of K cannot be simultaneously small in all embeddings). This is a generalization/analogue of the fact that $\mathfrak{o}_K$ is discrete in Minkowski space (the product of the archimedean completions).

For any finite set S of places, let $\mathbb{A}_S$ (resp. $\mathbb{A}_S^{\text{fin}}$) 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. Then we have the following result, which is essentially the Chinese remainder theorem.

PROPOSITION 16.2. *For any finite set S of places, $K+\mathbb{A}_S^{\text{fin}} = \mathbb{A}_K^{\text{fin}}$ and $K+\mathbb{A}_S = \mathbb{A}_K$.*

COROLLARY 16.3. *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 $M \times \mathbb{A}_K^{\text{fin}}$ is congruent modulo $\mathfrak{o}_K$ to an element of $T \times \mathbb{A}_K^{\text{fin}}$. By the proposition, the compact set $T \times \mathbb{A}_K^{\text{fin}}$ surjects onto $\mathbb{A}_K/K$, so the latter is also compact. □

Alternate description: restricted products of topological groups.

Let $G_1, G_2, \ldots$ be a sequence of locally compact topological groups and let H_i be a compact subgroup of G_i. The *restricted 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. For each set S, this product contains the subgroup G_S of tuples (g_i) such that $g_i \in H_i$ for $i \notin S$, and indeed G is the direct limit of the G_S. We make G into a topological

group by giving each G_S the product topology and saying that $U \subset G$ is open if its intersection with each G_S is open there.

In this language, the additive group of adèles over $\mathbb{Q}$ is simply the restricted product of the pairs $(\mathbb{R}, \mathbb{R})$ and $(\mathbb{Q}_p, \mathbb{Z}_p)$ for each p, and likewise over a number field.

Idèles and the idèle class group.

An *idèle* is a unit in the ring $\mathbb{A}_K$. In other words, it 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. Let I_K denote the group of idèles of K (sometimes thought of as $\mathrm{GL}_1(\mathbb{A}_K)$). This group is the restricted product of the pairs $(\mathbb{R}^*, \mathbb{R}^*)$, $(\mathbb{C}^*, \mathbb{C}^*)$, and $(K_\mathfrak{p}^*, \mathfrak{o}_\mathfrak{p}^*)$.

For example, for each element $\beta \in K$, we get an adèle in which $\alpha_v = \beta$ for all v; this adèle is an idèle if $\beta \neq 0$. We call these the *principal adèles* and *principal idèles*, and define the *idèle class group* of K as the quotient $C_K = I_K/K^*$ of the idèles by the principal idèles.

Warning. While the embedding of the idéles into the adéles is continuous, the restricted product topology on idéles does not coincide with the subspace topology for the embedding! For example, the set of idèles whose component at each finite prime $\mathfrak{p}$ is in $\mathfrak{o}_\mathfrak{p}^*$ is open, but not an intersection of the idèle group with an open subset of the adèles. See the exercises for one way to fix this, and the last part of this section for another.

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. The principal idèle corresponding to $\alpha \in K$ maps to the principal ideal generated by α. Thus we have a surjection $C_K \to \mathrm{Cl}(K)$.

Since the norm is trivial on K^*, 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 16.4. *The group C_K^0 is compact.*

This innocuous-looking fact actually implies two key theorems of algebraic number theory:

(a) The class group of K is finite.
(b) The group of units of K has rank $r + s - 1$, where r and s are the number of real and complex places, respectively. More generally, if S is a finite set of places containing the archimedean places, the group of S-units of K (elements of K which have valuation 0 at each finite place not contained in S) has rank $\#(S) - 1$.

In fact, (a) is immediate: C_K^0 is compact and it surjects onto $\mathrm{Cl}(K)$, so the latter must also be compact for the discrete topology, i.e., it must be finite. (In fact, $\mathrm{Cl}(K)$ is isomorphic to the group of connected components of C_K^0.) To see (b), let I_S be the group of idèles which are units outside S, and define the map $\log : I_S \to \mathbb{R}^{\#(S)}$ by taking log of the absolute value of the norm of each component in S. By the product formula, this maps into the sum-of-coefficients-zero hyperplane H in $\mathbb{R}^{\#(S)}$, and the

image of the group K_S^* of S-units is discrete therein. (Restricting an element of K_S^* to a bounded subset of H bounds all of its absolute values, so this follows from the discreteness of K in $\mathbb{A}_K$.) Let W be the span in H of the image of K_S^*; then we get a continuous homomorphism $C_K^0 \to H/W$ whose image generates H/W. But its image is compact; this is a contradiction unless H/W is the zero vector space. Thus K_S^* must be a lattice in H, so it has rank $\dim H = \#S - 1$.

Proof of Proposition 16.4. The inverse images of any two positive real numbers under the norm map are homeomorphic. So rather than prove that the inverse image of 0 is compact, we'll prove that the inverse image of some $\rho > 0$ is compact. Namely, we choose $\rho > c$, where c has the property that any idèle of norm $\rho > c$ is congruent modulo K^* to an idèle whose components all have norms in $[1, \rho]$. (The existence of c is left as an exercise.)

The set of idèles with each component having norm in $[1, \rho]$ 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 valuations between 1 and ρ.) This is a compact set, the set of idèles therein of norm ρ is a closed subset and so is also compact, and the latter set surjects onto C_K^0, so that's compact too. □

One more comment worth making: what are the open subgroups of I_K? In fact, for each formal product $\mathfrak{m}$ of places, one gets an open subgroup of idèles $(\alpha_v)_v$ such that:

(a) if v is a real place occurring in $\mathfrak{m}$, then $\alpha_v > 0$;
(b) if v is a finite place corresponding to the prime $\mathfrak{p}$, occurring to the power e, then $\alpha_v \equiv 1 \pmod{\mathfrak{p}^e}$.

Moreover, every open subgroup contains one of these. Thus using the surjection $C_K \mapsto \mathrm{Cl}(K)$, we get a bijection between open subgroups of C_K and generalized ideal class groups!

A presentation of $\mathbb{A}_\mathbb{Q}$. In the special case $K = \mathbb{Q}$, the idèle class group has a nice presentation. Namely, given an arbitrary idèle in $I_\mathbb{Q}$, there is a unique positive rational with the same norms at the finite places. Thus

$$I_\mathbb{Q} \cong \mathbb{R}^* \times \prod_p \mathbb{Z}_p^*.$$

This definitely does not generalize: as noted above, the idèle class group has multiple connected components when the class number is bigger than 1.

Aside: beyond class field theory. You can think of the idèle group as $\mathrm{GL}_1(\mathbb{A}_K)$. In that case, class field theory will become 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 $\mathrm{GL}_n(\mathbb{A}_K)$. In fact, with K replaced by the function field of a curve over a finite field, this prediction is a deep theorem of L. Lafforgue (based on work of Drinfeld).

Exercises.

(1) Prove Proposition 16.2.

(2) 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 $x \mapsto (x, x^{-1})$.
(3) Complete the proof of Proposition 16.4 by establishing the existence of the constant c. (Hint: see Lang, Section V.1, Theorem 0.)

CHAPTER 17

Adèles and idèles in field extensions

Reference. Neukirch, Section VI.1 and VI.2.

Adèles in Field Extensions.

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 set the w-component of the image of α to α_v. This embedding induces an inclusion $I_K \hookrightarrow I_L$ of idèle groups as well.

If L/K is Galois with Galois group G, then G acts naturally 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 of $\mathbb{A}_L$ with $\mathbb{A}_{L^g}$ and of I_L with I_{L^g}. Namely, if $(\alpha_v)_v$ is an idèle over L and $g \in G$, then g maps the completion L_v of L to a completion L_{v^g} of L^g. (Remember, a place v corresponds to an absolute value $|\cdot|_v$ on L; the absolute value $|\cdot|_{v^g}$ on L^g is given by $|a^g|_{v^g}| = |a|_v$.) As you might expect, this action is compatible with the embeddings of L in I_L and L^g in I_{L^g}, so it induces an isomorphism $C_L \to C_{L^g}$ of idèle class groups.

Aside. Neukirch points out that you can regard $\mathbb{A}_L$ as the tensor product $\mathbb{A}_K \otimes_K L$; in particular, this is a good way to see the Galois action on $\mathbb{A}_L$. Details are left to the reader.

We can define trace and norm maps as well:

$$\mathrm{Trace}_{\mathbb{A}_L/\mathbb{A}_K}(x) = \sum_g x^g, \qquad \mathrm{Norm}_{I_L/I_K}(x) = \prod_g x^g$$

where g runs over coset representatives of $\mathrm{Gal}(\overline{K}/L)$ in $\mathrm{Gal}(\overline{K}/K)$, the sum and product taking places 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 $\mathrm{Gal}(L/K)$.

In terms of components, these definitions translate as

$$(\mathrm{Trace}_{\mathbb{A}_L/\mathbb{A}_K}(\alpha))_v = \sum_{w|v} \mathrm{Trace}_{L_w/K_v}(\alpha_w)$$

$$(\mathrm{Norm}_{I_L/I_K}(\alpha))_v = \prod_{w|v} \mathrm{Norm}_{L_w/K_v}(\alpha_w).$$

The trace and norm do what you expect on principal adèles/idèles. In particular, the norm descends to a map $\mathrm{Norm}_{L/K} : C_L \to C_K$.

Aside. 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 $\mathbb{A}_K$-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 $\mathbb{A}_K$-module $\mathbb{A}_L$. (Yes, the action is on the *adèles* in both cases. Remember, idèles should be

thought of as automorphisms of the adèles, not as elements of the adèle ring, in order to topologize them correctly.)

If L/K is a Galois extension, then $\mathrm{Gal}(L/K)$ acts on $\mathbb{A}_L$ and I_L fixing $\mathbb{A}_K$ and I_K, respectively, and we have the following.

PROPOSITION 17.1. *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 nice consequence for the idèle class group, a fact which is quite definitely not true for the ideal class group: the map $\mathrm{Cl}_K \to \mathrm{Cl}_L^G$ is neither injective nor surjective in general. 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.

PROPOSITION 17.2 (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 2.2). So we again have a short exact sequence, and $C_L^G \cong I_K/K^* = C_K$. □

CHAPTER 18

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 18.1 (Adelic reciprocity law). *There is a canonical map $r_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ which induces, for each finite extension L/K of number fields, an isomorphism $r_{L/K} : C_K/\operatorname{Norm}_{L/K} C_L \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$.*

THEOREM 18.2 (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 $H = \operatorname{Norm}_{L/K} C_L$.*

In fact, using local class field theory, we can construct the map that will end up being r_K. For starters, let L/K be a finite abelian extension 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, $G_v \cong \mathrm{Gal}(L_w/K_v)$, so we can view the local reciprocity map $K_v^* \to \mathrm{Gal}(L_w/K_v)$ as a map $r_{K,v} : K_v^* \to G$. That is, if v is a finite place. If $v = \mathbb{C}$, then $\mathrm{Gal}(L_w/K_v)$ is trivial, so we just take $K_v^* \to G$ to be the identity map. If $v = \mathbb{R}$, then we take $K_v^* = \mathbb{R}^* \to \mathrm{Gal}(L_w/K_v) = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ to be the map sending everything positive to the identity, and everything negative to complex conjugation.

Now note that

$$(\alpha_v) \mapsto \prod_v r_{K,v}(\alpha_v)$$

is well-defined on idèles: for (α_v) an idèle, α_v is a unit for almost all v and L_w/K_v is unramified for almost all v. For the (almost all) v in both categories, $r_{K,v}$ maps α_v to the identity.

The subtle part is the following. As noted below, before proving reciprocity, we'll only be able to check this for the map obtained from $r_{K,v}$ by projecting from $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ to the torsion-free quotient of $\mathrm{Gal}(K(\zeta_\infty)/K)$, the Galois group of the

maximal cyclotomic extension; in that case, we can reduce to $K = \mathbb{Q}$ and do an explicit computation. The general case will actually only follow after the fact from the construction of global reciprocity!

PROPOSITION 18.3. *The map $r_{K,v}$ is trivial on K^*.*

Thus it induces a map $r_K : C_K \to \mathrm{Gal}(L/K)$ for each L/K abelian, and in fact to $r_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ using the analogous compatibility for local reciprocity.

Since each of the local reciprocity maps is continuous, so is the map r_K. That means the kernel of $r_K : C_K \to \mathrm{Gal}(L/K)$, for L/K abelian, is an open subgroup of C_K. Now recall that the quotient of C_K by any open subgroup of finite index is a generalized ideal class group. Thus r_K is giving us a canonical isomorphism between $\mathrm{Gal}(L/K)$ and a generalized ideal class group; could this be anything but Artin reciprocity itself?

Indeed, let U be the kernel of r_K, let $\mathfrak{m}$ be a conductor for the generalized ideal class group C_K/U, and let $\mathfrak{p}$ be a prime of K not dividing $\mathfrak{m}$ and unramified in L. Then the idèle $\alpha = (1, 1, \dots, \pi, \dots)$ with a uniformizer π of $\mathfrak{o}_{K_\mathfrak{p}}$ in the $\mathfrak{p}$ component and ones 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.

In fact, we discover from this a little bit more than we knew already about the Artin map. All we said before about the Artin map is that it factors through a generalized ideal class group, and that the conductor $\mathfrak{m}$ of that group is divisible precisely by the ramified primes (which we see from local reciprocity). In fact, we can now say *exactly* what is in 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.

What needs to be done.

Many of these steps will be analogous to the steps in local class field theory.

- It would be natural to start by verifying that the map r_K given above does indeed kill principal idèles, but this is too hard to do all at once (except for cyclotomic extensions, for which the explicit calculation is easy and an important input into the machine). Instead, we postpone this step all the way until the end; see below.
- Verify that for L/K cyclic, the Herbrand quotient of C_L as a $\mathrm{Gal}(L/K)$-module is $[L : K]$. In particular, that forces $\#H^0(\mathrm{Gal}(L/K), C_L) \geq [L : K]$ (the "First Inequality").
- For L/K cyclic, determine that

  $$\#H^0(\mathrm{Gal}(L/K), C_L) = [L : K], \qquad \#H^1(\mathrm{Gal}(L/K), C_L) = 1$$

  (the "Second Inequality"). This step is trivial in local CFT by Theorem 90, but is actually pretty subtle in the global case. We'll do it by reducing to the case where K contains enough roots of unity, so that L/K becomes a Kummer extension and we can compute everything explicitly. There is also an analytic proof given in Milne which I'll very briefly allude to.
- Check the conditions for abstract class field theory, using the setup described at the end of Chapter 15. In particular, the role of the unramified

extensions in local class field theory will be played by certain cyclotomic extensions. This gives an "abstract" reciprocity map, not yet known to be related to Artin reciprocity.

- Prove the existence theorem, by showing that every open subgroup of C_K contains a norm group. Again, we can enlarge K in order to do this, so we can get into the realm of Kummer theory.
- Use the compatibility between the proofs of local and global class field theory to see that the "abstract" global reciprocity map restricts to the usual reciprocity map from local class field theory. This will finally imply that the abstract map coincides with the adelic Artin reciprocity map, and therefore yield the adelic reciprocity map. It is only at this point that we will deduce that the reciprocity map r_K that we tried to define at the outset actually does kill principal idèles!
- We will also briefly sketch the approach taken in Milne, 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 12.6), one gets a reciprocity map from $H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathrm{Gal}(L/K)^{\mathrm{ab}}$ to $H_T^0(\mathrm{Gal}(L/K), C_K/\operatorname{Norm}_{L/K} C_L)$, which again can be reconciled with local reciprocity to get the Artin reciprocity map.

Part 6

The main results

CHAPTER 19

Cohomology of the idèles I: the "First Inequality"

Reference. Milne VII.2-VII.4; Neukirch VI.3; but see below about Neukirch.

By analogy with local class field theory, we want to prove that for K, L number fields and C_K, C_L their idèle class groups,

$$H^1(\mathrm{Gal}(L/K), C_L) = 1, \qquad H^2(\mathrm{Gal}(L/K), C_L) = \mathbb{Z}/[L:K]\mathbb{Z}.$$

In this chapter, we'll look at the special case L/K cyclic, and prove that

$$\#H^0_T(\mathrm{Gal}(L/K), C_L)/\#H^1_T(\mathrm{Gal}(L/K), C_L) = [L:K].$$

That is, the Herbrand quotient of C_L is $[L:K]$. As we'll see, this will end up reducing to looking at units in a real vector space, much as in the proof of Dirichlet's units theorem.

This will imply the "First Inequality".

THEOREM 19.1. *For L/K a cyclic extension of number fields,*

$$\#H^0_T(\mathrm{Gal}(L/K), C_L) \geq [L:K].$$

The "Second Inequality" will be the reverse, which will be a bit more subtle (see Theorem 20.1).

Some basic observations. But first, some general observations. Put $G = \mathrm{Gal}(L/K)$.

PROPOSITION 19.2. *For each $i > 0$, $H^i(G, I_L) = \oplus_v H^i(G_v, L_v^*)$. For each i, $H^i_T(G, I_L) = \oplus_v H^i_T(G_v, L_v^*)$.*

PROOF. For any finite set S of places of K containing all infinite places and all ramified primes, let $I_{L,S}$ be the set of idèles with a unit at each component other than at the places dividing any places in S. Note that $I_{L,S}$ is stable under G (because we defined it in terms of places of K, not L). By definition, I_L is the direct limit of the $I_{L,S}$ over all S, so $H^i(G, I_L)$ 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 9.1), $H^i(G, \prod_{w|v} L_w^*) = H^i(G_v, L_w^*)$, so we have what we want. The argument for Tate groups is analogous. □

Notice what this says for $i = 0$ on the Tate groups: an idèle is a norm if and only if each component is a norm. Obvious, perhaps, but useful.

In particular,

$$H^1(G, I_L) = 0, \qquad H^2(G, I_L) = \bigoplus_v \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}.$$

One other observation: if S contains all infinite places and all ramified places, then

$$\operatorname{Norm}_{L/K} I_{L,S} = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_{K_v}^*$$

where U_v is open in K_v^*. The group on the right is open in I_K, so $\operatorname{Norm}_{L/K} I_K$ is open.

By quotienting down to C_K, we see that $\operatorname{Norm}_{L/K} C_K$ is open. In fact, the snake lemma on the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^* & \longrightarrow & I_L & \longrightarrow & C_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \operatorname{Norm}_{L/K}} & & \downarrow{\scriptstyle \operatorname{Norm}_{L/K}} & & \downarrow{\scriptstyle \operatorname{Norm}_{L/K}} & & \\ 0 & \longrightarrow & K^* & \longrightarrow & I_K & \longrightarrow & C_K & \longrightarrow & 0 \end{array}$$

implies that the quotient $I_K/(K^* \times \operatorname{Norm}_{L/K} I_L)$ is isomorphic to C_K.

Cohomology of the units.

Remember, we're going to be assuming $G = \operatorname{Gal}(L/K)$ is cyclic until further notice, so that we may use periodicity of the Tate groups, and the Herbrand quotient.

First of all, working with I_L all at once is a bit unwieldy; we'd rather work with $I_{L,S}$ for some finite set S. In fact, we can choose S to make our lives easier: we choose S containing all infinite places, and all ramified primes, and perhaps some extra primes so that

$$I_L = I_{L,S} L^*.$$

This is possible because the ideal class group of L is finite, so it is generated by some finite set of primes, which we introduce into S; then I can move a generator of any other prime to some stuff in S times units. (This argument can also be used to prove that C_L^0 is compact, but then one doesn't recover the finiteness of the ideal class group as a corollary.)

Put $L_S = L^* \cap I_{L,S}$; that is, L_S is the group of S-units in L. From the exact sequence

$$1 \to L_S \to I_{L,S} \to I_{L,S}/L_S = C_L \to 1$$

we have, in case L/K is cyclic, an equality of Herbrand quotients

$$h(C_L) = h(I_{L,S})/h(L_S).$$

From the computation of $H^i(G, I_{L,S})$, it's easy to read off its Herbrand quotient:

$$h(I_{L,S}) = \prod_{v \in S} \# H_T^0(G_v, L_w^*) = \prod_{v \in S} [L_w : K_v].$$

So to get $h(C_L) = [L : K]$, we need

$$h(L_S) = \frac{1}{[L:K]} \prod_{v \in S} [L_w : K_v].$$

This will in fact be true even if we only assume S contains all infinite places, as we now check.

Let T be the set of places of L dividing the 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 $L_S \to V$ by

sending

$$\alpha \to \prod_w \log |\alpha|_w,$$

with the caveat that the norm at a complex place is the *square* of the usual absolute value; the kernel of this map consists solely of roots of unity (by Kronecker's theorem: any algebraic integer whose conjugates in $\mathbb{C}$ all have norm 1 is a root of unity). Let M be the quotient of L_S by the group of roots of unity; since the latter is finite, $h(M) = h(L_S)$. Let $H \subset V$ be the hyperplane of vectors with sum of coordinates 0; by the product formula, M maps into H. As noted earlier, in fact M is a discrete subgroup of H of rank equal to the dimension of H; that is, M is a lattice in H. Moreover, we have an action of G on V compatible with the embedding of M; namely, G acts on the places in T, so acts on V by permuting the coordinates.

Caveat. There seems to be an error in Neukirch's derivation at this point. Namely, his Lemma VI.3.4 is only proved assuming that G acts transitively on the coordinates of V; but in the above situation, 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 Milne instead.

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 above some v form a copy of $\mathrm{Ind}_{G_v}^G \mathbb{Z}$. Thus

$$h(G, M') = \prod_v h(G, \mathrm{Ind}_{G_v}^G \mathbb{Z}) = \prod_v h(G_v, \mathbb{Z}) = \prod_v \#G_v = \prod_v [L_w : K_v].$$

So all that remains is to prove the following.

LEMMA 19.3. *Let V be a real vector space on which a finite group G acts linearly, and let L_1 and L_2 be G-stable lattices in V for which $h(L_1)$ and $h(L_2)$ are both defined. Then $h(L_1) = h(L_2)$.*

In fact, one can show that if one of the Herbrand quotients is defined, so is the other.

PROOF. We first show that $L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as $\mathbb{Q}[G]$-modules. We are given that $L_1 \otimes_{\mathbb{Z}} \mathbb{R}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{R}$ are isomorphic as $\mathbb{R}[G]$-modules. That is, the real vector space $W = \mathrm{Hom}_{\mathbb{R}}(L_1 \otimes_{\mathbb{Z}} \mathbb{R}, L_2 \otimes_{\mathbb{Z}} \mathbb{R})$, 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 can also be written as

$$\mathrm{Hom}_{\mathbb{Z}}(L_1, L_2) \otimes_{\mathbb{Z}} \mathbb{R};$$

that is, $\mathrm{Hom}_{\mathbb{Z}}(L_1, L_2)$ sits inside as a sublattice. The fact that W has an invariant vector says that a certain set of linear equations has a nonzero solution over $\mathbb{R}$, namely the equations that express the fact that the action of G leaves the vector invariant. But those equations have coefficients in $\mathbb{Q}$, so there must already be invariant vectors over $\mathbb{Q}$. Moreover, if we fix an isomorphism (not G-equivariant) between $L_2 \otimes_{\mathbb{Z}} \mathbb{R}$ and $L_1 \otimes_{\mathbb{Z}} \mathbb{R}$, we can compose this with any element of W to

get a map from L_1 to itself, which has a determinant; and by hypothesis, there is some invariant vector of W whose determinant is nonzero. Thus the determinant doesn't vanish identically on the set of invariant vectors in W, so it also doesn't vanish identically on the set of invariant vectors in $\mathrm{Hom}_{\mathbb{Z}}(L_1, L_2) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Thus there is a G-equivariant isomorphism between $L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$; that is, L_1 is isomorphic to a 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 $h(L_1) = h(L_2)$. □

Aside: splitting of primes.

As a consequence of the First Inequality, we record the following fact which is *a posteriori* an immediate consequence of the adelic reciprocity law, but which will be needed in the course of the proofs. (See Neukirch, Corollary VI.3.8 for more details).

COROLLARY 19.4. *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 of prime order. Then if all but finitely many primes split completely, we can put the remaining primes into S and deduce that $C_K = \mathrm{Norm}_{L/K} C_L$, whereas the above calculation forces $H^0_T(\mathrm{Gal}(L/K), C_L) \geq [L : K]$, 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 of prime order; 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. □

CHAPTER 20

Cohomology of the idèles II: the "Second Inequality"

Reference. Milne VII.5; Neukirch VI.4.

In the previous chapter, 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 $[L : K]$. This time we'll prove the following.

THEOREM 20.1. *Let L/K be a Galois extension of number fields, with Galois group G. Then:*

(a) *the group $I_K/(K^* \operatorname{Norm}_{L/K} I_L)$ is finite of order at most $[L : K]$;*
(b) *the group $H^1(G, C_L)$ is trivial;*
(c) *the group $H^2(G, C_L)$ is finite of order at most $[L : K]$.*

By the first inequality, for L/K cyclic, these three are equivalent and all imply that $H^2(G, C_L)$ has order exactly $[L : K]$. That would suffice to prove the class field axiom in Neukirch's abstract class field theory.

There are two basic ways to prove this result: an analytic proof and an algebraic proof. Although the analytic proof is somewhat afield of what we have been doing (it requires some properties of zeta functions that we haven't discussed previously), it's somewhat simpler overall than the algebraic proof. So we'll sketch it first before proceeding to the algebraic proof.

The analytic proof.

For the analytic proof, we need to recast the Second Inequality back into classical, ideal-theoretic language. Let L/K be a finite Galois extension and $\mathfrak{m}$ a formal product of places of K. Back when we defined generalized ideal class groups, we defined the group $I_{\mathfrak{m}}$ of fractional ideals of K coprime to $\mathfrak{m}$ and $P_{\mathfrak{m}}$ the group of principal ideals admitting a generator α such that $\alpha \equiv 1 \pmod{\mathfrak{p}^e}$ if the prime power $\mathfrak{p}^e$ occurs in $\mathfrak{m}$ for a finite prime $\mathfrak{p}$, and $\tau(\alpha) > 0$ if τ is the real embedding corresponding to a real place in $\mathfrak{m}$. Also, let $J_{\mathfrak{m}}$ be the group of fractional ideals of L coprime to $\mathfrak{m}$. Then the Second Inequality states that

$$\#I_{\mathfrak{m}}/P_{\mathfrak{m}} \operatorname{Norm}_{L/K} J_{\mathfrak{m}} \leq [L : K].$$

Note that we don't have to assume $\mathfrak{m}$ is divisible by the ramified primes of L/K.

We'll need the following special case of the Chebotarev density theorem, which fortunately we can prove without already having all of class field theory.

PROPOSITION 20.2. *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 $1/[M : K]$.*

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; each such prime lies over an unramified prime $\mathfrak{p}$ of K of absolute degree 1 which splits completely in L.

Now recall how the Dirichlet density works: the set T having Dirichlet density 1 means that

$$\sum_{\mathfrak{q}\in T} \frac{1}{\mathrm{Norm}(\mathfrak{q})^s} \sim \frac{1}{s-1} \qquad s \searrow 1$$

(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

$$[L:K] \sum_{\mathfrak{p}\in T} \frac{1}{\mathrm{Norm}(\mathfrak{p})^s} \sim \frac{1}{s-1}.$$

That is, the Dirichlet density of S is $1/[L:K]$. □

Now for the inequality. For $\chi : I_{\mathfrak{m}}/P_{\mathfrak{m}} \to \mathbb{C}^*$ a character, we defined the L-function

$$L(s,\chi) = \prod_{\mathfrak{p}\not| \mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}}.$$

We'll use some basic properties of this function which can be found in any standard algebraic number theory text. For starters,

$$\log L(s,1) \sim \log \zeta_K(s) \sim \log \frac{1}{s-1} \qquad s \searrow 1,$$

while if χ is not the trivial character, $L(s,\chi)$ 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

$$\log L(s,\chi) \sim m(\chi) \log(s-1) = -m(\chi) \log \frac{1}{s-1}.$$

Let H be a subgroup of $I_{\mathfrak{m}}$ containing $P_{\mathfrak{m}}$. By finite Fourier analysis, or orthogonality of characters,

$$\sum_{\chi: I_{\mathfrak{m}}/H \to \mathbb{C}^*} \log L(s,\chi) \sim \#(I_{\mathfrak{m}}/H) \sum_{\mathfrak{p}\in H} \frac{1}{\mathrm{Norm}(\mathfrak{p})^{-s}}.$$

We conclude that the set of primes in H has Dirichlet density

$$\frac{1 - \sum_{\chi\neq 1} m(\chi)}{\#(I_{\mathfrak{m}}/H)};$$

this is $1/\#(I_{\mathfrak{m}}/H)$ if the $m(\chi)$ are all zero, and 0 otherwise.

We apply this with $H = P_{\mathfrak{m}} \,\mathrm{Norm}_{L/K}\, J_{\mathfrak{m}}$. This in particular includes every prime of K that splits completely, since such a prime is the norm of any prime of L lying over it. Thus the set of primes in H has Dirichlet density, on one hand, is at least $1/[L:K]$. On the other hand, this set has density either zero or $1/\#(I_{\mathfrak{m}}/H)$. We conclude $\#I_{\mathfrak{m}}/H \leq [L:K]$, as desired.

The algebraic proof.

We now proceed to the algebraic proof of the Second Inequality. To prove the theorem in general, we can very quickly reduce to the case of L/K not just cyclic, but cyclic of prime order. The reductions are similar to those we used to compute

$H^2(L^*)$ in the local case. First of all, if we have the theorem for all solvable groups, then if G is general and H is a Sylow p-subgroup of G, then for any G-module M,

$$\text{Res} : H^i_T(G, M) \to H^i_T(H, M)$$

is injective on p-primary components (because $\text{Cor} \circ \text{Res}$ is multiplication by $[G : H]$), so we can deduce the desired result. Thus it suffices to consider L/K solvable. In that case, starting from the cyclic-of-prime-order case we can induct using the inflation-restriction exact sequence (Corollary 13.8): if K'/K is a subextension and $H = \text{Gal}(L/K')$, then for $i = 1, 2$,

$$0 \to H^i(G/H, C_{K'}) \to H^i(G, C_L) \to H^i(H, C_L)$$

(using the fact that $H^1(H, C_L) = 0$ by the induction hypothesis). Upshot: we need only consider L/K cyclic of prime order p.

One more reduction to make things simpler: we reduce to the case where K contains a p-th root of unity. 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. To complete the reduction, it suffices to check that the homomorphism

$$H^0_T(\text{Gal}(L/K), C_L) \to H^0_T(\text{Gal}(L'/K'), C_{L'})$$

induced by the inclusion $C_L \to C_{L'}$ is injective. These groups are both killed by multiplication by p, since for $x \in C_K$, $\text{Norm}_{L/K}(x) = x^p$. Thus multiplication by $d = [K' : K]$, which divides $p - 1$, is an isomorphism on these groups. If $x \in C_K$ maps to the identity in $H^0_T(\text{Gal}(L'/K'), C_{L'})$, we can choose a representative of the same class as x in $H^0_T(\text{Gal}(L/K), C_L)$ of the form y^d; then y also maps to the identity in $H^0_T(\text{Gal}(L'/K'), C_{L'})$. That is, $y = \text{Norm}_{L'/K'}(z')$ for some $z' \in C_{L'}$, and

$$y^d = \text{Norm}_{K'/K}(y) = \text{Norm}_{L'/K}(z') \in \text{Norm}_{L/K} C_L.$$

Thus $x \in \text{Norm}_{L/K} C_L$, so the homomorphism is injective.

The key case.

To sum up: it suffices to prove the theorem for K containing a p-th root of unity ζ_p and L/K cyclic of order p. We now address this case.

As in the proof of the First Inequality, we will use a set S of places of K containing the infinite places, the primes that ramify in L, and enough additional primes so that $I_K = I_{K,S}K^*$; we also include all places above (p). Again, we put $K_S = I_{K,S} \cap K^*$. Also we write $s = \#S$.

The plan is to explicitly produce a subgroup of C_K of index $[L : K]$ consisting of norms from C_L. We do this by using an auxiliary set of places T disjoint from S. For such T, we define

$$J = \prod_{v \in S} (K^*_v)^p \times \prod_{v \in T} K^*_v \times \prod_{v \notin S \cup T} \mathfrak{o}^*_{K_v}.$$

Let $\Delta = (L^*)^p \cap K_S$. We will show that:

(a) $L = K(\Delta^{1/p})$;
(b) we can choose a set T of $s - 1$ primes such that Δ is the kernel of the map $K_S \to \prod_{v \in T} K^*_v/(K^*_v)^p$;
(c) for such a set T, if we put $C_{K,S,T} = JK^*/K^*$, then

$$\#C_K/C_{K,S,T} = [L : K] = p;$$

(d) with the same notation, $C_{K,S,T} \subseteq \operatorname{Norm}_{L/K} C_L$.

That will imply $\#C_K / \operatorname{Norm}_{L/K} C_L \leq p$, as desired.

We first concentrate on (a). By Kummer theory, since K contains a primitive p-th root of unity, we can write $L = K(D^{1/p})$ for $D = (L^*)^p \cap K^*$. Thus $K(\Delta^{1/p}) \subseteq L$ and since there is no room between K and L for an intermediate extension ($[L : K]$ being prime), all that we have to check is that $K(\Delta^{1/p}) \neq K$. Choose a single $x \in D$ such that $L = K(x^{1/p})$. For each $v \notin S$, the extension $K_v(x^{1/p})/K_v$ is unramified, so we can write x as a unit times a p-th power, say $x = u_v y_v^p$. If we put $y_v = 1$ for $v \in S$, we can assemble the y_v into an idèle y, which by $I_K = K^* I_{K,S}$ we can rewrite as zw for $z \in K^*$ and $w \in I_{K,S}$. Now for $v \notin S$, $(x/z^p)_v = u_v / w_v^p \in \mathfrak{o}_{K_v}^*$. Thus $x/z^p \in (L^*)^p \cap K_S \in \Delta$ but $x \notin (K^*)^p$. We conclude $L = K(\Delta^{1/p})$.

Now we move to (b). Put $N = K(K_S^{1/p})$. By Kummer theory,

$$\operatorname{Gal}(N/K) \cong \operatorname{Hom}(K_S/K_S^p, \mathbb{Z}/p\mathbb{Z}).$$

By the generalization of Dirichlet's units theorem to S-units, K_S modulo torsion is a free abelian group of rank $s - 1$, and the torsion subgroup consists of roots of unity, so is cyclic of order divisible by p. Thus $K_S/K_S^p \cong (\mathbb{Z}/p\mathbb{Z})^s$. Choose generators $g_1, \ldots, g_{s-1}$ of $\operatorname{Gal}(N/L)$; these correspond in $\operatorname{Hom}(K_S/K_S^p, \mathbb{Z}/p\mathbb{Z})$ to a set of homomorphisms whose common kernel is precisely Δ/K_S^p.

So to establish (b), we 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 $K_S \to K_{v_i}^*/(K_{v_i}^*)^p$. Let N_i be the fixed field of g_i; by the First Inequality (see Corollary 19.4), 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 (a/k/a 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 $L = \cap N_i$ is the maximal subextension of N in which all of the v_i split completely. We conclude that for $x \in K_S$, 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 $K_S \to \prod_i K_{v_i}^*/(K_{v_i}^*)^p$. In fact, under this map, K_S actually maps to the units in $K_{v_i}^*$ for each i. This proves (b).

Next, we verify (c), using the following lemma.

LEMMA 20.3. *$J \cap K^* = (K_{S \cup T})^p$.*

PROOF. Clearly $K_{S\cup T}^p \subseteq J \cap K^*$; we have to work to show the other inclusion. Take $y \in J \cap K^*$ and $M = K(y^{1/p})$. We'll show that $\operatorname{Norm}_{M/K} C_M = C_K$; by the First Inequality, this will imply $M = K$, so $y \in (K^*)^p \cap J = (K_{S\cup T})^p$.

Since $I_K = I_{K,S} K^*$, it is enough to choose $\alpha \in I_{K,S}$ and show that $\alpha/x \in \operatorname{Norm}_{M/K} I_M$ for some $x \in K^*$. As noted above, the map

$$K_S \to \prod_{v \in T} \mathfrak{o}_{K_v}^* / (\mathfrak{o}_{K_v}^*)^p$$

is surjective, and $\#K_S/\Delta = p^{s-1}$. That's also the order of the product, so the map is actually an isomorphism. Thus we can find $x \in K_S$ so that α/x has component

the p-th power of a unit of K_v at each $v \in T$. In particular, such a component is the norm of its p-th root, so α/x is a norm at each $v \in T$. For $v \in S$, we don't have anything to check: because y is a p-th power at v, $M_w = K_v$. Finally, for $v \notin S \cup T$, M_w/K_v is unramified, so any unit is a norm. Thus α/x is indeed a norm. We conclude $\operatorname{Norm}_{M/K} C_M = C_K$, so $M = K$ and $y \in K^p_{S\cup T}$, as desired. □

Given the lemma, we now have an exact sequence

$$1 \to (I_{K,S\cup T} \cap K^*)/(J \cap K^*) \to I_{K,S\cup T}/J \to I_{K,S\cup T}K^*/JK^* \to 1.$$

We can rewrite $I_{K,S\cup T}K^*$ as simply I_K, so the group on the right is precisely $C_K/C_{K,S,T}$. By the lemma, the group on the left is $K^*_{S\cup T}/(K^*_{S\cup T})^n$, which has order p^{2s-1} because $K_{S\cup T}$ is free of rank $2s-2$ plus a cyclic group of order a multiple of p. The group in the middle is the product of $K_v^*/(K_v^*)^p$ over all $v \in S$, and each of those has order p^2 (generated by ζ_p and a uniformizer of K_v). Adding it all up, we get $\#C_K/C_{K,S,T} = p$, proving (c).

Finally, to check (d), it suffices to check that $J \subseteq \operatorname{Norm}_{L/K} I_L$, which we may check component by component. It's automatic for the places $v \notin S \cup T$, since those places are unramified, so every unit is a norm. For places $v \in S$, any element of $(K_v^*)^p$ is a norm from $K_v(K_v^{1/p})$ by local reciprocity, so also from L_w. Finally, for places $v \in T$, from the construction of T, we see that $\Delta \subseteq (K_v^*)^p$, so $L_w = K_v$, and so K_v^* consists entirely of norms.

Aside. We get from this calculation that $H_T^{-1}(G, C_L) = 1$, so $H_T^0(G, L^*) \to H_T^0(G, C_L)$ is injective. That is,

$$K^*/\operatorname{Norm}_{L/K} L^* \to \bigoplus_v K_v^*/\operatorname{Norm}_{L_w/K_v} L_w^*$$

is injective. In other words, we have an interesting "local-to-global" statement, namely Hasse's Norm Theorem: if L/K is cyclic, $x \in K^*$ is a norm if and only if it is locally a norm.

CHAPTER 21

An "abstract" reciprocity map

Reference. Milne VII.5; Neukirch VI.4, but only loosely.

In this chapter, we'll manufacture a canonical isomorphism $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to C_K/\operatorname{Norm}_{L/K} C_L$ for any finite extension L/K of number fields, where C_K and C_L are the corresponding idèle class groups. However, we won't yet know it agrees with our proposed reciprocity map, which is the product of the local reciprocity maps. We'll check that in the next chapter.

Cyclotomic extensions.

The cyclotomic extensions (extensions by roots of unity) 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.

First of all, we should further articulate a distinction that has come up already. The extension $\cup_n \mathbb{Q}(\zeta_n)$ 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 $\prod_p \mathbb{Z}_p = \widehat{\mathbb{Z}}$. 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.

The reciprocity map via abstract CFT.

First of all, we 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. That gives a continuous surjection

$$d : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}};$$

if we regard $\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q}$ as the "maximal unramified extension" of $\mathbb{Q}$, we can define the ramification index $e_{L/K}$ and inertia degree $f_{L/K}$ for any extension of number fields, by the rules

$$f_{L/K} = [L \cap \mathbb{Q}^{\mathrm{smcy}} : K \cap \mathbb{Q}^{\mathrm{smcy}}], \qquad e_{L/K} = \frac{[L:K]}{f_{L/K}}.$$

To use abstract class field theory to exhibit the reciprocity map, we need a "henselian valuation" $v : C_{\mathbb{Q}} \to \widehat{\mathbb{Z}}$, i.e., a homomorphism satisfying:

(i) $v(C_{\mathbb{Q}})$ 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;
(ii) $v(\operatorname{Norm}_{K/\mathbb{Q}} C_K) = f_{K/\mathbb{Q}} Z$ for all finite extensions $K/\mathbb{Q}$.

Once we have that, our calculations from the preceding chapters (Theorem 19.1, Theorem 20.1) imply that the class field axiom is satisfied: for L/K cyclic,

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

So then abstract class field theory will kick in.

We can make that valuation using Artin reciprocity for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Recall that there is a canonical surjection

$$I_n \to (\mathbb{Z}/n\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) :$$

for p not dividing n, the ideal (p) goes to $p \in (\mathbb{Z}/n\mathbb{Z})^*$ and then to the automorphism $\zeta_n \mapsto \zeta_n^p$, which indeed does act as the p-th power map modulo any prime of $\mathbb{Q}(\zeta_n)$ above p.

That induces a homomorphism $I_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^*$ as follows: given an idèle α, pick $x \in \mathbb{Q}^*$ so that $\alpha_{\mathbb{R}}/x > 0$ and, for each prime p with $p^e | n$, α/x has p-component congruent to 1 modulo p^e. Then map α/x to $(\mathbb{Z}/n\mathbb{Z})^*$ as follows:

$$\alpha/x \mapsto \prod_{\ell | n} \ell^{v_\ell(\alpha_\ell/x)}.$$

This gives a well-defined map: if y is an alternate choice for x, then $x/y \equiv 1 \pmod{n}$ and $x/y > 0$, so the product on the right side is precisely x/y itself, and so is congruent to 1 in $(\mathbb{Z}/n\mathbb{Z})^*$.

We now have maps $I_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^*$ which are easily seen to be compatible, so by taking inverse limits we get $I_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^* \cong \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$. We define v by channeling this map through the projection $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q})$ and then using our chosen isomorphism $\mathrm{Gal}(\mathbb{Q}^{\mathrm{smcy}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}$.

Another way to say this: $I_{\mathbb{Q}}$ can be written as $\mathbb{Q}^* \times \mathbb{R}^* \times \widehat{\mathbb{Z}}^*$, and the map to $\widehat{\mathbb{Z}}^*$ is just projection onto the third factor! In particular, the map factors through $C_{\mathbb{Q}}$, and property (i) above is straightforward.

To check (ii), we need to do the same thing that we just did a bit more generally. For K now a number field, define the map

$$I_n \to (\mathbb{Z}/n\mathbb{Z})^* \supseteq \mathrm{Gal}(K(\zeta_n)/K),$$

where now I_n is the group of fractional ideals of K coprime to (n), by sending a prime $\mathfrak{p}$ first to its absolute norm. We then have to check that the result is always in the image of $\mathrm{Gal}(K(\zeta_n)/K)$, but in fact it must be: whatever the Frobenius of $\mathfrak{p}$ is, it sends ζ_n to a power of ζ_n congruent to $\zeta_n^{\mathrm{Norm}(\mathfrak{p})}$ modulo $\mathfrak{p}$. Since $\mathfrak{p}$ is prime to n, it's prime to the difference between any two powers of ζ_n, so the Frobenius of $\mathfrak{p}$ must in fact send ζ_n to $\zeta_n^{\mathrm{Norm}(\mathfrak{p})}$. This tells us first that the map above sends I_n to $\mathrm{Gal}(K(\zeta_n)/K)$ and second that it coincides with the Artin map.

From the First Inequality, we can deduce the following handy fact.

PROPOSITION 21.1. *For L/K a finite abelian extension of number fields, the Artin map always surjects onto* $\mathrm{Gal}(L/K)$.

PROOF. If the Artin map only hit the subgroup H of $\mathrm{Gal}(L/K)$, the fixed field M of H would have the property that all but finitely many primes of M split completely in L. We've already seen that this contradicts the First Inequality (Corollary 19.4). □

In particular, the Artin map $I_n \to \mathrm{Gal}(K(\zeta_n)/K)$ we wrote down above is surjective. Using that, we can verify (ii): given a prime ideal $\mathfrak{p}$ of K, the Artin map of $K(\zeta_n)/K$ applied to it gives the same element of $(\mathbb{Z}/n\mathbb{Z})^*$ as the Artin map of $\mathbb{Q}$ applied to $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})$. Meanwhile, the Artin map of $K(\zeta_n)/K$ surjects onto $\mathrm{Gal}(K(\zeta_n)/K)$, which has index $[K \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]$ in $(\mathbb{Z}/n\mathbb{Z})^*$. This verifies (ii).

Thus lo and behold, we get from abstract class field theory a reciprocity isomorphism for any finite extension of number fields:

$$r'_{L/K} : C_K / \operatorname{Norm}_{L/K} C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

These are compatible in the usual way, so we get a map $r'_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Of course, we don't know what this map is, so we can't yet use it to recover Artin reciprocity. (That depended on the reciprocity map being the product of the local maps.) But at least we deduce the norm limitation theorem.

THEOREM 21.2. *If L/K is a finite extension of number fields and $M = L \cap K^{\mathrm{ab}}$, then $\operatorname{Norm}_{L/K} C_L = \operatorname{Norm}_{M/K} C_M$.*

We do know one thing about the map $r'_{L/K}$: for "unramified" extensions L/K (i.e., $L \subseteq K^{\mathrm{smcy}}$), the "Frobenius" in $\mathrm{Gal}(L/K)$ maps to a "uniformizer" in C_K. That is, the element of $\mathrm{Gal}(L/K)$ coming from the element of $\mathrm{Gal}(K^{\mathrm{smcy}}/K)$ which maps to 1 under d_K is the element of C_K which maps to 1 under v_K. But we made v_K simply by mapping C_K to $\mathrm{Gal}(K^{\mathrm{smcy}}/K)$ via the Artin map and then identifying the latter with $\widehat{\mathbb{Z}}$ by the same identification we used to make d_K. Upshot: the choice of that identification drops out, and the reciprocity map coincides with the Artin map that we wrote down earlier.

A bit later (see Chapter 23), we will check that $r'_{L/K}$ agrees with the map that I called $r_{L/K}$, namely the product of the local reciprocity maps. Remember, I need this in order to recover Artin reciprocity in general.

CHAPTER 22

The existence theorem

Reference. Milne VII.9, Neukirch VI.6.

With the "abstract" reciprocity theorem in hand, we now prove the Existence Theorem, that every generalized ideal class group of a number field is identified by Artin reciprocity with the Galois group of a suitable abelian extension. Recall that the idelic formulation of this statement is as follows (see Theorem 18.2).

THEOREM 22.1. *For K a number field, the finite abelian extensions L/K correspond one-to-one with the open subgroups of C_K of finite index, via the map $L \mapsto \mathrm{Norm}_{L/K} C_L$.*

The proof of this result is very similar to the proof we gave in the local case. For example, the reciprocity law immediately lets us reduce to the following proposition.

PROPOSITION 22.2. *Every open subgroup U of C_K of finite index contains $\mathrm{Norm}_{L/K} C_L$ for some finite extension L of K.*

The proof of this proposition again uses Kummer theory, but more in the spirit of the algebraic proof of the Second Inequality.

PROOF. We first prove this proposition in case U has prime index p. 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 set S of places of K containing the infinite places and all places dividing (p), which we may choose large enough so that $I_{K,S} K^* = I_K$. Let $K_S = K^* \cap I_{K,S}$ be the group of S-units of K.

The group J must also contain I_K^p, so in particular contains

$$W_S = \prod_{v \in S} (K_v^*)^p \times \prod_{v \notin S} U_v.$$

Put $C_S = W_S K^*/K^*$; then $C_S \subseteq U$, so it suffices to show that C_S contains a norm subgroup.

If K contains a primitive p-th root of unity, then an argument as in the algebraic proof of the Second Inequality gives $C_S = \mathrm{Norm}_{L/K} C_L$ for $L = K(K_S^{1/p})$. Namely, one first computes that $\#C_K/C_S = p^{\#S} = [L : K]$ as in that proof, by reading orders off of the short exact sequence

$$1 \to K_S/(W_S \cap K_S) \to I_{K,S}/W_S \to C_K/C_S \to 1 :$$

on one hand, we have $W_S \cap K_S = K_S^p$ (as in the proof of Lemma 20.3), which gives $\#K_S/(W_S \cap K_S) = p^{\#S}$; on the other hand, $I_{K,S}/W_S$ is the product of

$\#S$ quotients of the form $K_v^*/(K_v^*)^p$, each of which has order p^2 (generated by a uniformizer and a p-th root of unity, since p is prime to the residue characteristic).

One then checks that $W_S \subseteq \mathrm{Norm}_{L/K} I_L$ by checking this place by place; the places not in S are straightforward (they don't ramify in L, so local units are local norms), and the ones in S follow from the fact that for any local field M containing a p-th root of unity, if $N = M((M^*)^{1/p})$, then

$$\mathrm{Norm}_{N/M} N^* = (M^*)^p,$$

which we proved in the course of proving the local existence theorem (see Lemma 14.3). Putting this all together, we have $C' \subseteq \mathrm{Norm}_{L/K} C_L$ and these two groups have the same index $[L : K]$ in C_K by the First and Second Inequalities (Theorem 19.1, Theorem 20.1).

We next drop the restriction that K contains a p-th root of unity by reducing to the previous case. Namely, put $K' = K(\zeta_p)$. For a choice of S as above, let S' be the set of places of K' above S; we can make S large enough so that $I_{K',S'}(K')^* = I_{K'}$. Then as above, $C_{S'} = \mathrm{Norm}_{L'/K'} C_{L'}$ if L' is the extension of K' obtained by adjoining all p-th roots. Also as above, $\mathrm{Norm}_{K'/K} W_{S'} \subseteq W_S$, so

$$\mathrm{Norm}_{L'/K} C_{L'} = \mathrm{Norm}_{K'/K}(\mathrm{Norm}_{L'/K'} C_{L'}) = \mathrm{Norm}_{K'/K} C_{S'} \subseteq C_S \subseteq U.$$

Finally, we handle the case where U has arbitrary index, by induction on that index using the above result as the base case. If $\#C_K/U$ is not prime, 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. □

CHAPTER 23

The connection with local reciprocity

Reference. Milne VII.5; Neukirch VI.4.

So far, we've used abstract class field theory to construct reciprocity isomorphisms

$$r'_{L/K} : C_K / \operatorname{Norm}_{L/K} C_L \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$$

and to establish the adelic form of the existence theorem. We also know that if L/K is a small cyclotomic extension, then this map induces the usual Artin map.

This time, we'll verify that this map coincides with the product of the local reciprocity maps. As noted earlier, this is enough to recover the classical Artin reciprocity law and existence theorem.

I've also included a sketch of a Galois-cohomological approach to the reciprocity isomorphism (as found in Milne), using H^2 and an explicit computation in local class field theory. One of the sketchy points is that this computation requires a little of the Lubin-Tate construction, which makes the local existence theorem rather explicit but will not be discussed herein.

The relationship with local reciprocity.

Caveat. This still does not follow Milne or Neukirch.

For any extension L/K of number fields, we currently have the map $r_{L/K} : I_K \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$ formed as the product of the local reciprocity maps, and the abstract reciprocity map $r'_{L/K} : I_K \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$, which actually factors through C_K and even through $C_K / \operatorname{Norm}_{L/K} C_L$. We want to show that these agree. Before doing so, let's observe some consequences of that which we'll then use in the proof that they agree.

If L/K is abelian, v is a place of K and w is a place of L above v, then we have an injection $K_v^* \to I_K$, which we then funnel through $r'_{L/K}$ to get a map into $\operatorname{Gal}(L/K)$. The following properties would follow from knowing that $r = r'$, but must be checked independently as part of the proof.

LEMMA 23.1. *The following statements hold:*

(i) *the composite map $K_v^* \to \operatorname{Gal}(L/K)$ actually maps into the decomposition group of w;*
(ii) *the subgroup $\operatorname{Norm}_{L_w/K_v} L_w^*$ is contained in the kernel of $K_v^* \to \operatorname{Gal}(L/K)$.*

In (ii), we would also know that "contained in" can be replaced by "equal to", but we won't try to check that independently.

PROOF. For (i), let M be the fixed field of the decomposition group of w; then we have the compatibility

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & C_K/\operatorname{Norm}_{L/K} C_L \\ \downarrow & & \downarrow \\ \mathrm{Gal}(M/K) & \longrightarrow & C_K/\operatorname{Norm}_{M/K} C_M \end{array}$$

and the image of $K_v^* \to I_K$ lands in $\operatorname{Norm}_{M/K} I_M$ because v splits completely in M. So this image lies in the kernel of $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, which is to say $\mathrm{Gal}(L/M)$, the decomposition group of w.

For (ii), we need only check that $\operatorname{Norm}_{L_w/K_v} L_w^*$ is contained in the kernel of $K_v^* \to C_K/\operatorname{Norm}_{L/K} C_L$. But $\operatorname{Norm}_{L_w/K_v} L_w^*$ is already in the kernel of $K_v^* \to I_K/\operatorname{Norm}_{L/K} I_L$, so we're all set. □

Our plan now is to attempt to recover the local reciprocity map from the maps $r'_{L/K}$. To do this, we need some auxiliary global extensions, provided by the Existence Theorem.

LEMMA 23.2. *Let K be a number field, v a place of K and 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.*

PROOF. This is easy if 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 22.1) and Lemma 23.1(ii), it suffices to produce an open subgroup U of C_K of finite index such that the preimage of U under $K_v^* \to C_K$ is contained in $N = \operatorname{Norm}_{M/K_v} M^*$. Let S be the set of infinite places and $T = S \cup \{v\}$, and let $G = K_T \cap N$. Then one can choose an additional place u (finite and distinct from v) and an open subgroup V of $\mathfrak{o}_{K_u}^*$ such that $V \cap K_T \subseteq G$. Now put

$$W = N \times V \times \prod_{w \in S} K_w^* \times \prod_{w \notin S \cup \{u,v\}} \mathfrak{o}_K^*$$

and $U = WK^*/K^*$. If $\alpha_v \in K_v^*$ maps into U, then there exists $\beta \in K^*$ such that $\alpha_v \beta \in W$. That means first of all that $\beta \in K_T$ and then that $\beta \in V$, so that $\beta \in G$ and so also $\beta \in N$. It also means that $\alpha_v \beta \in N$. Thus $\alpha_v \in N$, as desired. □

For each place v of K and each abelian extension M of K_v, we can now write down a map $r'_{K,v} : K_v^* \to \mathrm{Gal}(M/K_v)$ by choosing an abelian extension L such that $M \subseteq L_w$ for any place w of L above v, letting N be the fixed field of the decomposition group of w, and setting $r'_{K,v}$ equal to the composition

$$K_v^* \overset{r'_{L/K}}{\to} \mathrm{Gal}(L/N) = \mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(M/K_v).$$

By the same compatibility as above, this doesn't change if we enlarge L. Thus it doesn't depend on the choice of L at all! (Any two choices of L sit inside an abelian extension of K; compare both with that bigger field.)

Again by the usual compatibilities, these maps fit together to give a single map $r'_{K,v} : K_v^* \to \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$. This map has the following properties:

(a) For M/K unramified, the induced map $K_v^* \to \mathrm{Gal}(M/K_v^*)$ kills units and maps a uniformizer of K_v to the Frobenius automorphism. Since that extension is generated by roots of unity, we can check this using a suitable small cyclotomic extension of K, on which r' may be computed explicitly. We leave further details to the reader.

(b) For any finite extension M/K_v^*, $r'_{K,v}$ induces an isomorphism

$$K_v^*/\operatorname{Norm}_{M/K_v} M^* \to \mathrm{Gal}(M/K_v^*).$$

Note that *a priori* we only know that this map is injective, but by the local reciprocity law the two groups have the same order, so it's actually an isomorphism. (For this and other reasons, we do not get an independent proof of local class field theory by this process.)

But these properties *uniquely* characterize the local reciprocity map! We conclude that $r'_{K,v}$ is the local reciprocity map for K_v, and so $r_{L/K} = r'_{L/K}$ and at long last Artin reciprocity (and the classical existence theorem, and the whole lot) follows. Hooray!

It's worth repeating that only now do we know that the product $r_{L/K}$ of the local reciprocity maps kills principal idèles. That fact, which relates local behavior for different primes in a highly global fashion, is the basis of various *higher reciprocity laws*. See Milne, Chapter VIII for details.

An explicit computation in local CFT.

We sketch an alternate approach for comparing the "abstract" reciprocity map $r'_{L/K}$ with the product $r_{L/K}$ of the local reciprocity maps, following Milne (and Neukirch V.2).

We first verify that $r = r'$ for cyclotomic extensions of $\mathbb{Q}$, using an explicit computation in local class field theory. Namely, we compute that if we identify $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$ with $(\mathbb{Z}/p^m\mathbb{Z})^*$, then the local reciprocity maps are given by

$$r_{\mathbb{Q}_\ell(\zeta_{p^m})/\mathbb{Q}_\ell}(a) = \begin{cases} \mathrm{sign}(a) & \ell = \infty \\ \ell^{v_\ell}(a) & \ell \neq \infty, p \\ u^{-1} & \ell = p. \end{cases}$$

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 $\mathrm{Gal}(L/K)$. By Neukirch's definition of the reciprocity map, 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.,

$$r_{L/K}^{-1}(\sigma) \in u \operatorname{Norm}_{L/K} L^*.$$

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 Neukirch V.2 and V.4 and/or Milne I.3.

A bit about Brauer groups.

For background about Brauer groups, see Milne, IV. We'll be following Milne VII.8 for now, and omitting many details.

PROPOSITION 23.3. *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 previous section (factor n into prime powers and apply the previous argument to each factor). In general, we have a compatibility

$$\begin{array}{ccc} I_L & \longrightarrow & \mathrm{Gal}(L_w(\zeta_n)/L_w) \\ \Big\downarrow{\scriptstyle \mathrm{Norm}_{L_w/\mathbb{Q}_p}} & & \Big\downarrow \\ I_{\mathbb{Q}} & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \end{array}$$

and we know the bottom row kills principal idèles and the right column is injective. Thus the top row kills principal idèles too. □

To make more progress, we need to bring in H^2, as we did in local reciprocity. (Unfortunately, trying to compute H^2 of the idèle class group is a headache, so we can't imitate the argument perfectly.) Recall there that we saw that every element of $H^2(L/K)$ could be "brought in" from a suitable unramified extension of K. We have a similar situation here with "unramified" replaced by "cyclotomic".

PROPOSITION 23.4. *Let L/K be any finite Galois extension of number fields. Then for any element x of $H^2(\mathrm{Gal}(L/K), L^*)$, there exists a cyclic, cyclotomic extension M of K and an element y of $H^2(\mathrm{Gal}(M/K), M^*)$ such that x and y map to the same element of $H^2(\mathrm{Gal}(ML/K), ML^*)$.*

PROOF. Omitted. See above references. □

Hereafter L/K is abelian. From the exact sequence

$$0 \to L^* \to I_L \to C_L \to 0$$

we get a fragment

$$1 = H^1(\mathrm{Gal}(L/K), C_L) \to H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/K), I_L)$$

so the map $H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/K), I_L) = \oplus H^2(\mathrm{Gal}(L/K), I_L)$ is injective. Each factor in the direct sum is canonically a subgroup of $\mathbb{Q}/\mathbb{Z}$, so we get a sum map $H^2(\mathrm{Gal}(L/K), I_L) \to \mathbb{Q}/\mathbb{Z}$.

It turns out (see Milne, Lemma VII.8.5) that for any map $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$, there is a commuting diagram

$$\begin{array}{ccccc} K^* & \longrightarrow & I_K & \xrightarrow{r_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(L^*) & \longrightarrow & H^2(I_L) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

If L/K is cyclic, we may choose the map $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ to be injective, and then the first vertical arrow will be surjective. (In fact, it's $K^* \to K^*/\operatorname{Norm}_{L/K} L^* = H^0_T(L^*)$ plus the periodicity isomorphism $H^0_T(L^*) \to H^2_T(L^*)$.) Then the fact that $r_{L/K}$ kills principal idèles implies that the composite $H^2(L^*) \to \mathbb{Q}/\mathbb{Z}$ is the zero map.

Now if we know $H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$ vanishes for all cyclic extensions, we know it in particular for cyclic cyclotomic extensions. But then the previous proposition tells us that it also vanishes for any finite Galois extension! Now we can use the diagram in reverse: it tells us that for $a \in K^*$, $r_{L/K}(a)$ is killed by any homomorphism $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$. Since $\mathrm{Gal}(L/K)$ is an abelian group, that implies $r_{L/K}(a)$ is trivial.

To conclude, we now have that $r_{L/K}$ kills principal idèles in general. By construction, it also kills norms (since it does so locally), so it induces a surjection $C_K/\operatorname{Norm}_{L/K} C_L \to \mathrm{Gal}(L/K)$. (Remember, the fact that it's surjective follows from the First Inequality.) But the order of the first group is less than or equal to the order of the second by the Second Inequality. So it's an isomorphism, and the reciprocity law is established. Hooray again!

Part 7

Coda

CHAPTER 24

Parting thoughts

Class field theory is 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.
- The Artin reciprocity law for an abelian extension of a number field.
- The existence theorem classifying abelian extensions of number fields in terms of generalized ideal class groups.
- The Chebotarev density theorem, describing the distribution over primes of a number field of various splitting behaviors in an extension field.
- Some group cohomology "nuts and bolts", including some key results of Tate.
- The local reciprocity law and existence theorem.
- Adèles, idèles, and the idelic formulations of reciprocity and the existence theorem.
- Computations of group cohomology in the local (multiplicative group) and global (idèle class group) cases.

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.
- The Brauer group of a field (i.e., $H^2(\mathrm{Gal}(\overline{K}/K), K^*)$), its relationship with central simple algebras, and the Fundamental Exact Sequence.
- 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.
- 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.
- Explicit class field theory for imaginary quadratic fields, via elliptic curves with complex multiplication.
- Quadratic forms over number fields and the Hasse-Minkowski theorem.
- Artin (nonabelian) L-series, the basis of "nonabelian class field theory."

Some additional topics for further reading would include the following.

- The Golod-Shafarevich inequality and the class field tower problem (see Cassels-Fröhlich).

- Class field theory for function fields used to produce curves over finite fields with unusually many points (see the web site `http://manypoints.org` for references).
- Application of Artin reciprocity to cubic, quartic, and higher reciprocity (see Milne).
- Algorithmic class field theory (see the books of Henri Cohen).

And finally, some ruminations about where number theory has gone in the fifty or so years since the results of class field theory were established in the form that we saw them. 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 what is about the same, the higher-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$?

In fact, 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. In particular, it includes the "modularity of elliptic curves", proved by Breuil, Conrad, Diamond, and Taylor following on the celebrated work of Wiles on Fermat's Last Theorem.

Various analogues of the Langlands correspondence have been worked out very recently: for local fields by Taylor and Harris (and again, more simply, by Henniart and Scholze), and for function fields by Lafforgue, based on the work of Drinfeld. The work of Laumon and Ngo on the Langlands fundamental lemma is also part of this story.

Okay, enough rambling for now; I hope that helps provide a bit of perspective. Thanks for reading!