CLASS FIELD THEORY

KENZ KALLAL

Abstract. These notes are the result of my study of class field theory in a reading project under the supervision of Mark Kisin. This project was supported by summer 2019 HCRP (Harvard College Research Program) funding. In these notes, I've done my best to get directly to the point of being able to prove the main results of local and global class field theory, without the involvement of too much abstract machinery like the cohomology of the ideles. To do this, most of the exposition follows the second part of Lang's classic text on algebraic number theory. I've also included a section on the basic methods of explicit class field theory, in the case of local fields (Lubin–Tate theory) and imaginary quadratic number fields (complex multiplication).

Contents

Date: November 8, 2019.

1. HCRP Final Report

1.1. **Research goals, accomplishments, and challenges.** The main goal of this project was to learn the statements and proofs of local and global class field theory. The approach I followed was close to the historical one, which follows a global-to-local strategy. For most of the core material on this topic, I followed the canonical book by Lang [9], as recommended by Professor Kisin. One way to motivate the statements is as follows: to generalize Dirichlet's theorem on primes in arithmetic progressions to the primes in generalized ideal classes, we define the Hecke L-functions analogously to the Dirichlet L-functions, except with respect to characters of the *generalized ideal class group* $I(\mathfrak{m})/P_{\mathfrak{m}}$, generalizing the usual group $(\mathbf{Z}/m\mathbf{Z})^\times$. From the finiteness of $I(\mathfrak{m})/P_{\mathfrak{m}}$, one can show that $L(s,\chi)$ converges slightly to the left of $s=1$ when χ is nontrivial. The only remaining step is then to show that $L(1,\chi)\neq 0$. This can be done directly, but the important question is whether it can be done using a formula analogous to the one for Dirichlet L-functions, namely $\prod_\chi L(s,\chi) = \zeta_{\mathbf{Q}(\zeta_m)}(s)$ up to some entire factors. To do this, one can show the existence of an abelian extension K/k whose Galois group is isomorphic to $I(\mathfrak{m})/P_{\mathfrak{m}}$ via the Artin map, thereby proving a natural correspondence between Hecke and Artin L-functions in the abelian case. The relevant theorem of class field theory is the **existence theorem**, which is best stated in terms of the topological group of *idèles* J_k.

Theorem 1.1. *Let k be a number field and H an arbitrary open subgroup of $J_k/k^\times$. Then there exists an abelian extension K/k such that the Artin map $J_k/k^\times \to \mathrm{Gal}(K/k)$ has kernel H.*

Going the other way, it is useful to know that Artin L-functions converge on a right half-plane past 1 (to do this it suffices to show that the abelian Artin L-functions are all Hecke L-functions for some modulus). One reason it is useful is that in the abelian case, it can be used to prove the **Chebotarev density theorem**, a further generalization of Dirichlet's theorem on primes in arithmetic progression which has the following consequence:

Theorem 1.2. *Every abelian extension of k is uniquely determined by the set of primes of k which split completely in the extension.*

The desired fact that every abelian Artin L-function is equal to a Hecke L-function can be proved using the **global reciprocity law** of class field theory:

Theorem 1.3. *Let K/k be an abelian extension. Then for any admissible modulus $\mathfrak{m}$ for K/k, the Artin map induces an isomorphism $I(\mathfrak{m})/P_{\mathfrak{m}}N(\mathfrak{m}) \to \mathrm{Gal}(K/k)$.*

Though the motivation for these statements may be seen to be about the relationship between two different types of L-functions each with desirable properties (the Hecke L-functions having good convergence properties and the Artin L-functions having a good relationship with a certain Dedekind ζ function), the actual statements of Theorems 1.3 and 1.1 immediately lead to another story, namely the **class field correspondence**:

Theorem 1.4. *The abelian extensions of k are in bijection with the open subgroups of $J_k/k^\times$ via the map $K \mapsto N(J_k/k^\times)$.*

Theorems 1.2 and 1.4 follow the theme that the abelian extensions are determined by information given by the kernel of their respective Artin map. Theorem 1.4 is particularly interesting because it gives a description of the abelian extensions of k in terms of the arithmetic of k itself, stated in terms of the topology of the idèle class group.

There's another important theme in the main statements of class field theory, namely that of *local-global compatibility.* From the idèlic Artin map $J_k \to \mathrm{Gal}(K/k)$ we can extract the local Artin maps $k_v^\times \to \mathrm{Gal}(K/k)$ via the embeddings $k_v^\times \to J_k$, and prove the image of the local Artin map is the decomposition group of v, which is to be expected since it is naturally identified with $\mathrm{Gal}(K_w/k_v)$. So we get **local Artin reciprocity**:

Theorem 1.5. *The local Artin map induces an isomorphism $k_v^\times/N(K^\times) \to \mathrm{Gal}(K_w/k_v)$.*

The local statement is enormously helpful in finishing off the proof of the global existence theorem. It also leads to a whole part of the theory which relates the kernel of the Artin map to the ramification behavior of primes.

Gaining a thorough understanding of how to prove these statements took up the first half of the summer. Even from this global-first approach where the cohomological tools are pretty light, I picked up a number of tools in the process:

- General constructions of L-functions for number fields
- Adeles and Idèles, and the basic theory of topological groups
- Group cohomology
- Kummer theory

The second half of the summer, I learned about questions for which the surrounding theory is somewhat more modern. Neither local nor global class field theory can be very explicit in general (at the ramified primes the local reciprocity map is difficult to define explicitly. In the global theory, the existence theorem is nonconstructive). But in some special cases, the abelian extensions K/k can be described explicitly. For abelian extensions of local fields, the answer is given by *Lubin-Tate theory*, which for a local field k decomposes k^{ab} into the compositum of the maximal unramified abelian extension k^{ur} and a totally ramified extension k_π which is constructed (based on a choice of uniformizer π) by adjoining the torsion points of a *Lubin-Tate formal group law* on the maximal ideal of the separable closure of k. The group law may be defined in terms of power series in two variables, specifically so that adjoining the torsion points means adjoining roots of Eisenstein polynomials (thus creating the totally ramified extension k_π). This can be motivated by looking at the special case of totally ramified extensions of $\mathbf{Q}_p$. I learned about this topic from a book chapter of Serre [1, Ch. VI].

In the global case, the only known explicit generalization of Kronecker–Weber is in the imaginary quadratic case $k = \mathbf{Q}(\sqrt{-d})$. The idea is to consider all the elliptic curves E whose endomorphism ring has extra endomorphisms coming from multiplying the corresponding lattice $\Lambda \subset \mathbf{C}$ by elements of $\mathcal{O}_k$ (such elliptic curves are said to have *complex multiplication* by $\mathcal{O}_k$). The main result relating to explicit class field theory is that the maximal unramified abelian extension of k is explicitly equal to $k(j(E))$, and that in most cases, every finite abelian extension of k is contained in an extension of the form $k(j(E), x_i)$ where the x_i are coordinates of torsion points of E. This was the most challenging topic for me this summer, because of its reliance on technical results from the theory of elliptic curves. I used three sources for complex multiplication and elliptic curves: Silverman's books [13, 14] and Serre's other chapter [1, Ch. XIII].

1.2. **Personal implications.** Thanks to the HCRP funding, this summer was a great time of mathematical development for me. It allowed me to crystallize my understanding of the core concepts of algebraic number theory, and to gain technical competence with concepts which were new to me: not only the statements of class field theory, but also universally important tools, including the more general types of zeta functions and L-functions, Kummer theory, group cohomology, topological group theory, infinite Galois theory, and elliptic curves. The difficulty of my foray into elliptic curves also forced me to realize the importance that algebraic geometry will have in my future studies of number theory, and how crucial mastering as much of the subject as I can will be in the next two years. As a result, I have started a thorough reading of Vakil's introductory text [16].

1.3. **Implications for my senior thesis.** Though I don't have any fully fleshed-out ideas for my senior thesis topic, this project was influential for my thesis in that it allowed me to gain the technical competence to tackle more advanced projects in number theory. It also influenced me strongly in the direction of doing a senior thesis in the general area of number theory. Within that, there are a lot of places my study of algebraic number theory can lead, especially once I learn algebraic geometry properly. One very interesting topic which I have only seen glimpses of (from the theory of the j-invariant and separately from concrete applications like sums of 4 squares) is the theory of modular forms, which play an important role in the conjectural generalization of class field theory given by the Langlands correspondence. I might also be interested in topics in arithmetic geometry like étale cohomology (and its application to the Weil conjectures). Of course, this is strongly conditional on my knowledge of algebraic expanding substantially over the next year.

1.4. **Interaction with my faculty sponsor.** Professor Kisin and I met in person twice over the summer. The first time was after I read most of the class field theory content of Lang's book (by then we were already in communication over email about all the questions I had about the material). The main questions I had at this meeting were about how class field theory can be done explicitly. As a result, Professor Kisin recommended I read chapters by Serre in the classical book of Cassels and Fröhlich, the first on local class field theory and the second on complex multiplication. The exposition in both of these chapters is written at a higher level than in Lang's book, and it took some time for me to understand even the one on local class field theory. For complex multiplication, it was hard for me to get started due to my relative unfamiliarity with the theory of elliptic curves. At our second in-person meeting, Professor Kisin stressed the usefulness of the abstractions of algebraic geometry in dealing with objects like elliptic curves in a more canonical way. He recommended a book of Katz–Mazur [7] and an article of Deligne–Rapaport [4]. Both of these are somewhat beyond the reach of my technical understanding of algebraic geometry, but motivated my current project of reading Vakil's classic text on algebraic geometry. In the end, it was from the more concrete books of Silverman that I was able to understand the details of the theory of complex multiplication.

1.5. **Use of funds.** The HCRP award was used to support my living expenses (room and board) for the summer of 2019. Other than books, there were no expenses directly related to the project.

2. Introduction

3. L-functions

3.1. **Hecke L-functions and generalized ideal class groups.** Recall from the basics of analytic number theory (see for example [5, `dirichlet.pdf`]) the construction of the Dirichlet L-function, first on the right half-plane $\Re(s) > 1$ via the absolutely convergent series

$$L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s}$$

where χ is a *Dirichlet character* mod m. In particular, χ is a complex character of the finite abelian group $(\mathbf{Z}/m\mathbf{Z})^\times$ which lifts to a function $\mathbf{N} \to \mathbf{C}^\times$ by taking χ to be zero on all $n \in \mathbf{N}$ not coprime to m. These L-functions are useful for estimating the asymptotic growth of the prime-counting function $\pi(x; a \mod m)$[1] (see for example [5, `pnt_q.pdf`]), because of the fact from the representation theory of finite abelian groups that for $(a, m) = 1$,

$$\pi(x; a \mod m) = \sum_\chi \chi(a) \frac{1}{\varphi(m)} \sum_{b \in (\mathbf{Z}/m\mathbf{Z})^\times} \overline{\chi(b)} \pi(x; b \mod m),$$

and the estimate[2]

$$\log L(s, \chi) = \sum_p \chi(p) p^{-s} + O_{s_0}(1)$$

for $1 < s \leq s_0$. By observing (e.g. by the method of partial summation) that the L-series for nontrivial characters converge uniformly for $\Re(s) > 0$ and showing[3] that $L(1, \chi) \neq 0$, one can conclude at least the original statement of Dirichlet's theorem on primes in arithmetic progressions[4]:

Theorem 3.1. *Let $m \in \mathbf{N}$ and a be an integer such that $(a, m) = 1$. Then the set of primes congruent to $a \mod m$ have Dirichlet density $1/\varphi(m)$ in the set of all primes. As a consequence, there are infinitely many such primes.*

As usual in algebraic number theory, the question becomes how to generalize questions about congruence classes of primes to arbitrary number fields. Let K be a number field. The usual way of doing this is to order the ideals of $\mathcal{O}_K$ according to their norm. Then one can use the *Dedekind zeta function*, defined by the absolutely convergent Euler product

$$\zeta_K(s) = \prod_{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - (\mathrm{N}\mathfrak{p})^{-s}} = \sum_{0 \neq I \subseteq \mathcal{O}_K} (\mathrm{N}I)^{-s}$$

[1] The prime-counting function $\pi(x; a \mod m)$ is just the number of primes $\leq x$ congruent to a mod m.

[2] This uses the Taylor expansion for $\log(1 + x)$ and the absolutely-convergent Euler product $L(s, \chi) = \prod_p \frac{1}{1 - \chi(p) p^{-s}}$. Note that this involves a choice of branch for the complex logarithm when χ is not real.

[3] The fact that $L(1, \chi) \neq 0$ is usually considered the main nontrivial step in the proof of Dirichlet's theorem. One way to do it is to observe that up to some entire factors, $\prod_\chi L(s, \chi) = \zeta_{\mathbf{Q}(\zeta_m)}(s)$

[4] Adapting the proof of the prime number theorem (see [5, `pnt.pdf`]) to the machinery of L-functions of Dirichlet characters instead of the ζ-function can also yield the same statement for natural density, with error bounds depending on the strength of a zero-free region for an analytic continuation of $L(s, \chi)$ as an entire function.

for $\Re(s) > 1$, where the product is over all nonzero prime ideals, and the sum is over all nonzero ideals. One can continue ζ_K to a meromorphic function[5] with only simple poles at $s = 0, 1$. Armed with the appropriate analytic object, Landau [8] showed the generalization of the prime number theorem to the number of prime ideals of norm at most x via the usual contour integrals involving ζ_K'/ζ_K and the Perron integral formula. Given the success of adapting the prime number theorem, how might Dirichlet's theorem on primes in arithmetic progressions be generalized to the prime ideals of $\mathcal{O}_K$? Let $\mathfrak{m}$ be a nonzero ideal in $\mathcal{O}_K$. Analogously to considering the primes coprime to a fixed modulus $m \in \mathbf{Z}$, we consider the prime ideals in the group $I(\mathfrak{m})$ of fractional ideals coprime to $\mathfrak{m}$. For any nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$, let $m(\mathfrak{p})$ denote the multiplicity of $\mathfrak{p}$ in the factorization of $\mathfrak{m}$. At the very least, we should mod out by the subgroup of principal fractional ideals (α) of $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(\alpha - 1) \geq m(\mathfrak{p})$ for all nonzero primes $\mathfrak{p}$. In effect, we quotient by open subgroups (necessarily open neighborhoods of 1) with respect to each nonarchimedean valuation. For the archimedean valuations, $\mathbf{C}^\times$ has no nontrivial open subgroups, and $\mathbf{R}^\times$ has only the subgroup of positive real numbers. This has finite index in $\mathbf{R}^\times$, so we might as well also require that the group of principal ideals (α) we quotient by has $v(\alpha) > 0$ for some predetermined set of real valuations v. This discussion is summarized in the following definitions:

Definition 3.2. A *modulus* $\mathfrak{m}$ of k is a finite formal product of nonarchimedean and real valuations of k. In particular,

$$\mathfrak{m} = \prod_{v \in M_k} v^{m(v)}$$

where all but finitely many of the $m(v)$'s are zero and $m(v) \geq 0$ for all v. At all real places $v|\mathfrak{m}$, we might as well require $m(v) = 1$. Equivalently[6], we can separate the nonarchimedean from the real places and define a modulus to be a nonzero integral ideal $\mathfrak{m}_0$, together with a collection of real places $\mathfrak{m}_\infty$.

Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of k.

Definition 3.3. $I(\mathfrak{m})$ denotes the (abelian) group of fractional ideals of $\mathcal{O}_k$ coprime to $\mathfrak{m}_0$.

Definition 3.4. $P_\mathfrak{m}$ denotes the subgroup of $I(\mathfrak{m})$ consisting of all principal fractional ideals (α) such that $v_{\mathfrak{p}}(\alpha - 1) \geq m(v_{\mathfrak{p}})$ for all $\mathfrak{p}|\mathfrak{m}_0$, and $v(\alpha) > 0$ for all $v|\mathfrak{m}_\infty$.

Definition 3.5. Define the *generalized ideal class group* to be $I(\mathfrak{m})/P_\mathfrak{m}$. This is also sometimes called the *ray class group* of $\mathfrak{m}$.

[5] This is done by proving a functional equation analogous to the one for the Riemann zeta function. Hecke did it directly using the higher-dimensional Poisson summation formula. Later, Tate used Poisson summation on the ring of adeles to achieve the same result. For both of these proofs see [9, Ch. XIII, XIV]. The order and residue of the pole at $s = 1$ comes down to estimating the number of elements of $\mathcal{O}_K$ of norm at most x. It turns out (see [11, Ch. VII, §5]) that the residue is equal to $\frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{|\mu_K|\sqrt{|d_K|}}$ where r_1, $2r_2$ are number of real and complex embeddings, respectively, h_K is the class number, R_K is the regulator, μ_K is the group of roots of unity in K, and d_K is the absolute discriminant of K.

[6] The equivalence is due to the unique decomposition of nonzero (integral) ideals of $\mathcal{O}_K$ into nonzero primes.

Example 3.6. The option to require that the ideals in $P_{\mathfrak{m}}$ are generated by elements which are positive with respect to some valuations is concretely useful. Recall that the original motivation was to generalize the group of residues $(\mathbf{Z}/m\mathbf{Z})^\times$ to the ideals coprime to $\mathfrak{m}$. To achieve this as a special case of the generalized ideal class group, we must include the real valuation of $\mathbf{Q}$ in the modulus $\mathfrak{m}$. In particular, let $k = \mathbf{Q}$, m be a positive integer, and $\mathfrak{m}$ be the modulus whose finite part is $m\mathbf{Z}$ and whose infinite part is the single real valuation $v_\infty : \mathbf{Q} \to \mathbf{R}$. Then $I(\mathfrak{m})/P_{\mathfrak{m}} \cong (\mathbf{Z}/m\mathbf{Z})^\times$ via the following isomorphism: each element $\mathfrak{a} \in I(\mathfrak{m})$ can be written uniquely[7] in the form (a/b), where $a/b > 0$ and is in reduced form, while a, b are both coprime to m. Send (a/b) to the residue $(a \mod m)(b \mod m)^{-1}$. The kernel of this homomorphism is the set of ideals (a/b) such that $a \cong b \mod m$ and $a/b > 0$. This is precisely $P_{\mathfrak{m}}$, so this map induces the desired isomorphism of abelian groups. Note that if we did not require $v_\infty | \mathfrak{m}$, the resulting generalized ideal class group would have index 2 in $(\mathbf{Z}/m\mathbf{Z})^\times$.

Example 3.7. The generalized ideal class group deserves its name: If we set $\mathfrak{m} = 1$, then $I(\mathfrak{m})$ is the group of fractional ideals of $\mathcal{O}_k$, and $P_{\mathfrak{m}}$ is the group of principal ideals. In particular, in this special case the generalized ideal class group coincides with the class group I_k/P_k.

The attempt to generalize Dirichlet's theorem on arithmetic progressions can be easily stated:

Question 3.8. Are there infinitely many nonzero primes $\mathfrak{p} \subseteq \mathfrak{O}_k$ in each residue class in $I(\mathfrak{m})/P_{\mathfrak{m}}$? Do the primes in each class all have the same Dirichlet density?

Like the ideal class group, we will show that the generalized ideal class group is finite (in fact we will use the finiteness of the class group along the way). Once we know $I(\mathfrak{m})/P_{\mathfrak{m}}$ is finite, we can leverage the representation theory of finite abelian groups in the same way as in the proof of Dirichlet's theorem on primes in arithmetic progression. This will establish the connection between the L-functions coming from characters of $I(\mathfrak{m})/P_{\mathfrak{m}}$ and the nonzero prime ideals in $I(\mathfrak{m})$ with particular residues. Now that we have the desired group of ideal classes, we can define the appropriate characters and L-functions.

Definition 3.9. A *Hecke character* modulo $\mathfrak{m}$ is a complex character of the abelian group $I(\mathfrak{m})/P_{\mathfrak{m}}$.

Definition 3.10. Let $\chi : I(\mathfrak{m})/P_{\mathfrak{m}} \to \mathbf{C}^\times$ be a Hecke character. The corresponding L-function is defined on the half-plane $\Re(s) > 1$ by

$$L(s,\chi) = \sum_{\substack{I \subseteq \mathcal{O}_k \\ (I,\mathfrak{m})}} \chi(I)(\mathrm{N}I)^{-s} = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s}},$$

where the sum is over all nonzero (integral) ideals of $\mathcal{O}_K$ coprime to $\mathfrak{m}$.

To build a theory analagous to that of the Dirichlet L-function, two ingredients are still missing:

- The finiteness of the generalized ideal class group
- For nontrivial χ, the convergence of $L(s,\chi)$ on a right half-plane containing 1, and the nonvanishing of $L(1,\chi)$.

[7] The uniqueness follows from the fact that $\mathbf{Z}^\times = \{\pm 1\}$.

The first ingredient comes down to a simple dévissage argument.

Theorem 3.11. *Let $\mathfrak{m}$ be a modulus of k. Then $I(\mathfrak{m})/P_\mathfrak{m}$ is finite. In particular, it has*

$$h_\mathfrak{m} := \frac{h_k 2^{s(\mathfrak{m}_\infty)}}{[\mathcal{O}_K^\times : (\mathcal{O}_K^\times)_\mathfrak{m}]} \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathrm{N}\mathfrak{p} - 1)(\mathrm{N}\mathfrak{p})^{m(\mathfrak{p})-1}$$

elements, where h_k is the class number of k, $s(\mathfrak{m}_\infty)$ is the number of real places included in $\mathfrak{m}$, and $(\mathcal{O}_K^\times)_\mathfrak{m}$ is the group of units $\alpha \in \mathcal{O}_K^\times$ such that $v_\mathfrak{p}(\alpha - 1) > m(\mathfrak{p})$ for all nonarchimedean $v_\mathfrak{p}|\mathfrak{m}$ and $v(\alpha) > 0$ for all real $v|\mathfrak{m}_\infty$.

Proof. Let $\mathfrak{a} \in I_k$, and via the Chinese remainder theorem choose an $\alpha \in \mathcal{O}_k$ such that $\mathfrak{p}^{m(\mathfrak{p})}|\alpha$ for all $\mathfrak{p}|\mathfrak{m}$. Then in I_k/P_k, each element $[\mathfrak{a}]$ has a representative in $I(\mathfrak{m})$ given by $\alpha^{-1}\mathfrak{a}$. In particular, the homomorphism $I(\mathfrak{m}) \to I_k/P_k$ induced by the natural inclusion $I(\mathfrak{m}) \to I_k$ is surjective. So we have an isomorphism of finite abelian groups

$$I(\mathfrak{m})/(I(\mathfrak{m}) \cap P_k) \cong I_k/P_k.$$

We are interested in $I(\mathfrak{m})/P_\mathfrak{m}$, and we have only concluded that a quotient of this is finite. Now the relevant inclusion of groups is

$$P_\mathfrak{m} \subseteq I(\mathfrak{m}) \cap P_k.$$

This time, we have the homomorphism $k^\times \cap I(\mathfrak{m}) \to (P_k \cap I(\mathfrak{m}))/P_\mathfrak{m}$ given by $\alpha \mapsto [(\alpha)]$. It is surjective by definition of P_k, and its kernel is $\mathcal{O}_k^\times k_\mathfrak{m}$, where $k_\mathfrak{m}$ denotes the subgroup of $k^\times$ consisting of all α such that $v_\mathfrak{p}(\alpha - 1) > m(\mathfrak{p})$ for all $\mathfrak{p}|\mathfrak{m}_0$ and $v(\alpha) > 0$ for all $v|\mathfrak{m}_\infty$. So we have another isomorphism, this time

$$(k^\times \cap I(\mathfrak{m}))/(\mathcal{O}_k^\times k_\mathfrak{m}) \cong (P_k \cap I(\mathfrak{m}))/P_\mathfrak{m}.$$

So in fact it suffices to show that $(k^\times \cap I(\mathfrak{m}))/(\mathcal{O}_k^\times k_\mathfrak{m})$ is finite. Stronger than this, it's clear from the definitions that actually $(k^\times \cap I(\mathfrak{m}))/(k_\mathfrak{m})$ is already finite. This is because of the homomorphism

$$(k^\times \cap I(\mathfrak{m})) \to \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}})^\times \times \prod_{v|\mathfrak{m}_\infty} \mathbf{R}^\times/\mathbf{R}^\times_{\geq 0}$$

defined by taking α (whose valuation at all $\mathfrak{p}|\mathfrak{m}_0$ is necessarily zero) to its residue class in each term of the product. In particular, $\mathcal{O}_{k,\mathfrak{p}}$ is a DVR, so the residue mod $\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}}$ of any α is invertible if and only if α has zero $\mathfrak{p}$-adic valuation. For the real places we let the v-coordinate of the image of α be the residue of $v(\alpha)$.

This homomorphism is surjective by the weak approximation theorem[8], and its kernel is visibly $k_\mathfrak{m}$. So in fact there is an isomorphism

$$(k^\times \cap I(\mathfrak{m}))/(k_\mathfrak{m}) \cong \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}})^\times \times \prod_{v|\mathfrak{m}_\infty} \mathbf{R}^\times/\mathbf{R}^\times_{\geq 0}.$$

[8] There are only finitely many finite places corresponding to $\mathfrak{p}_1, \ldots, \mathfrak{p}_N$, and archimedean places $v_1, \ldots, v_M$ dividing $\mathfrak{m}$. For any choice of $\alpha_i \in \mathcal{O}_{k,\mathfrak{p}}^\times$ for all $1 \leq i \leq N$ and $\beta_i \in \mathbf{R}^\times$ for all $1 \leq i \leq M$, weak approximation guarantees the existence of an $x \in k^\times$ such that $x \equiv \alpha_i$ mod $\mathfrak{p}_i^{m(\mathfrak{p}_i)}\mathcal{O}_{k,\mathfrak{p}_i}$ and $x - \beta_i$ has small enough absolute value so that $v_i(x)$ has the same sign as $v_i(\beta_i)$. Since the units in $\mathcal{O}_{k,\mathfrak{p}_i}/\mathfrak{p}_i^{m(\mathfrak{p}_i)}\mathcal{O}_{k,\mathfrak{p}_i}$ are the same as the residues of the elements of $\mathcal{O}_{k,\mathfrak{p}_i}^\times$, it follows that x is the desired preimage. We also know that $x \in I(\mathfrak{m})$ since its $\mathfrak{p}$-adic valuation is zero for all $\mathfrak{p}|\mathfrak{m}$.

The right hand side is finite. Each archimedean local factor clearly has size 2 (there are 2 equivalence classes depending on the sign of the representative). The nonarchimedean factor corresponding to $\mathfrak{p}|\mathfrak{m}_0$ has size[9]

$$2^{s(\mathfrak{m}_\infty)}\prod_{\mathfrak{p}|\mathfrak{m}}(\mathrm{N}\mathfrak{p}-1)(\mathrm{N}\mathfrak{p})^{m(\mathfrak{p})-1}.$$

It follows immediately that $(k^\times \cap I(\mathfrak{m}))/(\mathcal{O}_k^\times k_\mathfrak{m})$ is finite, and its size is

$$\frac{|(k^\times \cap I(\mathfrak{m}))/k_\mathfrak{m}|}{|\mathcal{O}_k^\times/(k_\mathfrak{m}\cap \mathcal{O}_k^\times)|}=\frac{2^{s(\mathfrak{m}_\infty)}\prod_{\mathfrak{p}|\mathfrak{m}}(\mathrm{N}\mathfrak{p}-1)(\mathrm{N}\mathfrak{p})^{m(\mathfrak{p})-1}}{[\mathcal{O}_k^\times : (\mathcal{O}_k^\times)_\mathfrak{m}]}.$$

Finally, the index $[\mathcal{O}_k^\times : (\mathcal{O}_k^\times)_\mathfrak{m}]$ is clearly finite: $(\mathcal{O}_k^\times)_\mathfrak{m}$ is the intersection of finitely many subgroups of $\mathcal{O}_k^\times$, namely the subgroups $1+\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_k^\times$ for the $\mathfrak{p}|\mathfrak{m}_0$ and the subgroups consisting of units of positive absolute value with respect to the real $v|\mathfrak{m}_\infty$. It suffices to show[10] that each of these subgroups has finite index in $\mathcal{O}_k^\times$. This is easily seen for the archimedean places, since such an absolute value induces a group homomorphism $\mathcal{O}_k^\times \to \mathbf{R}^\times/\mathbf{R}_{\geq 0}\cong \mathbf{Z}/2\mathbf{Z}$ whose kernel is exactly the subgroup of elements $\alpha \in \mathcal{O}_k^\times$ such that $v(\alpha)>0$. For the nonarchimedean valuations $v_\mathfrak{p}$, just recall that

$$\mathcal{O}_k^\times/(1+\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_k)\cong \widehat{\mathcal{O}_{k,\mathfrak{p}}}^\times/(1+\mathfrak{p}^{m(\mathfrak{p})}\widehat{\mathcal{O}_{k,\mathfrak{p}}}),$$

but $\widehat{\mathcal{O}_{k,\mathfrak{p}}}^\times$ is compact, while $1+\mathfrak{p}^{m(\mathfrak{p})}\widehat{\mathcal{O}_{k,\mathfrak{p}}}$ is open, so the index is finite. Putting it all together, we have computed the size of the generalized ideal class group

$$\begin{aligned}|I(\mathfrak{m})/P_\mathfrak{m}| &= \frac{|I(\mathfrak{m})/(I(\mathfrak{m})\cap P_k)|}{|(I(\mathfrak{m})\cap P_k)/P_\mathfrak{m}|}\\ &= \frac{h_k}{|(I(\mathfrak{m})\cap P_k)/P_\mathfrak{m}|}\\ &= \frac{h_k}{|k^\times \cap I(\mathfrak{m})/(\mathcal{O}_k^\times k_\mathfrak{m})|}\\ &= \frac{h_k 2^{s(\mathfrak{m}_\infty)}\prod_{\mathfrak{p}|\mathfrak{m}}(\mathrm{N}\mathfrak{p}-1)(\mathrm{N}\mathfrak{p})^{m(\mathfrak{p})-1}}{[\mathcal{O}_k^\times : (\mathcal{O}_k^\times)_\mathfrak{m}]},\end{aligned}$$

as claimed. □

3.2. **Chebotarev's density theorem and the global reciprocity law.** It remains to show that $L(1,\chi)\neq 0$ for characters χ of $I(\mathfrak{m})/P_\mathfrak{m}$. In the case of $(\mathbf{Z}/m\mathbf{Z})$, the canonical way of doing this involves finding an Euler product expansion for $\prod_\chi L(s,\chi)$ valid on the usual right half-plane $\Re(s)>1$ which agrees up to some entire factor which doesn't vanish at 1 with the Euler product for $\zeta_{\mathbf{Q}(\zeta_m)}(s)$. Though they both satisfy functional equations and can be extended meromorphically to the whole complex plane, it suffices only to do this slightly to the left of 1. Once this

[9] Recall (the fact we've used already) that $\mathcal{O}_{k,\mathfrak{p}}^\times/(1+\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}})\cong(\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}})^\times$, and $(1+\mathfrak{p}^n\mathcal{O}_{k,\mathfrak{p}})/((1+\mathfrak{p}^{n+1}\mathcal{O}_{k,\mathfrak{p}})\cong\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}}$. As a result, $|(\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}})^\times| = |\mathcal{O}_{k,\mathfrak{p}}^\times/(1+\mathfrak{p}^{m(\mathfrak{p})}\mathcal{O}_{k,\mathfrak{p}})| = |\mathcal{O}_{k,\mathfrak{p}}^\times/(1+\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}})|\cdot|\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}}|^{m(\mathfrak{p})-1} = |(\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}}\times|\cdot|\mathcal{O}_{k,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}}|^{m(\mathfrak{p})-1} = (\mathrm{N}\mathfrak{p}-1)(\mathrm{N}\mathfrak{p})^{m(\mathfrak{p})-1}$.

[10] This is a basic fact from group theory: If H_1, H_2 are subgroups of G, then the cosets of $H_1\cap H_2$ are of the form $g(H_1\cap H_2)=gH_1\cap gH_2$ for $g\in G$. In particular, they are determined by a coset of H_1 and a coset of H_2, so in fact $[G:H_1\cap H_2]\leq[G:H_1][G:H_2]<\infty$.

is done, analytic continuation tells us that none of the $L(s,\chi)$ can have a zero at $s=1$ because this would delete the simple pole of $\zeta_{\mathbf{Q}(\zeta_m)}$. To generalize this, we must find an extension K/k such that $\prod_\chi L(s,\chi)$ agrees with $\zeta_K(s)$ up to some entire factors not vanishing at 1. In dealing with this issue, we will see that all the fundamental issues of global class field theory will crop up.

In the special case of $k=\mathbf{Q}$ and $I(\mathfrak{m})/P_\mathfrak{m}=(\mathbf{Z}/m\mathbf{Z})^\times$, the field extension $K/\mathbf{Q}$ was Galois with Galois group $(\mathbf{Z}/m\mathbf{Z})^\times$. In fact, the isomorphism

$$(\mathbf{Z}/m\mathbf{Z})^\times \to \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$$

is given by the Artin map $p\mapsto \left[\frac{\mathbf{Q}(\zeta_m)/\mathbf{Q}}{(p)}\right]$.

In particular, the bijectivity of the Artin map means that the characters of $(\mathbf{Z}/m\mathbf{Z})^\times$ are the same as the characters of $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$. Thus, in this case we can redefine the Dirichlet L-functions to correspond instead to a character of the Galois group of this particular extension. In particular, they are all of the form

$$L(s,\chi)=\prod_{p\nmid m}\frac{1}{1-\chi\left(\left[\frac{\mathbf{Q}(\zeta_m)/\mathbf{Q}}{(p)}\right]\right)(\mathrm{N}\mathfrak{p})^{-s}}$$

for characters χ of $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$, which is where the connection between L-functions corresponding to characters of the generalized ideal class group $(\mathbf{Z}/m\mathbf{Z})^\times$ and the zeta-function of the specific field $\mathbf{Q}(\zeta_m)/\mathbf{Q}$ comes from (we will prove this connection in generality). For Galois groups which are not necessarily abelian, the Artin map no longer necessarily gives a homomorphism from an ideal group to the Galois group, but we can still define L-series given an arbitrary representation of the Galois group (the natural generalization of the 1-dimensional characters of abelian groups), using the fact that the Artin map still yields a conjugacy class of the Galois group. This leads to the definition of Artin's L-functions:

Definition 3.12. Let K/k be a finite Galois extension of number fields, and let $\rho:\mathrm{Gal}(K/k)\to GL(V)$ be a finite-dimensional complex representation of $\mathrm{Gal}(K/k)$. Then the *Artin L-series* corresponding to ρ is, up to finitely many local factors corresponding to the ramified primes,

$$L^{\mathrm{Artin}}_{K/k}(s,\rho)=\prod_{\mathfrak{p}\nmid d_k}\frac{1}{\det\left(\mathrm{id}_V-(\mathrm{N}\mathfrak{p})^{-s}\rho\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)\right)},$$

well-defined due to the conjugacy-invariance of the characteristic polynomial.

In the case where K/k is abelian, the Artin L-function of an irreducible representation of $\mathrm{Gal}(K/k)$ has a product expansion $\prod_\mathfrak{p}\frac{1}{1-(\mathrm{N}\mathfrak{p})^{-s}\chi([\frac{K/k}{\mathfrak{p}}])}$ where χ is a (1-dimensional) character of $\mathrm{Gal}(K/k)$. Presumably after collecting more numerical data, Artin conjectured that the equivalence between Dirichlet L-functions corresponding to characters of the ray class group mod mv_∞ and Artin L-functions corresponding to irreducible representations of $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ extends in general via a natural isomorphism of groups (in fact the class field theory isomorphism was known by his time, but only non-canonically; his conjecture amounted to using the Artin map as this natural isomorphism).

Conjecture 3.13. *Let K/k be an abelian extension, and ρ a one-dimensional complex representation of* $\mathrm{Gal}(K/k)$. *Then there exists a modulus $\mathfrak{m}$ of k and a character $\chi:I(\mathfrak{m})/P_\mathfrak{m}\to\mathbf{C}^\times$ such that $L(s,\chi)=L^{\mathrm{Artin}}_{K/k}(s,\rho)$.*

This is clearly logically equivalent to the technical questions which are answered by the main theorems of global class field theory:

Question 3.14. Given an abelian extension K/k, does there exist a modulus $\mathfrak{m}$ of k divisible by only primes that ramify in K such that $P_{\mathfrak{m}}$ is contained in the kernel of the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$ and this map is surjective, so that the Artin map induces an isomorphism between $\mathrm{Gal}(K/k)$ and a quotient of the ray class group mod $\mathfrak{m}$? Is there a description in terms of the extension K/k of what to quotient by?

It's natural, too, to formulate the converse:

Question 3.15. Given a modulus $\mathfrak{m}$ of a number field k, does there exist a finite abelian extension K/k such that all the primes of k ramifying in K divide $\mathfrak{m}$, and the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$ is surjective with kernel containing $P_{\mathfrak{m}}$? This will yield an isomorphism between $\mathrm{Gal}(K/k)$ and a quotient of the ray class group mod $\mathfrak{m}$. Is it possible to achieve an abelian extension K/k inducing such an isomorphism between $\mathrm{Gal}(K/k)$ and any arbitrary quotient of the ray class group mod $\mathfrak{m}$?

Remark 3.16. Lang [9, page number] explains why we should expect these questions to be nontrivial: the Artin map is defined locally at each prime, but the definition of $P_{\mathfrak{m}}$ is a global one that has to do with arbitrary elements of $k^\times$.

It will turn out that there are remarkably simple answers to both questions, which are known today as the main results of class field theory. It comes down to a key technical condition on the modulus:

Definition 3.17. A modulus $\mathfrak{m}$ of k is *admissible* with respect to an abelian extension K/k if

$$N_{\widehat{K}_{\mathfrak{P}}/k_{\mathfrak{p}}}(\widehat{K}_{\mathfrak{P}}^\times) \subseteq 1 + \mathfrak{p}^{m(\mathfrak{p})}\widehat{\mathcal{O}}_{k,\mathfrak{p}}$$

for all $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{p}|\mathfrak{m}$. Of course, this is true for all $\mathfrak{P}|\mathfrak{p}$ if and only if it is true for a single one.

The most important result is a full answer to Question 3.14, known as Artin's reciprocity law.

Theorem 3.18. *Let K/k be an abelian extension, and $\mathfrak{m}$ any modulus for k admissible with respect to K/k. Let $\mathfrak{N}(\mathfrak{m})$ denote the subgroup of $I(\mathfrak{m})$ given by the relative norms of all the nonzero ideals $I \subseteq \mathcal{O}_K$ not containing any prime factors $\mathfrak{P}$ dividing any $\mathfrak{p}|\mathfrak{m}$. Then $\mathfrak{m}$ is divisible by all the primes ramifying in K, and the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$ is surjective and reduces to an isomorphism $I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}) \to \mathrm{Gal}(K/k)$.*

The answer in Theorem 3.18 leads to another important question, which we will answer later.

Question 3.19. By Theorem 3.18, the smallest (with respect to divisibility) admissible modulus of k is divisible by all the ramified primes. It will turn out that it is only divisible by ramified primes. What is its relationship with the discriminant d_K?

It turns out that Question 3.15 also has a full answer (in fact in much more generality) provided by class field theory, known as the *existence theorem.* It is relatively easy to state with the language we have so far, but because of the inconvenient nature of the generalized ideal class groups (mostly having to do with the fact that a modulus which is admissible for one extension may not be admissible for another), we'll postpone the discussion of this until the language of idèles has been developed. We will see with very little effort after these technical results have been proved that there is a correspondence holds between the arithmetic of the field k and the set of abelian extensions K/k. This is called the *class field correspondence*, and we have already caught a glimpse of it (the abelian extensions K/k are in correspondence with the subgroups of the generalized ideal class groups for admissible moduli given by the kernel of the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$). It is clumsy to state in terms of ideals again because of the need for the choice of an admissible modulus which is not consistent across extensions, so we postpone giving a precise statement until the idèles have been introduced.

Finally, we turn to Question 3.8, which was the original goal of this section. The important result on this question, which is indeed considered the most important generalization of Dirichlet's theorem on primes in arithmetic progression, is as follows:

Theorem 3.20 (Chebotarev density theorem). *Let K/k be a finite abelian extension. Then for each $\sigma \in \mathrm{Gal}(K/k)$, the set of nonzero primes $\mathfrak{p}$ of k such that $\left[\frac{K/k}{\mathfrak{p}}\right] = \sigma$ has density $1/[K:k]$ in the set of nonzero primes of k.*

Remark 3.21. In fact, despite the failure of any obvious generalization of Artin's reciprocity law in the nonabelian case, Chebotarev's density theorem actually easily extends from the abelian case to the general case of Galois extensions: if K/k is an arbitrary Galois extension, then the Artin map sends a nonzero prime of k to a certain conjugacy class of $\mathrm{Gal}(K/k)$. For any conjugacy class $\mathcal{C} \subseteq \mathrm{Gal}(K/k)$, the set of primes mapping to $\mathcal{C}$ has density $|\mathcal{C}|/[K:k]$ in the primes of k.

Proof of Theorem 3.20. When Chebotarev first proved his density theorem, the full strength of Artin reciprocity was not available to him. Instead, he had to use the cyclotomic case of the reciprocity law and build up the general case using a complicated "field crossing argument" (see my math 229x final project or [6, Ch. 6] for a complete description of this method of proof). In fact, it was by adapting the tools in Chebotarev's proof that Artin was able to prove his reciprocity law and thus Conjecture 3.13. In this proof, we will just show why it is a consequence of the full statements of class field theory, acknowledging that it doesn't need to depend on them.

By Artin reciprocity, there exists a modulus $\mathfrak{m}$ for k divisible by all primes ramifying in K such that the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$ is surjective and its kernel contains $P_\mathfrak{m}$. In particular, every character χ of $\mathrm{Gal}(K/k)$ induces a character $\chi \circ \left[\frac{K/k}{\cdot}\right]$ of the finite[11] abelian group $I(\mathfrak{m})/P_\mathfrak{m}$. For any unramified prime $\mathfrak{p}$ of k, we may compute the local factor

$$\prod_{\chi \in \widehat{\mathrm{Gal}(K/k)}} \frac{1}{1 - \chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)(\mathrm{N}\mathfrak{p})^{-s}}$$

[11] This finiteness will be important later in the proof, when we use the Artin L-functions for K/k as Hecke L-functions for a certain modulus.

of $\prod_\chi L(s, \chi \circ [\frac{K/k}{\cdot}]) = \prod_\chi L^{\text{Artin}}_{K/k}(s, \chi)$. In particular, we have[12]

$$\prod_{\chi \in \widehat{\mathrm{Gal}(K/k)}} \frac{1}{1 - \chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)(\mathrm{N}\mathfrak{p})^{-s}} = \left(\frac{1}{1 - (\mathrm{N}\mathfrak{p})^{-fs}}\right)^{[K:k]/f(\mathfrak{P}|\mathfrak{p})}$$
$$= \prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - (\mathrm{N}\mathfrak{P})^{-s}},$$

since there are exactly $[K:k]/f(\mathfrak{P}|\mathfrak{p})$ primes lying over $\mathfrak{p}$. Multiplying all these local factors together, we obtain the identity

$$\prod_{\chi \in \widehat{\mathrm{Gal}(K/k)}} L(s, \chi) \prod_{\mathfrak{p}|d_{K/k}} \prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - (\mathrm{N}\mathfrak{P})^{-s}} = \zeta_{K/k}(s)$$

for all s in the right half-plane $\Re(s) > 1$. By analytic continuation, the same is true of the meromorphic functions on both sides of the equation. Since $L(s, \chi \circ \left[\frac{K/k}{\cdot}\right])$ is the L-function associated with a Hecke character,[13], it converges on the right half-plane $\Re(s) > 1 - 1/[k/\mathbf{Q}]$ when χ is nontrivial, and otherwise has a simple pole at $s = 1$. Since $\zeta_{K/k}$ has a simple pole in the same place, it follows that $L(1, \chi \circ \left[\frac{K/k}{\cdot}\right]) \neq 0$. The conclusion follows easily from this and the representation theory of the finite abelian group $\mathrm{Gal}(K/k)$. Fix a $\sigma \in \mathrm{Gal}(K/k)$ and let $\pi(x;\sigma)$ be the number of primes of k of norm at most x whose corresponding Frobenius is

[12] The first step comes from a simple manipulation in the representation theory of finite groups. The Frobenius element $\left[\frac{K/k}{\mathfrak{p}}\right]$ has order $f_\mathfrak{p} = f(\mathfrak{P}|\mathfrak{p}) = |D_\mathfrak{P}|$ in $\mathrm{Gal}(K/k)$ for any $\mathfrak{P}|\mathfrak{p}$, since $\mathfrak{p}$ is unramified. As a result, $\chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)$ is an f-th root of unity for all $\chi \in \widehat{\mathrm{Gal}(K/k)}$. There is one character of $\langle\left[\frac{K/k}{\mathfrak{p}}\right]\rangle$ for each choice of f-th root of unity to send the generator to. Every such character extends to a character of $\mathrm{Gal}(K/k)$ in exactly $[K:k]/f$ ways, so the complex numbers $\chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)$ run over the f-th roots of unity, each with multiplicity $[K:k]/f$.

As a result, $\prod_\chi(1 - \chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)X)$ has exactly the f-th roots of unity as its roots, each root having multiplicity $[K:k]/f$. From this we obtain the polynomial identity $\prod_\chi(1 - \chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)X) = (1 - X^f)^{[K:k]/f}$, and the identity we use in the first step is obtained by substituting $(\mathrm{N}\mathfrak{p})^{-s}$ for X.

[13] This is where the finiteness of $I(\mathfrak{m})/P_\mathfrak{m}$ is used. Without the finiteness, it's impossible to extend the L-function to the left of $s = 1$.

equal to σ. Using the standard summation by parts technique,

$$\begin{aligned}
\sum_{\left[\frac{K/k}{\mathfrak{p}}\right]=\sigma} \frac{1}{(\mathrm{N}\mathfrak{p})^s} &= \int_1^\infty \frac{1}{y^s}\, d\left(\pi(y;\sigma)\right) \\
&= -s\int_1^\infty \pi(y;\sigma)y^{-s}\frac{dy}{y} \\
&= -s\int_1^\infty \left(\sum_{\chi\in\widehat{\mathrm{Gal}(K/k)}} \langle \chi, \pi(y;\cdot)\rangle \chi(\sigma)\right) y^{-s}\frac{dy}{y} \\
&= -s\int_1^\infty \left(\sum_{\chi\in\widehat{\mathrm{Gal}(K/k)}} \frac{1}{[K:k]} \sum_{\tau\in\mathrm{Gal}(K/k)} \chi(\tau)\pi(y;\tau)\overline{\chi}(\sigma)\right) y^{-s}\frac{dy}{y} \\
&= \frac{1}{[K:k]} \sum_{\chi\in\widehat{\mathrm{Gal}(K/k)}} \overline{\chi}(\sigma)\cdot(-s)\int_1^\infty \sum_{\tau\in\mathrm{Gal}(K/k)} \chi(\tau)\pi(y;\tau)y^{-s}\frac{dy}{y} \\
&= \frac{1}{[K:k]} \sum_{\chi\in\widehat{\mathrm{Gal}(K/k)}} \overline{\chi}(\sigma) \sum_{\mathfrak{p}\nmid\mathfrak{d}_{K/k}} \frac{\chi\left(\left[\frac{K/k}{\mathfrak{p}}\right]\right)}{(\mathrm{N}\mathfrak{p})^s}.
\end{aligned}$$

Taking logs of product expansions, we can reformulate this in terms of our L-functions as

$$\sum_{\left[\frac{K/k}{\mathfrak{p}}\right]=\sigma} \frac{1}{(\mathrm{N}\mathfrak{p})^s} = \frac{1}{[K:k]} \sum_{\chi\in\widehat{\mathrm{Gal}(K/k)}} \overline{\chi}(\sigma)\log L(s,\chi) + O(1).$$

We've shown that $L(s,\chi)$ converges to some finite nonzero value as $s\to 1^+$ when χ is a nontrivial character. So we can absorb the contributions of all the nontrivial characters into the error term, ultimately getting

$$\sum_{\left[\frac{K/k}{\mathfrak{p}}\right]=\sigma} \frac{1}{(\mathrm{N}\mathfrak{p})^s} = \frac{1}{[K:k]}\log L(s,1) + O(1).$$

But by the Euler product expansion, $\log L(s,1)$ is a bounded additive factor away from $\log\zeta_k(s)$ as $s\to 1^+$. This shows that indeed the Dirichlet density of the primes with Frobenius element equal to any fixed σ is $1/[K:k]$. □

Remark 3.22. Though the Chebotarev density theorem is not a direct answer to Question 3.8, it is most of the way there. The remaining ingredient is the existence theorem of class field theory, the answer to Question 3.15. A special case of the existence theorem says that there exists an abelian extension K/k such that the Artin map induces an isomorphism $I(\mathfrak{m})/P_{\mathfrak{m}} \to \mathrm{Gal}(K/k)$. In that case, the Chebotarev density theorem reduces to the desired statement that there are infinitely many prime ideals in each generalized ideal class.

Remark 3.23. The key ingredient in the proof of Theorem 3.20 was the fact that the Artin L-functions for the abelian extensions coincide with Hecke L-functions for a specific modulus. This is important because the finiteness of the generalized ideal class group implies that these L-functions actually converge on a right half-plane left of $s = 1$. The Artin L-functions (once the ramified local factors have been added in) actually do satisfy a functional equation, but it is unknown whether they always extend to a meromorphic function on the whole complex plane (this is known as *Artin's conjecture*). The convergence of Hecke L-functions (along with Artin reciprocity) settles this in the case of Artin L-functions of abelian extensions. This was the only reason we needed to pass through the machinery of Hecke L-functions and use Artin reciprocity to deduce Chebotarev's density theorem. Indeed, the Artin L-functions on their own already satisfy the general product formula

$$\zeta_K(s) = \prod_{\rho} L(s,\rho)^{\deg \rho}$$

where the product is over all irreducible representations of $\mathrm{Gal}(K/k)$.

Chebotarev's density theorem has a number of interesting consequences. First of all, if we had proved it in the historical manner without assuming Artin reciprocity, it's a trivial consequence of the theorem that the Artin map is surjective. It also contributes to the overall picture of class field theory in the following way: the class field correspondence says that an abelian extension is uniquely determined by the kernel of its Artin map. The Chebotarev density theorem implies that an abelian extension is also uniquely determined by the primes in the kernel of its Artin map.

Theorem 3.24. *Let k be a number field and K_1, K_2 abelian extensions of k. Let $\mathrm{Spl}(K_i/k)$ denote the set of primes of k which split completely in K_i. Then the following are equivalent:*

- $K_1 = K_2$.
- $\mathrm{Spl}(K_1/k)$ *and* $\mathrm{Spl}(K_2/k)$ *differ by a set of Dirichlet density zero in the primes.*

Proof. By the properties of the Artin symbol, a prime $\mathfrak{p}$ splits completely in K_1K_2 if and only if it splits completely in K_1 and in K_2. So,

$$\mathrm{Spl}(K_1K_2/k) = \mathrm{Spl}(K_1/k) \cap \mathrm{Spl}(K_2/k).$$

If the two sets on the right hand side differ by a set of Dirichlet density zero, then each of their Dirichlet densities must be the same, and this density is the same as the density of their intersection. By the Chebotarev density theorem, this means that

$$[K_1 : k] = [K_2 : k] = [K_1K_2 : k].$$

It follows that $K_1 = K_2$, as desired. □

Remark 3.25. Because of the generality in which Chebotarev's density theorem holds, the statement of Theorem 6.3 is actually true for arbitrary Galois extensions.

4. The Idèles

4.1. **Definitions.** Let k be a number field. The group of idèles of k is a locally compact topological group which is meant to contain all the information about the completions of k and the open neighborhoods of 1 in those completions. It is defined as a restricted product (rather than a direct product) in order to ensure it is locally compact. Restricted products of topological groups are defined as follows:

Definition 4.1. Let I be an index set, and $\{G_v\}_{v\in I}$ be a collection of locally compact topological groups. Suppose that for all but finitely many $v \in I$, $H_v \subseteq G_v$ is a compact open subgroup. Then the *restricted product* of the G_v's with respect to the H_v's is the set of all elements $(\alpha_v)_{v\in I} \in \prod_{v\in I} G_v$ such that $\alpha_v \in H_v$ for all but finitely many v. For any finite subset S of I containing at least all the $v \in I$ such that H_v is not defined, the restricted product contains

$$\prod_{v\in I\setminus S} H_v \times \prod_{v\in S} A_v$$

where the A_v's are arbitrary open subsets of G_v. We define the topology on the restricted direct product to have these sets as a basis of open sets.

Remark 4.2. The restricted product topology is defined the way it is in order to force it be locally compact, despite sitting inside the direct product of infinitely many locally compact groups. In particular, the H_v's are compact, and the A_v's are locally compact (but there are finitely many). So the open sets in the topology are all locally compact[14]. The opens A_v are included in order to cover the entire space (else we would have to consider just the product of the H_v's which wouldn't be as useful).

One can check that the restricted product topology defines a Hausdorff topological group structure on the idèles.

Let k be a number field. For each place v of k, we have a locally-compact completion k_v, its locally compact multiplicative group $k_v^\times$, and the compact open unit group $\widehat{\mathcal{O}}_{k,v}^\times$.

Definition 4.3. The *group of idèles* of k, which we will denote by J_k, is the restricted topological product of the $k_v^\times$ with respect to the $\widehat{\mathcal{O}}_{k,v}^\times$, which is defined for all but the archimedean places.

J_k comes with a map of sets $k^\times \to J_k$ given by $\alpha \mapsto (\alpha)_v$, which is well-defined because any $\alpha \in k^\times$ has zero $\mathfrak{p}$-adic valuation for all but finitely many $\mathfrak{p}$. The image of $k^\times$ in J_k is known as the group of *principal idèles.* Analogously to the ideal class group of k, we may mod out J_k by the principal idèles to get

Definition 4.4. The *idèle class group* of k is $C_k := J_k/k^\times$.

The idèle class group inherits its own topological group structure as a quotient of the idèles. It will turn out that C_k will coincide with certain generalized ideal

[14] The product of arbitrarily many compact sets H_v is compact by Tychonoff's theorem. Then taking the product with finitely many locally compact sets A_v keeps it locally compact: if X, Y are locally compact then we can take the sets $U \times V$ as a basis for the topology of $X \times Y$, and use the local compactness to observe that $\overline{U \times V} = \overline{U} \times \overline{V}$ is compact, from which we conclude the local compactness of $X \times Y$. Note that the product of infinitely many locally compact spaces is not necessarily locally compact.

class groups (see the next section), and since it doesn't depend on any choice of modulus it will be somewhat more convenient to use in class field theory.

Before discussing the norms on the idèles, it will be instructive to consider the simpler case of a single completion at a time.

If K/k is a finite extension of number fields, for every $v \in M_k$ there may be several $w \in M_K$ lying over v. However, if K/k is Galois, recall (e.g. from [11, Ch. II, §9]) that $\mathrm{Gal}(K/k)$ acts transitively on the valuations $w|v$, where the action is defined by $\sigma(w) = w \circ \sigma^{-1}$ (the inverse inserted to make it a valid group action). For any two $w, w'|v$, this means there is some $\tau \in \mathrm{Gal}(K/k)$ such that $w' = w \circ \tau$ and thus $D_w = \tau D_{w'} \tau^{-1}$. It follows[15] that $N_{\hat{K}_w/\hat{k}_v}(\hat{K}_w^\times)$ does not depend on the choice of $w|v$. So we may consider for each $v \in M_k$ the subgroup of $\hat{k}_v^\times$ consisting of the local norms from any of the completions lying over it.

Definition 4.5. Let $v \in M_k$. The *group of local norms* in $\hat{k}_v^\times$ is the group $N_{\hat{K}_w/\hat{k}_v}(\hat{K}_w^\times)$. By the discussion above we can use any $w|v$ to obtain it.

Remark 4.6. This norm subgroup will be important for the purposes of local class field theory. We will show using Galois cohomology that $N(K_w^\times)$ is of finite index in $k_v^\times$ when K/k is abelian. In fact, local class field theory will show that even if K/k is an arbitrary Galois extension, $N(K_w^\times)$ will always coincide with the norm subgroup of the maximal abelian subextension of K_w/k_v. So at least in the abelian case, the finiteness of the "norm index" $[k_v^\times : N(K_w^\times)]$ does not require class field theory. However, the specifics of what this index is one of the important technical issues in the proofs of class field theory, and a key step in the proof of the local reciprocity law.

Lemma 4.7. *Suppose that* $[k_v^\times : N(K_w^\times)] < \infty$. *Then actually* $N(K_w^\times)$ *is open in* $k_v^\times$. *Also,* $N(\widehat{\mathcal{O}}_{K,w}^\times)$ *is open in* $\widehat{\mathcal{O}}_{k,v}^\times$.

Proof. The second fact will be the important one in the proof. The norm is continuous with respect to w and v, so $N(\widehat{\mathcal{O}}_{K,w}^\times)$, the image of a compact set under a continuous map, is compact in the metric space k_v. So in particular it must be closed. We have an inclusion of groups

$$\widehat{\mathcal{O}}_{k,v}^\times/(N(K_w^\times) \cap \widehat{\mathcal{O}}_{k,v}^\times) \subseteq K_v^\times/N(k_w^\times),$$

and thus an inequality of norm indices

$$[\widehat{\mathcal{O}}_{K,w}^\times : N(\widehat{\mathcal{O}}_{K,w}^\times)] \leq [k_v^\times : N(K_w^\times)] < \infty.$$

So $N(\widehat{\mathcal{O}}_{K,w}^\times)$ is a finite-index closed subgroup of $\widehat{\mathcal{O}}_{K,w}^\times$. Its complement is therefore a finite union of closed subgroups, and is thus closed, which implies the desired openness of the norm subgroup. Already this openness implies that $N(K_w^\times)$ contains an open neighborhood of $1 \in k_v^\times$, and hence the whole subgroup is open, as desired. □

Remark 4.8. The lemma above assumes the finiteness of an index which comes from harder machinery like cohomology or class field theory. In fact, it's possible

[15] The elements of $\mathrm{Gal}(\hat{K}_w/\hat{k}_v)$ are just extended by continuity from the elements of D_w. The norm of an element α of $K \subseteq \hat{K}_w$ down to $\hat{k}_v$ is $\prod_{\sigma \in D_w} \sigma(\alpha) = \prod_{\sigma \in D_{w'}} \tau\sigma\tau^{-1}(\alpha) = \tau N_{\hat{K}_{w'}/\hat{k}_v}(\tau^{-1}\alpha) = N_{\hat{K}_{w'}/\hat{k}_v}(\tau^{-1}\alpha)$. Applying this equality to the Cauchy sequences defining the elements of the upstairs completions gives the equality of norm subgroups.

to conclude the openness of the norm subgroup directly: since it's a subgroup, it suffices to show that it contains an open neighborhood of 1. To get this open set, it will suffice to consider only the norms of elements already in $\hat{k}_v^\times$. The archimedean case is easy (in the only nontrivial case, we see that the positive reals are open in $\mathbf{R}^\times$). So assume that v is $\mathfrak{p}$-adic. The norm map restricts on $\hat{k}_v^\times$ to the $[k_w : k_v]$-power map. The $\mathfrak{p}$-adic logarithm gives an isomorphism (of additive and multiplicative topological groups) between a small neighborhood of 0 and a small neighborhood of 1. So it suffices to show that the multiplication by $[k_w : k_v]$ map on a small open ball around 0 in k_v hits every point in a (possibly smaller) open ball around 0. But this is evident, as $x/[k_w : k_v]$ will be in the range of the log isomorphism for sufficiently small $x \in k_v$ (it might need to be smaller to accommodate any nontrivial $\mathfrak{p}$-adic valuation of $[k_w : k_v]$).

The analysis of the norm subgroup in the local case leads up to the same analysis in the case of the idèles. We can extend the notion of the norm $K^\times \to k^\times$ to the idèles $J_K \to J_k$, and examine the norm subgroup in J_k. Once we have shown the connection between the idèle class group and the generalized ideal class group, the norm subgroups of J_k will be one of the important ingredients in global class field theory.

The Galois group $\mathrm{Gal}(K/k)$ acts on J_K by permuting transitively the completions $\hat{K}_w$ lying over the $\hat{k}_v$ (each automorphism τ induces an isomorphism $K_w \to K_{\sigma w} = K_{w \circ \sigma^{-1}}$). Specifically, if $(\alpha_v)_v$ is an idèle of K, then its image under the action of σ has $\sigma(\alpha_v) \in \hat{K}_{\sigma v}$ for its σv-component.

So we should define the norm as follows:

Definition 4.9. Let K/k be a Galois extension of number fields, and $\alpha = (\alpha_v)_v \in J_K$. Then the norm of α is $N_{K/k}(\alpha) := \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(\alpha)$.

Under this definition, $N_{K/k}(\alpha)$ is defined as an element of J_K, but for any $v \in M_k$ we expect the w-components of $N_{K/k}(\alpha)$ for $w|v$ to be related to each other. In particular, the decomposition groups D_w for $w|v$ are all conjugate to each other and have the same size, namely $|D_w| = [\hat{K}_w : \hat{k}_v] = e(w|v)f(w|v)$. For all $w, w'|v$, by the orbit-stabilizer theorem, there are therefore exactly $|D_w|$ elements of $\mathrm{Gal}(K/k)$ sending w' to w. We can write down exactly what these are in terms of the decomposition group and a single automorphism sending w' to w, to observe that the w-component of $N_{K/k}(\alpha)$ has a contribution from each valuation $w'|v$ such that $w' = \tau w$ lying over v equal to

$$\prod_{\substack{\sigma \in \mathrm{Gal}(K/k) \\ \sigma w' = w}} \sigma(\alpha_{w'}) = \prod_{\sigma \in D_w} \sigma\tau(\alpha_{w'}) = \prod_{\sigma \in D_{w'}} \tau\sigma(\alpha_{w'}) = \tau N_{\hat{K}_w/\hat{k}_v}(\alpha_{w'}) = N_{\hat{K}_{w'}/\hat{k}_v}(\alpha_{w'}).$$

It follows that the w-components of $N_{K/k}(\alpha)$ coincide for all $w|v$ and are equal to

$$\prod_{w|v} N_{\hat{K}_w/\hat{k}_v}(\alpha_w).$$

So in fact the idèle norm is naturally a homomorphism of groups $J_K \to J_k$ just by keeping only one of the $w|v$-components for each v, equivalently defined in the following way:

Definition 4.10. The norm down to J_k of an idèle $\alpha = (\alpha_v)_v \in J_K$ is the element of J_k whose v-component is $\prod_{w|v} N_{\hat{K}_w/\hat{k}_v}(\alpha_w)$.

Definition 4.9 will be useful because it defines the norm directly in terms of the action of $\mathrm{Gal}(K/k)$ on J_K. This will be useful especially in the use of Galois cohomology to study the norm subgroup of J_K in J_k. But oftentimes Definition 4.10 is slightly more convenient since it doesn't require keeping track of the switching between different valuations extending v.

The norm is in fact a continuous homomorphism of topological groups. The extra fact that it is continuous is not very hard: we need to check that every element of the basis of open sets of J_k has open preimage under $N_{K/k} : J_K \to J_k$. Because of the way the basis of open sets is defined, and the fact that the norm of a unit is always a unit, it suffices to show that open subsets of $\hat{k}_v$ have open preimages under the map $\prod_{w|v} \hat{K}_w \to \hat{k}_v$ given by $(\alpha_w)_w \mapsto \prod_{w|v} N_{\hat{K}_w/\hat{k}_v}(\alpha_w)$. This is clear because this is a pointwise product of the maps that take the norm of one coordinate. Pointwise products of continuous maps of topological groups are continuous, and the norms are each continuous in the coordinate they act on (and thus on the whole product if they leave the other coordinates alone). The norm subgroup $N(J_K) \subseteq J_k$ will be of great importance to class field theory (in idèlic language, the class field correspondence says that the abelian extensions of k correspond exactly with the open subgroups of $J_k/k^\times$ via the norm map).

We can also check using [11, Ch. II, (8.4)] that the notation $N_{K/k}$ means the same thing for elements of J_K and for $K^\times$, in that for $\alpha \in K^\times$ the idèle norm coincides with the field norm.

As expected, we have a result on the norm subgroup of J_k.

Lemma 4.11. *$N(J_K)$ is open in J_k.*

Proof. The norm of J_K is just the union of the norms of the open sets

$$J_{K,S} = \prod_{w \in M_K \setminus S} \widehat{\mathcal{O}}_{K,w}^\times \times \prod_{w \in S} K_w$$

over all finite subsets $S \subset M_k$ containing the archimedean places. We can also choose S so that for any $v \in M_k$, it either contains all $w|v$ or none of them[16]. Now we specifically make use of Definition 4.10. As a result of that definition and the fact that the norm subgroup (for either the local field or the units of its valuation ring) doesn't depend on the choice of $w|v$,

$$N(J_{K,S}) = \prod_v N(\widehat{\mathcal{O}}_{K,w}^\times) \times \prod_v N(K_w),$$

where the first product is over all but finitely many v and the second product is over the remaining ones. To conclude that $N(J_{K,S})$ is open, as a result of Lemma 4.7, we just need to show that $N(\widehat{\mathcal{O}}_{K,w}^\times) = \widehat{\mathcal{O}}_{k,v}^\times$ for all but finitely many v. In fact, this is true whenever v is unramified in K, which we will show via group cohomology. This is also an easy consequence of Hensel's lemma (see [9, hensel]). □

A key fact in the class field correspondence will be that in fact **all** the open subgroups of $J_k/k^\times$ are obtained by taking norms from the idèles of some finite abelian extension K/k. It is part of the main goal of class field theory to show that the quotient group is in fact isomorphic to $\mathrm{Gal}(K/k)$. In this section, we'll be able to see that any open subgroup of C_k has finite index. Unlike in the case of the adeles, it isn't true that C_k is compact.

[16] this choice is convenient but obviously not necessary

Lemma 4.12. *The idèle class group of k is not compact.*

Proof. Recall the product formula for normalized valuations, which says that for any $\alpha \in k^\times$,

$$\prod_{v \in M_k} |\alpha|_v = 1.$$

In general, we may define the absolute value homomorphism (I use this name to distinguish it from the norm $J_K \to J_k$) $|\cdot| : J_k \to \mathbf{R}^\times_{\geq 0}$ given by

$$|(\alpha_v)_v| = \prod_{v \in M_k} |\alpha_v|_v.$$

This is well-defined because $|\alpha_v|_v = 1$ for cofinitely many valuations v by definition of J_k. The product formula shows that the absolute value homomorphism is trivial on $k^\times \subset J_k$, so it projects to a homomorphism $C_k \to \mathbf{R}^\times_{\geq 0}$. First, $|\cdot|$ is obviously surjective (fix all coordinates but one corresponding to an archimedean valuation). It is also continuous as a map of topological groups, even as defined on the idèles. The trick is the same as the one for checking that the pointwise product of finitely many continuous maps is continuous. It suffices to check that it is continuous on each open subset $J_{k,S} = \prod_{v \in M_k \setminus S} \widehat{\mathcal{O}}^\times_{k,v} \times \prod_{v \in S} k_v^\times$ for finite sets S of places including all the archimedean ones. But $|\cdot|$ restricts on $J_{k,S}$ to a finite product of absolute values with respect to the $v \in S$. Moreover, $|\cdot|_v : k_v^\times \to \mathbf{R}^\times_{\geq 0}$ is always continuous[17] so $|\cdot| : J_{k,S} \to \mathbf{R}^\times_{\geq 0}$ can be written as the composition

$$J_{k,S} \to (\mathbf{R}^\times_{>0})^{|S|} \to \mathbf{R}^\times_{>0},$$

where the first map is into each coordinate via $|\cdot|_v$ and the second map is just multiplying all the coordinates together. Both are continuous (the first is a fact about continuous maps and direct products, the second is the definition of a topological group). Since the $J_{k,S}$ are an open cover for J_k and continuity is a local property, we have concluded that $|\cdot| : J_k \to \mathbf{R}^\times_{>0}$ is continuous. But the continuous image of a compact space is compact, which $\mathbf{R}^\times_{>0}$ is not. So J_k and even C_k is not compact. □

That being said, it turns out that the possibility of all values of $\mathbf{R}^\times_{\geq 0}$ is the only obstruction to $J_k/k^\times$ being compact.

Proposition 4.13. *Let C_k^0 be the set of idèle classes of absolute value zero, i.e. $C_k^0 = \ker|\cdot|$. Then C_k^0 is compact, and there is an isomorphism of topological groups $C_k \cong \mathbf{R}^\times_{>0} \times C_k^0$.*

Proof. The main point of this fact is its reliance on the geometry of numbers (in fact it is easy to deduce the unit theorem from the statement; we will do this in the next subsection). Fix a positive real number λ and idèle class $[a] \in C_k$ with $|a| = \lambda$. The goal is to find a representative a of $[a]$ such that each coordinate of a has absolute value in some compact set depending only on λ. To do this we must multiply a by a suitable element $\alpha_a \in k^\times$ (which is allowed to depend on a). It suffices to ensure that $|\alpha_a a|_v$ is bounded above and below over all $v \in M_k$ and

[17] The continuity is a general fact about metric spaces. By the triangle inequality, $|x-y|_v < \epsilon \implies ||x|_v - |y|_v| \leq |x-y|_v < \epsilon$.

$a \in J_k$ of norm λ. Isolating α_a, to get a lower bound $|\alpha_a a|_v \geq 1$ for example, we need to choose $\alpha_a \in k^\times$ such that

$$|\alpha_a^{-1}|_v \leq |a_v|_v.$$

for all v[18] The condition at the nonarchimedean places $v_\mathfrak{p}$ means that we restrict α_a^{-1} to be in the fractional ideal $I_a = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a_{v_\mathfrak{p}})}$. At the archimedean places, the requirement is that under the embedding $k \to \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ coming from the archimedean places, α_a^{-1} is inside a box of volume

$$\prod_{v \in S_\infty} |a_v|_v = \frac{\prod_{v \in M_k} |a_v|_v}{\prod_\mathfrak{p} |a_{v_\mathfrak{p}}|_{v_\mathfrak{p}}} = \frac{\lambda}{\prod_\mathfrak{p} (\mathrm{N}\mathfrak{p})^{-v_\mathfrak{p}(a_{v_\mathfrak{p}})}} = \lambda \frac{\operatorname{covol}(I_a)}{\operatorname{covol}(\mathcal{O}_k)}$$

where $\operatorname{covol}(\Lambda)$ denotes the covolume of a lattice Λ embedded in $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$. By Minkowski's theorem, for sufficiently large λ (where how large depends only on k and not on a, since the factor of $\operatorname{covol}(I_a)$ coincides with the one in the numerator of the volume bound in the theorem), we know there exists a nonzero $\alpha \in k^\times$ such that $|\alpha^{-1}|_v \leq |a_v|_v$ for all $v \in M_k$. In other words, if λ is selected sufficiently large, then any $a \in J_k$ of absolute value λ has some $\alpha_a \in k^\times$ such that

$$|\alpha_a a|_v \geq 1$$

for all $v \in M_k$. Actually, this inequality is already enough to force the absolute values of $\alpha_a a$ to all be bounded above by λ, since $\prod_v |\alpha_a a|_v = \lambda$. So we have concluded that if λ is chosen sufficiently large, every $[a] \in C_k$ of absolute value λ has a representative $b \in J_k$ for which $1 \leq |b_v|_v \leq \lambda$ for each $v \in M_k$. Recall that the nonarchimedean absolute values are normalized in such a way that the smallest possible value of $|\cdot|_\mathfrak{p}$ greater than 1 is $\mathrm{N}\mathfrak{p}$. But there are only finitely many primes $\mathfrak{p}$ with norm less than λ (every such $\mathfrak{p}$ must be a divisor of $\lambda \cdot \mathcal{O}_k$), which means that there is a finite set $S \subseteq M_k$ which only depends on k for which our representative b is guaranteed to satisfy $|b_v|_v = 1$ for all $v \in M_k \setminus S$.[19] In particular every idèle class of norm λ has a representative in the compact set

$$X = \prod_{v \in S} \{x \in k_v : 1 \leq |x|_v \leq \lambda\} \times \prod_{v \in M_k \setminus S} \widehat{\mathcal{O}})k, v^\times \subseteq J_k.$$

The fact that every idèle class of absolute value λ has a representative in X means that for the subset $A_\lambda \subseteq J_k$ consisting of all idèles of absolute value λ, the projection $A \to J_k/k^\times = C_k$ has image equal to the image of X. Since X is compact, and the projection is continuous (C_k is given the quotient topology), we know that the image of X is compact. That image contains all the idèle classes of absolute value λ, the set of which is closed (it is the preimage of the closed set $\{\lambda\}$ under the continuous absolute value map). So the set of idèle classes of absolute value λ is indeed compact.

But we cannot just set $\lambda = 1$, since our argument works only for sufficiently large λ, depending on k. This is fine, since there is a topological isomorphism between the set of idèle classes of absolute value λ and C_k^0 given by multiplying by some fixed choice of idèle a_λ of absolute value λ. It's clearly invertible (with inverse a_λ^{-1}),

[18] The subscripts might be confusing here. The subscript a on α emphasizes that α depends on the idèle a. The subscript v on a refers to the v-coordinate of a.

[19] A priori we always had such a set S by virtue of b being an idèle, but it wasn't clear that it can't grow without bound depending on the value of a and the choice of α.

and for that reason bicontinuous. So the compactness we proved readily implies the compactness of C_k^0. □

Corollary 4.14. *Every open subgroup of C_k has finite index.*

Proof. From what we've shown, each element of C_k is determined by its absolute value and an element of C_k^0. So we have an isomorphism of topological groups

$$C_k^0 \times \mathbf{R}_{>0}^\times \cong C_k$$

which may explicitly be given by

$$(a, \lambda) \mapsto a \cdot [b_\lambda],$$

where b_λ is a choice of idèle of absolute value λ which varies continuously with λ. For instance, k has at least one infinite place v_∞, so we can set b_λ to have v_∞-coordinate equal to λ and all the other coordinates equal to 1 ($\lambda \mapsto b_\lambda$ is clearly continuous). Then $(a, \lambda) \mapsto a \cdot [b_\lambda]$ is clearly a continuous homomorphism of topological groups. It has an inverse given by

$$[a] \mapsto (a \cdot b_{|a|}^{-1}, b_{|a|})$$

which is continuous by the same type of reasoning with topological groups and the fact that $a \mapsto |a|$ is continuous. Armed with the isomorphism $C_k^0 \times \mathbf{R}_{>0}^\times \cong C_k$, we can see that every open subgroup G of C_k is a union of sets of the form $U \times V$ where U and V are open subgroups of C_k^0 and $\mathbf{R}_{>0}^\times$, respectively. But the only open subgroup of $\mathbf{R}_{>0}^\times$ is itself, and C_k^0 is compact so U has finite index in it. It follows that the index of G in C_k is the same as the index of U in C_k^0 and is in particular finite, as desired. □

With this chain of results about the idèle class group, we've caught a glimpse of what class field theory will later tell us remarkably specific information about. The open subgroups all have finite index because by the existence theorem, they are the norm subgroups of finite abelian extensions K/k, whose norm subgroup has quotient $C_k/N(C_K) \cong \mathrm{Gal}(K/k)$ which is finite.

4.2. Idèle classes and generalized ideal classes.

The construction of the idèles of k gives them a natural relationship with the fractional ideals of k. In particular, by unique factorization a fractional ideal can be described by a choice of integer valuations at finitely many primes. So we have a well-defined group homomorphism

$$\psi : J_k \to I_k$$

given by

$$(a_v)_v \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(a_v)}.$$

Note that ψ doesn't depend at all on the archimedean places. It is clearly surjective by definition of J_k, and its kernel is just the set of elements with arbitrary valuations at the archimedean places and zero valuation everywhere else, i.e. the open set

$$\ker \psi = J_{k,S_\infty} := \prod_{v \in M_k \setminus S_\infty} \widehat{\mathcal{O}}_{k,v}^\times \times \prod_{v \in S_\infty} k_v^\times.$$

So ψ induces an isomorphism of abelian groups

Lemma 4.15. $J_k/J_{k,S_\infty} \cong I_k$.

We will play the game of successively restricting and/or quotienting to see what isomorphisms we can induce between further quotients of (subgroups) of $J_k/J_{k,S_\infty}$ and ideal groups, eventually arriving at the desired connection between C_k and $I(\mathfrak{m})/P_\mathfrak{m}$ for admissible moduli $\mathfrak{m}$ of k.

Lemma 4.16. $J_k/k^\times J_{k,S_\infty} \cong I_k/P_k$.

Proof. We already know the map $\psi : J_k \to I_k$ is surjective. It suffices to compute $\psi^{-1}(P_k)$. We claim that it is equal to $k^\times J_{k,S_\infty}$. The inclusion $k^\times J_{k,S_\infty} \subseteq \psi^{-1}(P_k)$ is clear (by definition of the $\mathfrak{p}$-adic valuations, any $\alpha \in k^\times$ maps under ψ to $\alpha\mathcal{O}_k \in P_k$; as we saw before, J_{k,S_∞} maps to the trivial principal ideal $1 \cdot \mathcal{O}_k$). On the other hand, let $a \in \psi^{-1}(P_k)$. Then $\psi(a) = (\alpha)$ for some $\alpha \in k^\times$, and thus $\psi(\alpha^{-1}a) = 1$. It follows that $\alpha^{-1}a \in \ker\psi = J_{k,S_\infty}$, and thus $a \in k^\times J_{k,S_\infty}$, proving the remaining inclusion. □

Lemma 4.17. *For all sufficiently large finite set $S \subseteq M_k$ containing S_∞ (with the size of S depending on k), we have $k^\times J_{k,S} = J_k$.*

Proof. If S contains S_∞, we know $J_{k,S} \supseteq J_{k,S_\infty}$ and thus $J_k/k^\times J_{k,S}$ can be identified with a quotient of the finite group I_k/P_k. We just need to make sure that for any such S, if $k^\times J_{k,S} \neq J_k$, then by augmenting S to some larger finite set $S' \supset S$, we can always get $k^\times J_{k,S'}$ to strictly contain $k^\times J_{k,S}$. It's a typical theme that actually thinking about the groups $k^\times J_{k,S}$ is too difficult. Instead, just think about $J_{k,S'}$ large enough that $k^\times$ doesn't matter.

Suppose there is an idèle $a \in J_k$ which is not in $k^\times J_{k,S}$. Then by enlarging S to include all places where a is not a unit in the valuation ring, we guarantee that $J_{k,S'} \supsetneq k^\times J_{k,S}$ and thus $k^\times J_{k,S'} \supsetneq k^\times J_{k,S}$. Inductively augmenting S and using the finiteness of I_k/P_k tells us that eventually $J_k/k^\times J_{k,S}$ is trivial and thus $J_k = k^\times J_{k,S}$ for large enough finite S. □

This lemma is a useful consequence which will come up later, but for now we return to the generalized ideal class group. We just achieved the ideal class group I_k/P_k as a group of idèle classes. The goal of the next part of this section will be to achieve $I(\mathfrak{m})/P_\mathfrak{m}$ and its quotient $I(\mathfrak{m})/P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})$ as quotients of C_k. This will allow us to translate between the ideal-theoretic and idèlic statements of class field theory.

The most obvious first step (one we will need to modify slightly to get things to work) would be to consider the surjective map $J_k(\mathfrak{m}) \to I(\mathfrak{m})$ induced from ψ by restriction, where $J_k(\mathfrak{m})$ is defined by

Definition 4.18. Let $J_k(\mathfrak{m})$ denote the subset of idèles $a \in J_k$ such that $v(a_v) = 0$ whenever $v|\mathfrak{m}_0$.

All the isomorphisms we find are only algebraic and not topological, since the generalized ideal class group comes with no natural topology.

Lemma 4.19. *ψ induces an isomorphism $J_k(\mathfrak{m})/J_{k,S_\infty} \cong I(\mathfrak{m})$*

Proof. By Lemma 4.15, the kernel of the surjective map $\psi : J_k(\mathfrak{m}) \to I(\mathfrak{m})$ is $J_k(\mathfrak{m}) \cap J_{S_\infty}$. But $J_{S_\infty} \subseteq J_k(\mathfrak{m})$ by definition, so the kernel is still just J_{S_∞}. □

Lemma 4.20. *ψ induces an isomorphism $J_k(\mathfrak{m})/k_\mathfrak{m} J_{k,S_\infty} \cong I(\mathfrak{m})/P_\mathfrak{m}$.*

Proof. It suffices to show that $\psi^{-1}(P_{\mathfrak{m}}) = k_{\mathfrak{m}} J_{k,S_\infty}$. The inclusion $k_{\mathfrak{m}} J_{k,S_\infty} \subseteq \psi^{-1}(P_{\mathfrak{m}})$ is obvious. On the other hand, suppose $a \in J_k(\mathfrak{m})$ such that $\psi(a) \in P_{\mathfrak{m}}$. Then $\psi(a) = (\alpha)$ for some $\alpha \in k_{\mathfrak{m}}$, so $\psi(\alpha^{-1}a) = 1$, which means $\alpha^{-1}a \in \ker\psi = J_{k,S_\infty}$ and thus $a \in k_{\mathfrak{m}} J_{k,S_\infty}$ as desired. □

To establish $I(\mathfrak{m})/P_{\mathfrak{m}}$ as a quotient of $J_k/k^\times$, the only thing we can do is consider the map $J_k(\mathfrak{m}) \to J_k/k^\times$ induced by the inclusion $J_k(\mathfrak{m}) \to J_k$.

Lemma 4.21. $J_k(\mathfrak{m})/k(\mathfrak{m}) \cong J_k/k^\times$.

Proof. It suffices to prove that the induced map $\tilde{\iota} : J_k(\mathfrak{m}) \to J_k/k^\times$ is surjective (the kernel of the map is clearly $k^\times \cap J_k(\mathfrak{m}) = k(\mathfrak{m})$). Let $a \in J_k$. By the weak approximation theorem, there exists $\alpha \in k^\times$ such that

$$\left|\alpha - \frac{1}{a_v}\right|_v < \frac{1}{|a_v|_v}$$

for all $v|\mathfrak{m}_0$. Then $|\alpha a_v - 1|_v < 1$ for all such v, from which it follows that $\alpha a_v \in \widehat{\mathcal{O}}_{k,v}^\times$ for all $v|\mathfrak{m}_0$, i.e. $\alpha a_v \in J_k(\mathfrak{m})$. This means $[a] = [\alpha a_v]$ is in the preimage of $\tilde{\iota}$, as desired. □

The problem now is that there is no obvious way to write $I(\mathfrak{m})/P_{\mathfrak{m}} \cong J_k(\mathfrak{m})/k_{\mathfrak{m}} J_{k,S_\infty}$ as a quotient of $J_k/k^\times \cong J_k(\mathfrak{m})/k(\mathfrak{m})$. The trick is to consider $J_{\mathfrak{m}}$ instead of $J(\mathfrak{m})$.

Definition 4.22. Let $J_{\mathfrak{m}}$ be the set of idèles a of k such that a_v is in the open set specified by m for all $v|\mathfrak{m}$. Specifically, $v_{\mathfrak{p}}(1 - a_{v_{\mathfrak{p}}}) > m(\mathfrak{p})$ for all $\mathfrak{p}|\mathfrak{m}_0$ and $v(a_v) > 0$ for all $v|\mathfrak{m}_\infty$.

Lemma 4.23. *The inclusion $J_{\mathfrak{m}} \to J_k$ induces an isomorphism $J_{\mathfrak{m}}/k_{\mathfrak{m}} \to J_k/k^\times$.*

Proof. The proof is essentially the same as that of Lemma 4.21. Since $k^\times \cap J_{\mathfrak{m}} = k_{\mathfrak{m}}$ by definition, it suffices to show the inclusion $J_{\mathfrak{m}} \to J_k$ induces a surjective map $J_{\mathfrak{m}} \to J_k/k^\times$. Let $a \in J_k$, and by weak approximation choose $\alpha \in k^\times$ such that

$$v_{\mathfrak{p}}\left(\alpha - \frac{1}{a_{v_{\mathfrak{p}}}}\right) > m(\mathfrak{p}) - v_{\mathfrak{p}}(a_{v_{\mathfrak{p}}}).$$

for all $\mathfrak{p}|\mathfrak{m}_0$ and

$$\left|\alpha - \frac{1}{a_v}\right|_v < \frac{1}{|a_v|_v}$$

for all $v|\mathfrak{m}_\infty$. The condition at the archimedean places implies that

$$v_{\mathfrak{p}}(\alpha a_{v_{\mathfrak{p}}} - 1) > m(\mathfrak{p}),$$

and the condition at the infinite places implies that $|\alpha a_v|_v > 0$ at all $v|\mathfrak{m}_\infty$. This means every element of $J_k/k^\times$ has a representative in J_m, as desired. □

We also get an analogue to Lemma 4.20. We use the following shorthand:

Definition 4.24. Let $W_{\mathfrak{m}}$ be the open subset of $J_{\mathfrak{m}}$ given by

$$W_{\mathfrak{m}} = \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 + \mathfrak{p}^{m(\mathfrak{p})} \widehat{\mathcal{O}}_{k,v}) \times \prod_{v|\mathfrak{m}_\infty} \mathbf{R}_{>0}^\times \times \prod_{v \nmid \mathfrak{m}} \widehat{\mathcal{O}}_{k,v}^\times.$$

Lemma 4.25. $\psi : J_k \to I_k$ *induces an isomorphism* $J_{\mathfrak{m}}/W_{\mathfrak{m}} \cong I(\mathfrak{m})$.

Proof. We obviously have $\psi(J_{\mathfrak{m}}) = I(\mathfrak{m})$. On the other hand, the kernel of the restriction of ψ to $J_{\mathfrak{m}}$ is $J_{k,S_\infty} \cap J_{\mathfrak{m}}$, which is $W_{\mathfrak{m}}$ by definition. □

Lemma 4.26. *$\psi : J_k \to I_k$ induces an isomorphism $J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m}$.*

Proof. It suffices to show that $\psi^{-1}(P_\mathfrak{m}) = k_\mathfrak{m}W_\mathfrak{m}$. The inclusion $\psi^{-1}(P_\mathfrak{m}) \supseteq k_\mathfrak{m}W_\mathfrak{m}$ is clear from the definitions. On the other hand, let $a \in J_\mathfrak{m}$ such that $\psi(a) = (\alpha)$ where $\alpha \in k_\mathfrak{m}$. The $\psi(\alpha^{-1}a) = 1$ which means that $\alpha^{-1}a \in \ker(\psi|_{J_\mathfrak{m}}) = W_\mathfrak{m}$ by the previous lemma. □

Now our situation is much better. We have $I(\mathfrak{m})/P_\mathfrak{m} \cong J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m}$, and $J_\mathfrak{m}/k_\mathfrak{m} \cong J_k/k^\times$, so since the second isomorphism is induced by the natural inclusion we have the desired result:

Lemma 4.27. *$J_k/k^\times W_\mathfrak{m} \cong J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m}$.*

Proof. The isomorphism $J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m} \to I(\mathfrak{m})/P_\mathfrak{m}$ has already been described. Because of how the isomorphism $J_\mathfrak{m}/k_\mathfrak{m} \to J_k/k^\times$ is defined, subgroup $W_\mathfrak{m} \subseteq J_\mathfrak{m}/k_\mathfrak{m}$ corresponds under this isomorphism to the subgroup $W_\mathfrak{m} \subseteq J/k^\times$. So when we mod out by this subgroup we get the desired isomorphism $J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m} \to J_k/k^\times W_\mathfrak{m}$. Indeed, if ι is the inclusion $J_\mathfrak{m} \to J_k$, then $\iota^{-1}(k^\times W_\mathfrak{m}) = k^\times W_\mathfrak{m} \cap J_\mathfrak{m} = k_\mathfrak{m}W_\mathfrak{m}$ is clear. □

Remark 4.28. The isomorphism $J_k/k^\times W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m}$ offers a new proof of the finiteness of $I(\mathfrak{m})/P_\mathfrak{m}$ in light of Corollary 4.14.

Remark 4.29. Getting from an element of $J_k/k^\times W_\mathfrak{m}$ to an element of $I(\mathfrak{m})/P_\mathfrak{m}$ uses the approximation theorem to first pull back to $J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m}$. So the ideal class corresponding to an idèle class without the knowledge of a representative in $J_\mathfrak{m}$ is not convenient to describe.

Remark 4.30. Lemma 4.27 gives an expression for $I(\mathfrak{m})/P_\mathfrak{m}$ as a quotient of C_k by an open subgroup. As a result, the idèlic statement of the existence theorem proves the existence of a class field corresponding to the ray class group modulo $\mathfrak{m}$.

To use the idèles to do class field theory, recall from Theorem 3.18 that we'll need to write $I(\mathfrak{m})/P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})$ as a quotient of C_k as well. We've done this for $I(\mathfrak{m})/P_\mathfrak{m}$ already, so it suffices to see what $\mathfrak{N}(\mathfrak{m})$ corresponds to under the isomorphism of Lemma 4.27. The key idea is that if $\alpha \in K_w^\times$ for $w|v$, then

$$w(N\alpha) = [K : k]w(\alpha) = \frac{[K : k]}{e} = f(w|v),$$

so the norm of an idèle corresponds to the norm of the corresponding ideal. First, we go from $I(\mathfrak{m})/P_\mathfrak{m}$ to $J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m}$.

Lemma 4.31. *Let K/k be a Galois extension of k. Then $I(\mathfrak{m})/P_\mathfrak{m}\mathfrak{N}(\mathfrak{m}) \cong J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m}N_{K/k}J_K(1, \mathfrak{m})$ where $J_K(1, \mathfrak{m})$ is the subgroup of idèles of K consisting of elements whose v-coordinates are all 1 at $v|\mathfrak{m}$.*

Proof. The point of the notation $J_K(1, \mathfrak{m})$ is just that the values at $v|\mathfrak{m}$ should all be trivial since the norms on the ideal side of things are only for ideals coprime to $\mathfrak{m}$. It suffices to show that

$$\psi^{-1}(P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})) = k_m W_m N_{K/k}J_K(1, \mathfrak{m}).$$

The inclusion of the right hand side into the left we have already shown for $k_\mathfrak{m}$ and $W_\mathfrak{m}$. It's also obvious for $N_{K/k}J_K(1, \mathfrak{m})$, since the v-coordinate of any $a \in N_{K/k}J_K(1, \mathfrak{m})$ has $v(a_v) = 0$ whenever $v|\mathfrak{m}$ and $f(w|v)$ divides $v(a_v)$ for all v. It suffices now to prove the other inclusion. Let $a \in J_\mathfrak{m}$ such that $\psi(a) = (\alpha)\prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})n_\mathfrak{p}}$, where $\alpha \in k_{\mathfrak{m}}$ and the $n_{\mathfrak{p}}$ are arbitrary integers all but finitely many of which are zero (all norms of fractional ideals of K prime to $\mathfrak{m}$ are of this form by definition of the ideal norm). Then

$$\psi(\alpha^{-1}a) = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})n_{\mathfrak{p}}}.$$

For each prime $\mathfrak{p}$ not dividing $\mathfrak{m}$ and exactly one $\mathfrak{P}|\mathfrak{p}$, define the idèle $A \in J_K(1, \mathfrak{m})$ to have $v_{\mathfrak{P}}$-coordinate equal to an arbitrary element of $K_{\mathfrak{P}}$ with $\mathfrak{P}$-adic valuation equal to $n_{\mathfrak{p}}$. At all the other $\mathfrak{P}|\mathfrak{p}$ and in fact all other absolute values, take A to have coordinate 1. Then $N_{K/k}A$ has v-coordinate 1 except for when $v = v_{\mathfrak{p}}$ for some $\mathfrak{p}$ not dividing $\mathfrak{m}$. In that case, the $\mathfrak{p}$-adic valuation of the $v_{\mathfrak{p}}$-coordinate is $f(\mathfrak{P}|\mathfrak{p})n_{\mathfrak{p}}$. In particular,

$$\psi(N_{K/k}A) = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})n_{\mathfrak{p}}} = \psi(\alpha^{-1}a),$$

which means $N_{K/k}A$ and a differ by an element of $\ker \psi = W_{\mathfrak{m}}$. As a result, $a \in k_{\mathfrak{m}} W_{\mathfrak{m}} N_{K/k} J_K(1, \mathfrak{m})$ as desired. □

Checking what this corresponds to in $J_k/k^\times$ ends up not being very complicated so long as $\mathfrak{m}$ is admissible. Recall the definition:

Definition 4.32. $\mathfrak{m}$ is *admissible* with respect to K/k if $W_{\mathfrak{m}} \subseteq N_{K/k}J_K$.

Lemma 4.33. *If $\mathfrak{m}$ is admissible for K/k, then*

$$J_k/k^\times N_{K/k}J_K \cong J_{\mathfrak{m}}/k_{\mathfrak{m}}W_{\mathfrak{m}}N_{K/k}J_K(1, \mathfrak{m}) \cong I(\mathfrak{m})/P_{\mathfrak{m}}.$$

Proof. It suffices to show that $k^\times N_{K/k}J_K \cap J_{\mathfrak{m}} = k_{\mathfrak{m}}W_{\mathfrak{m}}N_{K/k}J_K(1, \mathfrak{m})$. From the fact that $W_{\mathfrak{m}}$ is admissible, the inclusion of the right hand side into the left hand is obvious. For the other, we use the fact from the previous lemma that $k_{\mathfrak{m}}W_{\mathfrak{m}}N_{K/k}J_K(1, \mathfrak{m}) = \psi^{-1}(P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}))$. So it suffices to show that

$$\psi(k^\times N_{K/k}J_K \cap J_{\mathfrak{m}}) \subseteq P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}).$$

Let $\alpha N_{K/k}a \in k^\times N_{K/k}J_K$. By the approximation theorem, choose $\beta \in K^\times$ so that β is very close to a_w for each $w|v$ with $v|\mathfrak{m}$. In particular, recall that for each $v \in M_k$ the map $\prod_{w|v} K_w^\times \to k_v^\times$ given by taking products of norms is continuous. So by taking β sufficiently close to a_w for each $w|v$, we can guarantee that $|N_{K/k}\beta - N_{K/k}a|_v < \min\left(\frac{\mathrm{N}\mathfrak{p}^{-m(\mathfrak{p})}}{|\alpha|_v}, |N_{K/k}a|_v\right)$ when $v|\mathfrak{m}_0$, and $|N_{K/k}\beta - N_{K/k}a|_v < |N_{K/k}a|_v$ when $v|\mathfrak{m}_\infty$.

Then for each $\mathfrak{p}$-adic $v|\mathfrak{m}_0$, we have $|\alpha N_{K/k}\beta - \alpha N_{K/k}a|_v < \mathrm{N}\mathfrak{p}^{-m(\mathfrak{p})}$, i.e.

$$v_{\mathfrak{p}}(\alpha N_{K/k}\beta - \alpha N_{K/k}a) > m(\mathfrak{p}). \tag{4.34}$$

Similarly, for $v|\mathfrak{m}_0$ our construction of β guarantees that

$$|\alpha N_{K/k}\beta - \alpha N_{K/k}a|_v < |\alpha N_{K/k}a|_v. \tag{4.35}$$

It follows from (4.34), (4.35) and the fact that $\alpha N_{K/k}a \in J_{\mathfrak{m}}$ that $\alpha N_{K/k}\beta \in k_{\mathfrak{m}}$. It also follows (this time from $|N_{K/k}\beta - N_{K/k}a|_{\mathfrak{p}} < |N_{K/k}a|_{\mathfrak{p}}$) that $v_{\mathfrak{p}}(N_{K/k}\beta) = v_{\mathfrak{p}}(N_{K/k}a_{v_{\mathfrak{p}}})$ for all $\mathfrak{p}|\mathfrak{m}_0$, so that $(N_{K/k}\beta^{-1})\psi(N_{K/k}a) = \psi(N_{K/k}\beta^{-1}a) \in \mathfrak{N}(\mathfrak{m})$. As a result,

$$\psi(\alpha N_{K/k}a) = \psi(\alpha N_{K/k}\beta)\psi(N_{K/k}\beta^{-1}a) \in P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$$

as desired. □

Remark 4.36. As usual, our isomorphism between the relevant group $I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ from class field theory and the quotient $J_k/k^\times N_{K/k}J_K$ depends on the approximation theorem to get from an idèle class to an ideal class. So when an idèle class is not already represented by an element of $J_{\mathfrak{m}}$, it isn't immediately evident what the corresponding ideal class is.

Remark 4.37. Lemma 4.33 is particularly convenient because it allows one to state the results of class field theory without the use of a specific modulus of K. It is valid as long as $\mathfrak{m}$ is admissible, but in fact this condition is true for many values of $\mathfrak{m}$. We will show in the next section using group cohomology that if v is unramified in K, then $\widehat{\mathcal{O}}_{k,v}^\times = N_{K/k}\widehat{\mathcal{O}}_{k,w}^\times$. So in fact $\mathfrak{m}$ is admissible if and only if the ramified places $v \in M_k$ have the property that $1 + \mathfrak{p}^{m(\mathfrak{p})}\widehat{\mathcal{O}}_{k,v} \subseteq N_{K_w/k_v}\widehat{\mathcal{O}}_{K,w}^\times$ when v is $\mathfrak{p}$-adic and $\mathbf{R}_{>0}^\times \subseteq N_{K_w/k_v}K_w^\times$ when v is archimedean. Recall from Lemma 4.7 and the remarks following it that $N_{K_w/k_v}K_w^\times$ is an open subset of $k_v^\times$ containing 1. So each of these norm subgroups contain an open ball around 1. For each ramified prime $\mathfrak{p}|d_{K/k}$, this means there is a minimal nonnegative integer $m_0(\mathfrak{p})$ [for all we know at the moment it could still be zero and in fact all the units are still local norms] such that $1+\mathfrak{p}^{m(\mathfrak{p})}\widehat{\mathcal{O}}_{k,v} \subseteq N_{K_w/k_v}\widehat{\mathcal{O}}_{K,w}^\times$. In the archimedean case, if v ramifies then the norms are just the norms from $\mathbf{C}^\times$ to $\mathbf{R}^\times$, in other words the positive real numbers. As a result, we have a minimal modulus of k which is admissible for K/k. It is clear that the moduli of k which are admissible for K/k are precisely those which are divisible by the minimal one. So our isomorphism $I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}) \cong J_k/k^\times N_{K/k}J_K$ actually holds for a wide class of moduli $\mathfrak{m}$ of k. The important part is that each abelian extension K/k has a well-defined Artin reciprocity isomorphism from a group of idèle classes, due to the existence of an admissible modulus (by Lemma 4.7). So, proving the reciprocity isomorphism for any admissible modulus is all we will actually want to do.

4.3. More applications.

Lemma 4.38. *$k^\times$ is discrete (and therefore closed) in J_k.*

Proof. Since $k^\times \subset J_k$ is itself a subgroup, it suffices to show that 1 is isolated in J_k as an element of $k^\times$. Taking advantage of the ability to make arbitrarily small open sets at finitely many valuations, we claim that no element of $k^\times$ other than 1 can be found in the open set

$$U = \prod_{v\in S_\infty} B_1(1) \times \prod_{v\in M_k\setminus S_\infty} \widehat{\mathcal{O}}_{k,v}^\times,$$

where S_∞ denotes the set of infinite places of k. Recall the product formula for normalized valuations: if $|\cdot|_v$ is the normalized absolute value corresponding to the place v, and $\alpha \in k^\times$, then $\prod_v |\alpha|_v = 1$. If $\alpha \neq 1$, then $\alpha - 1 \in k^\times$, so

$$\prod_v |\alpha - 1|_v = 1.$$

This means it is impossible for α to be in U, since that would require $|\alpha-1|_v < 1$ at all archimedean v, and $|\alpha - 1|_v \leq 1$ at all nonarchimedean v, since $\alpha, 1 \in \widehat{O}_{k,v}$. □

I don't think I actually need this lemma. Maybe later I'll add a short note on how to prove the general version of the unit theorem on S-units using the compactness theorem we proved above, as well as the finiteness of the class group.

5. Group Cohomology

Let K/k be a Galois extension of number fields and let $w|v$ be places of them. Then $\mathrm{Gal}(K/k)$ In the previous sections, we saw three quotient groups which we saw were all related to each other. We also claimed they were crucial to the main statements of class field theory. They were as follows:

- $k_v^\times/N_{K_w/k_v}(K_w^\times)$
- $\widehat{\mathcal{O}}_{k,v}^\times/N_{K_w/k_v}\widehat{\mathcal{O}}_{K,w}^\times$
- $C_k/N_{K/k}C_K$.

It is therefore useful to consider the general case of an abelian group A (in our case some object coming from K) along with a group G with an action $G \to \mathrm{Aut}(A)$ (in our case $G = \mathrm{Gal}(K/k)$). We are interested in the quotient of A^G, the set of elements of A fixed by G, by the subgroup of it given by the elements of the form $\sum_{\sigma\in G}\sigma(a)$ for $a \in A$. We switch to additive notation for the group A even though in practice for class field theory it will always be multiplicative.

5.1. Generalities on group cohomology and Tate cohomology.

[20] Let G be a finite group.

Definition 5.1. A G-module (M, ρ) is an abelian group M together with a group homomorphism $\rho : G \to \mathrm{End}(M)$. As usual we suppress ρ and use $g \cdot m$ or gm to denote the action of $g \in G$ on an $m \in M$ instead of $\rho(g)m$.

We now describe the construction of a chain complex based on G and M. For each $n \geq 0$, let B_n be the free $\mathbf{Z}[G]$-module on G^n (N.B. the $\mathbf{Z}[G]$-modules are the same as G-modules). In particular, B_n is the set of formal $\mathbf{Z}[G]$-linear combinations

$$\sum_{(g_1,\ldots,g_n)\in G^n} a_{(g_1,\ldots,g_n)}e_{(g_1,\ldots,g_n)}$$

where the e_g are the basis elements and the a_g are elements of $\mathbf{Z}[G]$. We define maps $d_n : B_n \to B_{n-1}$ on the basis elements by

$$d_n(e_{(g_1,\ldots,g_n)}) = g_1e_{(g_2,\ldots,g_n)}+(-1)^ne_{(g_1,\ldots,g_{n-1})}+\sum_{i=1}^{n-1}(-1)^ie_{(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_n)}.$$

One can easily check that $d_n \circ d_{n+1} = 0$ for all $n \geq 0$. In fact, it is true (but harder to show) that the sequence $\cdots \to B_2 \to B_1 \to B_0 \to \mathbf{Z} \to 0$ is exact (the map $B_0 = \mathbf{Z}[G] \to \mathbf{Z}$ is just defined by taking the sum of the coefficients). So taking homology or cohomology now would be useless (it also wouldn't involve M at all). Instead, we apply the contravariant functor $\mathrm{Hom}_{\mathbf{Z}[G]}(-, M)$ to get the induced cochain complex

$$0 \to \mathrm{Hom}_{\mathbf{Z}[G]}(B_0, M) \xrightarrow{\partial^1} \mathrm{Hom}_{\mathbf{Z}[G]}(B_1, M) \xrightarrow{\partial^2} \cdots .$$

The fact that this is a valid cochain complex follows directly from the functoriality of $\mathrm{Hom}_{\mathbf{Z}[G]}(-, M)$. Now we can take cohomology:

Definition 5.2. Let $i \geq 0$. The i-th *cohomology group* is

$$H^i(G, M) := \ker(\partial^{i+1})/\mathrm{im}(\partial^i).$$

[20] later I should reframe this in terms of projective resolutions and derived functors

The only groups we will actually have a need for are H^0 and H^1 (though we'll have to make a modification to the definition to make it work out).

Remark 5.3. It will be more convenient to view B_n as the set of functions from G^n to M (the coefficients of an element of the free $\mathbf{Z}[G]$-module on G^n just tell you where to send the elements of G^n).

Example 5.4. Let M be a G-module. Then $B_0 = \mathbf{Z}[G]$, B_1 is the free $\mathbf{Z}[G]$-module on G, and $d_1 : B_1 \to B_0$ is given by

$$e_g \mapsto g - 1.$$

So the induced map $\partial^1 : \mathrm{Hom}(B_0, M) \to \mathrm{Hom}(B_1, M)$ is given by $f \mapsto f \circ d_1$. Of course, a homomorphism from $\mathbf{Z}[G]$ to M is determined by where it sends 1, so $\mathrm{Hom}(B_0, M) \cong M$. Then ∂^1 takes the element of $\mathrm{Hom}(B_0, M)$ defined by $g \mapsto g \cdot m$ to the element of $\mathrm{Hom}(B_1, M)$ defined on the basis elements by

$$e_g \mapsto f(g - 1) = gm - m.$$

The map $e_g \mapsto gm - m \in \mathrm{Hom}(B_1, M)$ is identically zero if and only $gm = m$ for all $g \in G$. So the zeroth cohomology group is simply

$$H^0(G, M) = \ker \partial^1 = \{m \in M | gm = m \text{ for all } m \in M\} =: M^G.$$

Example 5.5. The other cohomology group which will be important for us is H^1. From the previous example, the image of ∂^1 is the set of all elements of $\mathrm{Hom}(B_1, M)$ given by $e_g \mapsto gm - m$ for some $m \in M$. Now $d_2 : B_2 \to B_1$ is given by

$$e_{g_1, g_2} \mapsto g_1 e_{g_2} + e_{g_1} - e_{g_1 g_2}.$$

So $\partial_2 : \mathrm{Hom}(B_1, M) \to \mathrm{Hom}(B_2, M)$, given by $f \mapsto f \circ d_2$, has kernel equal to the set of elements $h \in \mathrm{Hom}(B_1, M)$ such that $h \circ d_1$ is identically zero on B_2. This function acts on the basis elements by

$$e_{(g_1, g_2)} \mapsto h(g_1 e_{g_2} + e_{g_1} - e_{g_1 g_2}).$$

So $h \in \ker \partial^2$ if and only if $h(g_1 e_{g_2} + e_{g_1} - e_{g_1 g_2}) =$, i.e. if $h(e_{g_1 g_2}) = g_1 h(e_{g_2}) + h(g_1)$. So according to the previous remark, $H^1(G, M) = (\ker \partial^2)/(\mathrm{im} \partial^1)$ can be viewed as the G-module of "crossed homomorphisms", namely the functions $h : G \to M$ with the property that $h(g_1 g_2) = g_1 h(g_2) + h(g_1)$, modded out by those of the form $h(g) = gm - m$.

Now we examine the functoriality of the H^i. First of all, taking the cochain complex $0 \to \mathrm{Hom}(B_0, M) \to \mathrm{Hom}(B_1, M) \to \cdots$ is functorial in M. In particular, let M_1, M_2 be G-modules with a homomorphism $f : M_1 \to M_2$. Then we have a map of chain complexes given by taking $\mathrm{Hom}(B_i, M_1) \to \mathrm{Hom}(B_i, M_2)$ in the way described by the vertical maps in Figure 1. It's clear from the description of the maps that the induced map is a bona fide map of chain complex (the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}(B_0, M_1) \arrow[r, "h \mapsto h \circ d_0"] \arrow[d, "h \mapsto f \circ h"] & \mathrm{Hom}(B_1, M_1) \arrow[r] \arrow[d, "h \mapsto f \circ h"] & \cdots \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}(B_0, M_2) \arrow[r, "h \mapsto h \circ d_0"'] & \mathrm{Hom}(B_1, M_2) \arrow[r] & \cdots
\end{tikzcd}$$

Figure 1.

clearly commutes), and that taking the cochain complex is a covariant functor from the category of G-modules to the category of cochain complexes of G-modules. It remains to show that the induced maps $\mathrm{Hom}(B_i, M_1) \to \mathrm{Hom}(B_i, M_2)$ induce maps of cohomology groups. Once this is shown, the functoriality is obvious because of how the maps are defined on the cohomology classes (in particular we just need to show the induced maps are well-defined). This follows easily from the commutativity of the diagram in Figure 1. If $h \in \ker(\partial^i : \mathrm{Hom}(B_i, M_1) \to \mathrm{Hom}(B_{i+1}, M_1))$, then $h \circ d_i : \mathrm{Hom}(B_{i+1}, M_1)$ is identically zero. The vertical map of cochain complexes takes h to $f \circ h \in \mathrm{Hom}(B_i, M_2)$. The coboundary map on the bottom part of the diagram, namely $\partial^i : \mathrm{Hom}(B_i, M_2) \to \mathrm{Hom}(B_{i+1}, M_2)$, takes this to $f \circ h \circ d_i = f \circ (h \circ d_i)$, which is identically zero in $\mathrm{Hom}(B_{i+1}, M_2)$ because $h \circ d_i$ is identically zero in $\mathrm{Hom}(B_{i+1}, M_1)$. So this map of cochain complexes actually sends $\ker \partial^i$ upstairs to $\ker \partial^i$ downstairs. Finally, if $h \in \mathrm{im}(\partial^i : \mathrm{Hom}(B_i, M_1) \to \mathrm{Hom}(B_{i+1}, M_1))$, then we have $h = h' \circ d_i$ for some $h' \in \mathrm{Hom}(B_i, M_1)$. And the image of h under the vertical map $\mathrm{Hom}(B_{i+1}, M_1) \to \mathrm{Hom}(B_{i+1}, M_2)$ is therefore $f \circ h = f \circ (h' \circ d_i) = (f \circ h') \circ d_i$ which is in the image of the downstairs coboundary map $\partial^i : \mathrm{Hom}(B_i, M_2) \to \mathrm{Hom}(B_{i+1}, M_2)$. So we have shown that the induced map of cochain complexes restricts to a map

$$\ker(\partial^{i+1} : \mathrm{Hom}(B_{i+1}, M_1) \to \mathrm{Hom}(B_{i+2}, M_1)) \to \ker(\partial^{i+1} : \mathrm{Hom}(B_{i+1}, M_2) \to \mathrm{Hom}(B_{i+2}, M_2))$$

and to a map

$$\mathrm{im}(\partial^i : \mathrm{Hom}(B_i, M_1) \to \mathrm{Hom}(B_{i+1}, M_1)) \to \mathrm{im}(\partial^i : \mathrm{Hom}(B_i, M_2) \to \mathrm{Hom}(B_{i+1}, M_2)),$$

hence (functorially) inducing the desired map $H^i(M_1) \to H^i(M_2)$. What we have just verified is actually just the easy part of the snake lemma. Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of G-modules. Then for each $i \geq 0$ we get an induced sequence

$$0 \to \mathrm{Hom}(B_i, M_1) \to \mathrm{Hom}(B_i, M_2) \to \mathrm{Hom}(B_i, M_3) \to 0.$$

Since B_i is free, the usual flatness arguments apply (or one can just check directly by pulling things back at the basis elements) to show that this sequence is also exact. Of course, there are also the coboundary maps for each M_i, namely $\partial^i_j : \mathrm{Hom}(B_i, M_j) \to \mathrm{Hom}(B_{i+1}, M_j)$. Expanding and rotating the diagram in Figure 1 gives a commutative diagram with exact rows and columns, shown in Figure 2. The easy part of the snake lemma gives us the maps between cokernels and between kernels. Notice that since $\mathrm{im}(\partial^i_j) \subseteq \ker(\partial^{i+1}_j)$, we get an induced map $\partial^{i+1}_j : \mathrm{coker}(\partial^i_j) \to \ker(\partial^{i+2}_j)$. Its kernel is just the set of projections of elements of $\mathrm{Hom}(B_{i+1}, M_1)$ in the kernel of ∂^{i+1}_j. In other words, its kernel is $\ker(\partial^{i+1}_j)/\mathrm{im}(\partial^i_j) = H^i(G, M_j)$. Similarly, the cokernel is $\ker(\partial^{i+2}_j)/\mathrm{im}(\partial^{i+1}_j) = H^{i+1}(G, M_j)$. So we have another diagram, the one shown in Figure 3. The definitions of the horizontal maps as restrictions or quotients of those in Figure 2 means that the diagram in Figure 3 commutes. So we can apply the snake lemma to recover the same natural maps $H^i(G, M_1) \to H^i(G, M_2) \to H^i(G, M_3)$ we constructed by hand earlier. More importantly, the nontrivial part of the snake lemma (applied for each i) gives a long exact sequence

$$0 \to H^0(G, M_1) \to H^0(G, M_2) \to H^0(G, M_3) \to H^1(G, M_1) \to H^1(G, M_2) \to H^1(G, M_3) \to H^2(G, M_1) \to \cdots.$$

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker(\partial_1^i) \arrow[r] \arrow[d] & \ker(\partial_2^i) \arrow[r] \arrow[d] & \ker(\partial_3^i) \arrow[d] & \\
0 \arrow[r] & \mathrm{Hom}(B_i, M_1) \arrow[r] \arrow[d, "\partial_1^i"] & \mathrm{Hom}(B_i, M_2) \arrow[r] \arrow[d, "\partial_2^i"] & \mathrm{Hom}(B_i, M_3) \arrow[r] \arrow[d, "\partial_3^i"] & 0 \\
0 \arrow[r] & \mathrm{Hom}(B_{i+1}, M_1) \arrow[r] \arrow[d] & \mathrm{Hom}(B_{i+1}, M_2) \arrow[r] \arrow[d] & \mathrm{Hom}(B_{i+1}, M_3) \arrow[r] \arrow[d] & 0 \\
 & \mathrm{coker}(\partial_1^i) \arrow[r] \arrow[d] & \mathrm{coker}(\partial_2^i) \arrow[r] \arrow[d] & \mathrm{coker}(\partial_3^i) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

FIGURE 2.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & H^i(G, M_1) \arrow[d] & H^i(G, M_2) \arrow[d] & H^i(G, M_3) \arrow[d] & \\
 & \mathrm{coker}(\partial_1^i) \arrow[r] \arrow[d, "\partial_1^{i+1}"] & \mathrm{coker}(\partial_2^i) \arrow[r] \arrow[d, "\partial_2^{i+1}"] & \mathrm{coker}(\partial_3^i) \arrow[r] \arrow[d, "\partial_3^{i+1}"] & 0 \\
0 \arrow[r] & \ker(\partial_1^{i+2}) \arrow[r] \arrow[d] & \ker(\partial_2^{i+2}) \arrow[r] \arrow[d] & \ker(\partial_3^{i+2}) \arrow[d] & \\
 & H^{i+1}(G, M_1) \arrow[d] & H^{i+1}(G, M_2) \arrow[d] & H^{i+2}(G, M_3) \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

FIGURE 3.

This long exact sequence will figure into our analysis of the Herbrand quotient, but only once we develop a slightly different cohomology theory, namely Tate cohomology. We do this now.

Recall that we had $H^0(G, M) = M^G$, namely the set of elements of M fixed by G. For the purposes of computing norm indices, we really are interested in something more like $M^G/\mathrm{Tr}_G M$, where $\mathrm{Tr}_G m := \sum_{g \in G} gm$ for any $m \in M$.[21]

Definition 5.6. The *Tate cohomology groups* of (G, M) are defined by $\hat{H}^0(G, M) := M^G/\mathrm{Tr}_G M$, and $\hat{H}^i(G, M) := H^i(G, M)$ for all $i \geq 1$.

[21] I should add material on homology and the full definition of Tate cohomology and homology.

It's fairly straightforward to get a long exact sequence for Tate cohomology, since it only depends on adapting the proof for the part of the sequence near H^0.

Theorem 5.7. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of G-modules. This induces a long exact sequence of Tate cohomology groups*

$$\hat{H}^0(G, M_1) \to \hat{H}^0(G, M_2) \to \hat{H}^0(G, M_3) \to \hat{H}^1(G, M_1) \to \cdots$$

Proof. Because the Tate cohomology groups coincide with the usual cohomology groups for $i \geq 1$, we can define the part of the long exact sequence starting at $\hat{H}^1(G, M_1)$ in the same way. Recall that $H^0(G, M) = M^G$. First, we explicitly write down the maps in the part of the usual long exact sequence given by

$$M_1^G \to M_2^G \to M_3^G \to H^1(G, M_1).$$

Recall that the map $M_j^G \to M_{j+1}^G$ is induced by restriction from the map $\mathrm{Hom}(B_0, M_j) \to \mathrm{Hom}(B_0, M_{j+1})$ induced by the map $\varphi : M_j \to M_{j+1}$ we started out with. In particular, it is defined by taking the homomorphism $g \mapsto gm$ to the homomorphism $\varphi \circ (g \mapsto gm) = g \mapsto g\varphi(m)$. Via the isomorphism $\mathrm{Hom}(B_0, M_j) \cong M_j$, this means the maps $M_j^G \to M_{j+1}^G$ are just defined by $m \mapsto \varphi(m)$.

Let $m \in \mathrm{Tr}_G M_j$, so that $m = \sum_{g \in G} gm'$ for some $m' \in M_j$. Then $\varphi(m) = \sum_{g \in G} g\varphi(m')$, which means $\varphi(\mathrm{Tr}_G M_j) \subseteq \mathrm{Tr}_G M_{j+1}$. In particular, we have induced maps

$$M_1^G/\mathrm{Tr}_G M_1 \xrightarrow{\tilde{\alpha}} M_2^G/\mathrm{Tr}_G M_2 \xrightarrow{\tilde{\beta}} M_3^G/\mathrm{Tr}_G M_3.$$

Now we need to check that this is exact at $M_2^G/\mathrm{Tr}_G M_2$. The fact that $\mathrm{im}\tilde{\alpha} \subseteq \ker \tilde{\beta}$ is clear from the exactness of $M_1^G \to M_2^G \to M_3^G$. On the other hand, let $m_2 \in M_2^G$ such that $\tilde{\beta}([m_2]) = 0$. Then

$$\beta(m_2) = \sum_{g \in G} gm_3$$

for some $m_3 \in M_3$. By the exactness of the original sequence, there exists $m_2' \in M_2$ such that $\beta(m_2') = m_3$. Taking traces, we have

$$\beta\left(\sum_{g \in G} gm_2'\right) = \beta(m_2) = \mathrm{Tr}_G m_3.$$

So $\sum_{g \in G} gm_2'$ and m_2 differ by an element of $\ker \beta = \mathrm{im}\alpha$, namely $\alpha(m_1)$. Both $\sum_{g \in G} gm_2'$ and m_2 are invariant under the action of G, so $\alpha(m_1)$ is as well. It follows that $m_1 - gm_1 \in \ker \alpha$ for all $g \in G$. But α is injective, so actually $m_1 \in M_1^G$. This proves that $[m_1] \in M_1^G/\mathrm{Tr}_G M_1$, and thus $\tilde{\alpha}([m_1]) = [m_2]$, proving the second desired inclusion.

It remains to define the map $M_3^G/\mathrm{Tr}_G M_3 \to H^1(G, M_1)$, and show exactness at $M_3^G/\mathrm{Tr}_G M_3$ and $H^1(G, M_1)$. Consider the exact sequence of cohomology groups

$$M_2^G \xrightarrow{\beta} M_3^G \xrightarrow{\gamma} H^1(G, M_1).$$

Consider an arbitrary element $\sum_{g \in G} gm_3 \in \mathrm{Tr}_G M_3$ for $m_3 \in M_3$. If we show it is always in $\ker \gamma$, then we can construct the desired map. This is equivalent to showing it is in $\mathrm{im}\beta$. By the exactness of the original sequence, there is some $m_2 \in M_2$ such that $\beta(m_2) = m_3$. Then $\beta(\mathrm{Tr}_G m_2) = \mathrm{Tr}_G m_3$. Since $\mathrm{Tr}_G m_2 \in M_2^G$, this means $\mathrm{Tr}_G M_3 \subseteq \ker \gamma$, and we have an induced map

$$\tilde{\gamma} : M_3^G/\mathrm{Tr}_G M_3 \to H^1(G, M_1).$$

The rest of the exactness is easy since we didn't mod the H^1's out by anything. For any $[m_2] \in M_2^G/\mathrm{Tr}_G M_2$, we have

$$\tilde{\gamma}(\tilde{\beta}([m_2])) = \gamma(\beta(m_2)) = 0.$$

And if $[m_3] \in \ker \tilde{\gamma}$, then actually $\gamma(m_3) = 0$ so $m_3 \in \mathrm{im}(\beta)$ and thus $[m_3] \in \mathrm{im}\tilde{\beta}$. This proves exactness at $M_3^G/\mathrm{Tr}_G M_3$. For the exact same reason, our sequence

$$M_1^G/\mathrm{Tr}_G M_1 \xrightarrow{\tilde{\alpha}} M_2^G/\mathrm{Tr}_G M_2 \xrightarrow{\tilde{\beta}} M_3^G/\mathrm{Tr}_G M_3 \xrightarrow{\tilde{\gamma}} H^1(G, M_1) \to H^1(G, M_2) \to \cdots$$

is exact at $H^1(G, M_1)$ as well. The rest of the exactness is induced by the exactness of the long exact sequence for cohomology. □

5.2. **Cyclic groups and the Herbrand quotient.** For an arbitrary group G, only H^0 and $\hat{H}^0$ have any clear arithmetic meaning. But when G is cyclic of finite order, Tate cohomology becomes much nicer. For example, recall that for an arbitrary finite group G and G-module M, we have $\hat{H}^0(G, M) = M^G/\mathrm{Tr}_G M$, but H^1 only has a description in terms of "crossed homomorphisms." In the cyclic case it's easy to write down H^1 explicitly.

Example 5.8. Let $G = \langle \sigma \rangle$ be a finite cyclic group. If $f : G \to M$ is a crossed homomorphism, then it must satisfy

$$f(\sigma^n) = \sigma^{n-1} f(\sigma) + f(\sigma^{n-1}).$$

By induction, it follows that for all $n \geq 1$,

$$f(\sigma^n) = (1 + \cdots + \sigma^{n-1}) f(\sigma).$$

So f is determined by where it sends σ. Moreover, we have

$$f(\sigma) = f(\sigma^{|G|+1}) = (1 + \cdots + \sigma^{|G|}) f(\sigma),$$

so f must also satisfy $f(\sigma) \in \ker \mathrm{Tr}_G =: M_{\mathrm{Tr}_G}$. Finally, for any $m \in M_{\mathrm{Tr}_G}$, we can define the map $f : G \to M$ defined by $f(\sigma^n) = (1 + \cdots + \sigma^{n-1})m$ for $1 \leq n \leq |G|$. Then since $\mathrm{Tr}_G m = 0$, it's actually true that $f(\sigma^n) = (1 + \cdots + \sigma^{n-1})m$ for all $n \geq 1$. So for any positive integers x, y we have

$$f(\sigma^x \sigma^y) = (1 + \cdots + \sigma^{x+y-1}) f(\sigma) = \sigma^x f(\sigma^y) + f(\sigma^x),$$

making f a crossed homomorphism. This means that the group of crossed homomorphisms is isomorphic to M_{Tr_G}. The principal crossed homomorphisms $g \mapsto gm - m$ correspond under this isomorphism to the elements of the form $(\sigma - 1)m$ for $m \in M$, since an element m of M_{Tr_G} corresponds to a principal crossed homomorphism if and only if $f(\sigma) = \sigma n - n$ for some $n \in M$, which is equivalent to $m \in (\sigma - 1)M$. We therefore have a natural identification

$$H^1(G, M) \cong M_{\mathrm{Tr}_G}/((1 - \sigma)M).$$

It turns out that (when G is finite and cyclic) the Tate cohomology groups contain no information other than H^1 and H^0. In particular, the long exact sequence of Tate cohomology groups loops back around after H^1.

Theorem 5.9. *Let G be a finite cyclic group. Then for any integer $n \geq 0$, we have $\hat{H}^{2n}(G, M) \cong \hat{H}^0(G, M)$, and $\hat{H}^{2n+1}(G, M) \cong \hat{H}^1(G, M)$.*

Proof. The key fact is the one from homological algebra which says that we can use any free resolution of $\mathbf{Z}$ to compute H^n.[22]. In particular, consider the sequence

$$\cdots \overset{\mathrm{Tr}_G}{\to} \mathbf{Z}[G] \overset{\sigma-1}{\to} \mathbf{Z}[G] \overset{\mathrm{Tr}_G}{\to} \mathbf{Z}[G] \overset{\sigma-1}{\to} \mathbf{Z}[G] \to \mathbf{Z} \to 0,$$

where σ is a fixed generator for G and the map $\mathbf{Z}[G] \to \mathbf{Z}$ is just by adding the coordinates. We need to check that $\ker(\sigma-1) = \mathrm{im}\mathrm{Tr}_G$, $\ker \mathrm{Tr}_G = \mathrm{im}(\sigma-1)$, and $\ker(f : \mathbf{Z}[G] \to \mathbf{Z}) = \mathrm{im}(\sigma-1)$. The last fact is easy, since if $\sigma = \mathrm{id}$ then $\sigma g - g = 0$, and otherwise $f(\sigma g - g) = 0$; the other inclusion is because if $\sum a_n\sigma^n \in \mathbf{Z}[G]$ has $\sum a_n = 0$, then $\sum a_n\sigma^n = (\sigma-1)x$ is equivalent to specifying the differences between consecutive b_n's for which $x = \sum b_n\sigma^n$. The inclusions $\mathrm{im}\mathrm{Tr}_G \subseteq \ker(\sigma-1)$ and $\mathrm{im}(\sigma-1) \subseteq \ker(\mathrm{Tr}_G)$ are both obvious, since if $x \in \mathbf{Z}[G]$, then

$$(\sigma-1)\mathrm{Tr}_G x = \mathrm{Tr}_G x - \mathrm{Tr}_G x = 0$$

and

$$\mathrm{Tr}_G(\sigma x - x) = \mathrm{Tr}_G x - \mathrm{Tr}_G = 0.$$

The remaining two are also not so hard to do the restrictiveness of G being finite and cyclic. If $x \in \ker(\sigma-1)$, then this forces an equality between each of the consecutive coefficients of x, i.e. x is of the form $\sum a\sigma^n$. In other words, $x = \mathrm{Tr}_G(a)$. This proves $\ker(\sigma-1) \subseteq \mathrm{im}(\mathrm{Tr}_G)$. Finally, one of our previous arguments shows that $\ker(\mathrm{Tr}_G) \subseteq \mathrm{im}(\sigma-1)$, as having trivial trace means you can be equal to $\sigma x - x$ just by specifying that the difference between consecutive coordinates of x differ by the prescribed coordinate of the given element of $\ker(\mathrm{Tr}_G)$.

Now that we know this is a bona fide free resolution, we can use it to compute cohomology groups. Taking homs, we get the cochain complex

$$0 \to \mathrm{Hom}(\mathbf{Z}[G], M) \to \mathrm{Hom}(\mathbf{Z}[G], M) \to \cdots$$

where the maps alternate between $h \mapsto h \circ (\sigma-1)$ and $h \mapsto h \circ \mathrm{Tr}_G$. As predicted, we get $H^0(G, M) = \ker(h \mapsto h \circ (\sigma-1))$. Recall that $\mathrm{Hom}(\mathbf{Z}[G], M)$ is identified with M because of how an element $f \in \mathrm{Hom}(\mathbf{Z}[G], M)$ is determined by $f(1)$. So as a subset of M, we can verify that as before[23]

$$H^0(G, M) = \{m \in M : (\sigma\tau)m = \tau m \text{ for all } \tau \in G\} = M^G.$$

We can also see that

$$\ker(\partial^2) = \{m \in M : \sum \sigma^n \tau m = 0 \text{ for all } \tau \in G\} = M_{\mathrm{Tr}_G},$$

and

$$\mathrm{im}(\partial^1) = \{\sigma m - m : m \in M\} = (\sigma-1)M.$$

By the periodicity of the definitions of the maps, we get the part of the statement of the theorem which says that the odd cohomology groups are all isomorphic. In particular, they are all

$$H^{2n+1}(G, M) \cong M_{\mathrm{Tr}_G}/((\sigma-1)M).$$

For the even ones, we see that

$$\ker(\partial^3) = M^G$$

[22] I should add an appendix including all the homological algebra we need

[23] Though we don't have to, since this is guaranteed to agree with the old definition of group cohomology.

since $\partial^3 = \partial^1$. For ∂^2, note that $\partial^2(m)$ takes 1 to $(\mathrm{Tr}_G 1)m = \mathrm{Tr}_G m$, so

$$\mathrm{im}(\partial^2) = \mathrm{Tr}_G M.$$

It follows that

$$H^{2n}(G, M) \cong M^G/\mathrm{Tr}_G M$$

for all $n \geq 1$, as desired. In particular,

$$\hat{H}^{2n}(G, M) \cong M^G/\mathrm{Tr}_G M$$

for all $n \geq 0$. □

So the only two nonisomorphic Tate cohomology groups are $\hat{H}^0(G, M)$ and $\hat{H}^1(G, M)$. Though both of these are often difficult to compute, there's another quantity which tends to be simpler:

Definition 5.10. Let M be a G-module. The corresponding *Herbrand quotient* is

$$Q(G, M) := |\hat{H}^0(G, M)|/|\hat{H}^1(G, M)|.$$

Example 5.11. Let $M = \mathbf{Z}$ with the trivial action of the finite cyclic group G. Then $M^G = M$ and Tr_G is multiplication by $|G|$. So $\hat{H}^0(G, \mathbf{Z}) = \mathbf{Z}/|G|\mathbf{Z}$ and $\hat{H}^1(G, \mathbf{Z}) = 0$, which means $Q(G, \mathbf{Z}) = |G|$.

Note that the isomorphisms between cohomology groups given by Theorem 5.9 have the property that (for example) the induced map $\hat{H}^2(G, M_1) \to \hat{H}^2(G, M_2)$ for $f : M_1 \to M_2$ corresponds under the isomorphisms to the induced map $\hat{H}^0(G, M_1) \to \hat{H}^0(G, M_2)$. This is due to the formal definition of $\hat{H}^0$ and the definitions of the induced maps. As a result, if $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of G-modules, the long exact sequence for Tate cohomology (see Theorem 5.7) loops around to the "exact hexagon"[24], as shown in Figure 4. The Herbrand quotient is easier to deal with than even the sizes of the individual cohomology groups because of the following fact, which Lang refers to as the **Q-machine**.

$$\begin{tikzcd}
\hat{H}^0(G, M_1) \arrow[r] & \hat{H}^0(G, M_2) \arrow[r] & \hat{H}^0(G, M_3) \arrow[d] \\
\hat{H}^1(G, M_3) \arrow[u] & \hat{H}^1(G, M_2) \arrow[l] & \hat{H}^1(G, M_1) \arrow[l]
\end{tikzcd}$$

Figure 4.

Corollary 5.12. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of G-modules. Then*

$$Q(G, M_3)Q(G, M_1) = Q(G, M_2)$$

as long as any two of the three quotients are defined.

Proof. We use the exactness of the exact hexagon. If two of the quotients are defined, then each possibly infinite group is stuck between two finite groups in an exact sequence and is therefore finite. So we may assume all the cohomology groups are finite.

[24] I don't draw it as a hexagon because it doesn't make sense to do that. The important thing is that it has 2 sides, coming from the two periods of the long exact sequence, not 6.

For all $i \in \mathbf{Z}/6\mathbf{Z}$, let k_i denote the size of the kernel of the i-th map in the hexagon (order them clockwise starting at $\hat{H}^0(G, M_1) \to \hat{H}^0(G, M_2)$ when $i = 0$), and let m_i denote the size of the image. The exactness of the hexagon means that $k_i = m_{i-1}$ for all i. As a result,

$$\frac{k_0 m_0}{k_3 m_3} \frac{k_2 m_2}{k_5 m_5} = \frac{k_1 m_1}{k_4 m_4},$$

which yields the desired

$$\frac{|\hat{H}^0(G, M_1)|}{|\hat{H}^1(G, M_1)|} \frac{|\hat{H}^0(G, M_3)|}{|\hat{H}^1(G, M_3)|} = \frac{|\hat{H}^0(G, M_2)|}{|\hat{H}^1(G, M_2)|}$$

by the first isomorphism theorem. □

Lemma 5.13. *If M is finite, then $Q(G, M) = 1$.*

Proof. Consider the map of abelian groups $f : M \to (1-\sigma)M$ given by $m \mapsto (1-\sigma)m$. Note that an element of M is fixed by G if and only if it is fixed by σ, i.e. if it is in the kernel of f. So f is surjective with kernel M^G, and we have $[M : M^G] = |(1-\sigma)M|$. Similarly, $[M : M_{\mathrm{Tr}_G}] = |\mathrm{Tr}_G M|$. Then the fact that

$$|M| = [M : M^G][M^G : \mathrm{Tr}_G M]|\mathrm{Tr}_G M| = [M : M_{\mathrm{Tr}_G}][M_{\mathrm{Tr}_G} : (1-\sigma)M]|(1-\sigma)M|$$

implies that $[M^G : \mathrm{Tr}_G M] = [M_{\mathrm{Tr}_G} : (1-\sigma)M]$ as desired. □

This is all the general machinery we will need to deal with norm subgroups of cyclic extensions of local and global fields. For the idèles, recall that the Galois action on J_K permutes the local factors corresponding to $w|v$ transitively. So if we restrict to the valuations lying over a single $v \in M_k$, we are in the following situation:

Definition 5.14. A G-module M, along with a choice of decomposition into abelian groups $M = \prod_{i=1}^n M_i$, is *semilocal* if G permutes the factors M_i transitively.

Definition 5.15. If $\prod_{i=1}^n M_i$ is a semilocal G-module, then for each $i \leq n$ we have a *decomposition group* D_i defined to be the subgroup of G consisting of all elements taking M_i to M_i. Note that M_i is a D_i-module.

In the remainder of this section, we will show that the Tate cohomology groups (and thus the Herbrand quotient) can be computed for (G, M) or for any (D_i, M_i) without changing the answer.

Lemma 5.16. *Let $M = \prod_{i=1}^n M_i$ be a semilocal G-module. Then $\hat{H}^0(G, M) \cong \hat{H}^0(D_i, M_i)$.*

Proof. Let $g \in G$ be such that $g(M_i) = M_j$. Such an element of G is guaranteed to exist since M is semilocal. Then if $g' \in G$ such that $g'(M_i) = M_j$, we must actually have $g^{-1} \circ g'(M_i) = M_i$, so $g^{-1}g' \in D_i$. In particular, every element of G taking M_i to M_j is of the form $g \circ \sigma$ where g is the fixed element of G from before and σ is some element of D_i. This is just the decomposition of G into left cosets of D_i. The coset gD_i, where $g(M_i) = M_j$, is equal to the set of elements of G sending M_i to M_j.

Fix $1 \leq i \leq n$. Let $m = \sum_{j=1}^n m_j \in M^G$. The fact that m is fixed by all of G means that if $g_j(M_i) = M_j$, every element of $g_j D_i$ must take $m_i \mapsto m_j$. So

$m_j = g_j(\sigma m_i)$ for all $\sigma \in D_i$. The action of g_j is an automorphism of M, so this means $m_i \in M_i^{D_i}$. Conversely, an element of the form

$$\sum_{j=1}^{n} g_j m_i$$

where $m_i \in M_i$ and $g_j(M_i) = M_j$ is clearly fixed by G, since the cosets of D_i are permuted by multiplying by an element of G. This means M^G is exactly the set of such elements $\sum_{j=1}^{n} g_j m_i$. The important thing is that such an element is uniquely determined by the choice of $m_i \in M_i^{D_i}$, so at least the projection gives an isomorphism $M^G \cong M_i^{D_i}$. Finally, let $m_i \in M_i$ and consider its trace $m_i' = \sum_{\sigma \in D_i} \sigma m_i \in M_i^{D_i}$. This pulls back uniquely under π to the element

$$\sum_{j=1}^{n} g_j(m_i') = \sum_{j=1}^{n} g_j \sum_{\sigma \in D_i} \sigma m_i = \sum_{j=1}^{n} \sum_{\sigma \in D_i} g_j \sigma m_i = \mathrm{Tr}_G(m_i).$$

So every element of $\mathrm{Tr}_{D_i} M_i$ is the M_i-coordinate of an element of $\mathrm{Tr}_G M$. Similarly, if $m = \sum_{j=1}^{n} m_j \in M$, its trace is $\sum_{j=1}^{n} \sum_{k=1}^{n} \sum_{\sigma \in D_j} g_k \sigma m_j$ where g_k is chosen so that $g_k(M_j) = M_k$. The M_i-coordinate of that trace is

$$\sum_{j=1}^{n} \sum_{\sigma \in D_j} g_i \sigma m_j = \sum_{j=1}^{n} \sum_{\sigma \in D_i} g_i g_i^{-1} \sigma g_i m_j = \sum_{j=1}^{n} \sum_{\sigma \in D_i} \sigma g_i m_j = \mathrm{Tr}_{D_i} \sum_{j=1}^{n} g_i m_j \in \mathrm{Tr}_{D_i} M_i.$$

So the isomorphism $\pi : M^G \to M_i^{D_i}$ restricts to a bijection $\mathrm{Tr}_G M \to \mathrm{Tr}_{D_i} M_i$ and thus an isomorphism $\hat{H}^0(G, M) \cong \hat{H}^0(D_i, M_i)$. □

Lemma 5.17. [25] *Let $M = \prod_{i=1}^{n} M_i$ be a semilocal G-module. Then $\hat{H}^1(G, M) \cong \hat{H}^1(D_i, M_i)$.*

Proof. For each $1 \leq j \leq n$, choose $g_{i,j} \in G$ such that $g_{i,j}(M_i) = M_j$. Set $g_{j,k} := g_{i,k} g_{i,j}^{-1}$ for each $1 \leq j, k \leq n$ so that $g_{j,k} g_{i,j} = g_{i,k}$. Consider an arbitrary element $m = \sum_{j=1}^{n} m_j \in M$. Then we can write $m_j = g_{i,j}(m_i^{(j)})$ where $m_i^{(j)} \in M_i$.

[25] in fact this lemma, like the previous one, is true even if G is not cyclic. Then you need to write H^1 as a quotient by $I_G M$ instead of $(1 - \sigma)M$ as in this special case. The proof is then identical.

Therefore,

$$\begin{aligned}\mathrm{Tr}_G m &= \sum_{g\in G}\sum_{j=1}^{n} g g_{i,j}(m_i^{(j)})\\ &= \sum_{j=1}^{n}\sum_{\sigma\in D_j}\sum_{k=1}^{n} g_{j,k}\sigma g_{i,j}(m_i^{(j)})\\ &= \sum_{j=1}^{n}\sum_{\sigma\in D_i}\sum_{k=1}^{n} g_{j,k} g_{i,j}\sigma g_{i,j}^{-1} g_{i,j}(m_i^{(j)})\\ &= \sum_{j=1}^{n}\sum_{k=1}^{n} g_{j,k} g_{i,j}\mathrm{Tr}_{D_i}(m_i^{(j)})\\ &= \sum_{k=1}^{n} g_{i,k}\mathrm{Tr}_{D_i}\left(\sum_{j=1}^{n} m_i^{(j)}\right).\end{aligned}$$

So we have decomposed $\mathrm{Tr}_G m$ into its M_k-components, and $\mathrm{Tr}_G m = 0$ if and only if $\mathrm{Tr}_{D_i}\left(\sum_{j=1}^{n} m_i^{(j)}\right) = 0$. This means we have a well-defined[26] group homomorphism $\varphi : M_{\mathrm{Tr}_G} \to (M_i)_{\mathrm{Tr}_{D_i}}$ given by $m \mapsto \sum_{j=1}^{n} m_i^{(j)}$. The map φ is clearly surjective ($m_i \in (M_i)_{\mathrm{Tr}_{D_i}}$ has preimage m_i for example). Let τ be a generator for G and τ_i a generator for D_i. If $\tau(M_j) = M_\tau(j)$, for each j there is a unique $\sigma_{\tau(j)} \in D_i$ such that

$$\tau g_{i,j} = g_{i,\tau(j)}\sigma_{\tau(j)}.$$

Then

$$\begin{aligned}(1-\tau)m &= \sum_{j=1}^{n} g_{i,j}m_i^{(j)} - \sum_{j=1}^{n}\tau g_{i,j}m_i^{(j)}\\ &= \sum_{j=1}^{n} g_{i,j}m_i^{(j)} - \sum_{j=1}^{n} g_{i,\tau(j)}\sigma_{\tau(j)}m_i^{(j)}\\ &= \sum_{j=1}^{n} g_{i,j}m_i^{(j)} - \sum_{j=1}^{n} g_{i,j}\sigma_j m_i^{(\sigma^{-1}j)}\\ &= \sum_{j=1}^{n} g_{i,j}(m_i^{(j)} - \sigma_j m_i^{(\sigma^{-1}j)}).\end{aligned}$$

Therefore,

$$\varphi((1-\tau)m) = \sum_{j=1}^{n} m_i^{(j)} - \sigma_j m_i^{(\sigma^{-1}j)} \in (1-\tau_i)M_i$$

since each summand is in the subgroup $(1-\tau_i)M_i$. As a result φ induces a surjective map $\tilde{\varphi} : M_{\mathrm{Tr}_G}/((1-\tau)M) \to (M_i)_{\mathrm{Tr}_{D_i}}/((1-\tau_i)M_i)$. It remains to show injectivity.

[26] Well-defined up to a choice of $g_{i,j}$'s.

Suppose that $[m] = \left[\sum_{j=1}^n g_{i,j} m_i^{(j)}\right] \in \ker \tilde{\varphi}$. Then

$$\sum_{j=1}^n m_i^{(j)} \in (1-\tau_i)M_i \subseteq (1-\tau)M,$$

which means

$$[m] = \left[m - \sum_{j=1}^n m_i^{(j)}\right] = \left[\sum_{j=1}^n g_{i,j} m_i^{(j)} - m_i^{(j)}\right] = 0,$$

as desired. □

5.3. **Some norm indices.** Let K/k be a Galois extension and $w|v$ a choice of nonarchimedean valuations. In the previous sections we used two facts about norm indices:

- $[k_v^\times : N_{K_w/K_v} K_w^\times], [\widehat{\mathcal{O}}_{k,v}^\times : N_{K_w/k_v} \widehat{\mathcal{O}}_{K,w}^\times] < \infty$.[27]
- If v is unramified, then $\widehat{\mathcal{O}}_{k,v}^\times = N_{K_w/k_v} \widehat{\mathcal{O}}_{K,w}^\times$.

We will prove both of these by explicitly computing the indices in the cyclic case, using the tools of group cohomology from the previous section. To apply that theory, notice that the action of $\mathrm{Gal}(K_w/k_v)$ on K_w makes $K_w^\times$ a $\mathrm{Gal}(K_w/k_v)$-module restricting to the $\mathrm{Gal}(K_w/k_v)$-module $\widehat{\mathcal{O}}_{K,w}^\times$. Translating between additive and multiplicative notation, $\mathrm{Tr}_{\mathrm{Gal}(K_w/k_v)}$ stands for N_{K_w/k_v}. Since K_w/k_v is Galois, we have $(K_w^\times)^{\mathrm{Gal}(K_w/k_v)} = k_v^\times$, and $(\widehat{\mathcal{O}}_{K,w}^\times)^{\mathrm{Gal}(K_w/k_v)} = \widehat{\mathcal{O}}_{k,v}^\times$. Suppose $\mathrm{Gal}(K_w/k_v)$ is cyclic with generator τ. From the previous section, we have

$$\begin{aligned}
\hat{H}^0(\mathrm{Gal}(K_w/k_v), K_w^\times) &= k_v^\times / N_{K_w/k_v} K_w^\times \\
\hat{H}^0(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times) &= \widehat{\mathcal{O}}_{k,v}^\times / N_{K_w/k_v} \widehat{\mathcal{O}}_{K,w}^\times \\
\hat{H}^1(\mathrm{Gal}(K_w/k_v), K_w^\times) &= \{x \in K_w^\times : N_{K_w/k_v} x = 1\} / \{x/\tau x : x \in K_w^\times\} \\
\hat{H}^1(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times) &= \{x \in \widehat{\mathcal{O}}_{K,w}^\times : N_{K_w/k_v} x = 1\} / \{x/\tau x : x \in \widehat{\mathcal{O}}_{K,w}^\times\}
\end{aligned}$$

Hilbert's theorem 90 (just the classical version for cyclic Galois groups) says that $\hat{H}^1(\mathrm{Gal}(K_w/k_v), K_w^\times) = 1$. This means that we may compute the desired norm index for $k_v^\times$ by computing the Herbrand quotient $Q(\mathrm{Gal}(K_w/k_v), K_w^\times)$. To do that it will be useful to know the Herbrand quotient for the units:

Lemma 5.18. *If K_w/k_v is cyclic, then* $Q(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times) = 1$.

Proof. Let B be an open $\mathrm{Gal}(K_w/k_v)$-submodule of $\widehat{\mathcal{O}}_{K,w}^\times$. By the compactness of this unit group, we know $|\widehat{\mathcal{O}}_{K,w}^\times / B| < \infty$. Using Corollary 5.12,

$$Q(\mathrm{Gal}(K_w/k_v), B) Q(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times / B) = Q(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times)$$

so by Lemma 5.13 we have

$$Q(\mathrm{Gal}(K_w/k_v), B) = Q(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times).$$

In particular it suffices to compute the Herbrand quotient of any open $\mathrm{Gal}(K_w/K_v)$-submodule of $Q(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times)$. To do this, we suppose $v = v_{\mathfrak{p}}$ and use the $\mathfrak{p}$-adic logarithm along with the cohomology theory of semilocal G-modules. By the

[27] We used this to show that norm subgroups are open. But we also noted that this can be shown using the $\mathfrak{p}$-adic logarithm. Hensel's lemma also works.

normal basis theorem, K_w has a k_v-basis $\{\omega_\sigma\}_{\sigma\in\mathrm{Gal}(K_w/k_v)}$ such that $\tau(\omega_\sigma)=\omega_{\tau\sigma}$ for all $\sigma,\tau\in\mathrm{Gal}(K_w/k_v)$. We can also multiply the ω_sigma's by a nonzero elements of k_v of large valuation to ensure that ω_σ is in the domain of the isomorphism given by the $\mathfrak{p}$-adic exponential. Let

$$A=\sum_{\sigma\in\mathrm{Gal}(K_w/k_v)}\widehat{\mathcal{O}}_{k,v}\omega_\sigma.$$

A is a G-submodule of K_w (N.B. this abelian group is the additive one). Since the ω_σ's are a normal basis, A is semilocal. The decomposition group D_σ is just the set of $\tau\in\mathrm{Gal}(K_w/k_v)$ such that $\tau\sigma=\sigma$, i.e. $D_\sigma=1$. So by Lemma 5.16 and Lemma 5.17,

$$Q(\mathrm{Gal}(K_w/k_v),A)=Q(1,\widehat{\mathcal{O}}_{k,v}\omega_\sigma)=1$$

since trivial groups have trivial cohomology. Moreover, A is clearly open in K_w, since it is an open box under the sup norm given by the basis $\{\omega_\sigma\}_\sigma$. It was constructed to lie inside an open ball around 0 small enough for the $\mathfrak{p}$-adic exponential to be a topological isomorphism between it and an open set around 1. Since the action of $\mathrm{Gal}(K_w/k_v)$ is continuous, it respects power series, which means the logarithm and exponential in fact produce a topological isomorphism of $\mathrm{Gal}(K_w/k_v)$-modules. In particular, since A is an open $\mathrm{Gal}(K_w/k_v)$-submodule of K_w with trivial cohomology with respect to $\mathrm{Gal}(K_w/k_v)$, we know that $\exp(A)$ is an open $\mathrm{Gal}(K_w/k_v)$-submodule of $K_w^\times$ also with trivial cohomology. Since it is in a small open ball around 1, we have produced the desired subgroup $B=\exp(A)\subseteq\widehat{\mathcal{O}}_{K,w}^\times$. □

Lemma 5.19. *If K_w/k_v is cyclic, then $[k_v^\times:N_{K_w/k_v}K_w^\times]=[K_w:k_v]$.*

Proof. Since $\hat{H}^1(\mathrm{Gal}(K_w/k_v),K_w^\times)=1$ by Hilbert's theorem 90, the desired norm index is

$$[k_v^\times:N_{K_w/k_v}K_w^\times]=Q(\mathrm{Gal}(K_w/k_v),K_w^\times).$$

The $\mathrm{Gal}(K_w/k_v)$-submodule $\widehat{\mathcal{O}}_{K,w}^\times\subseteq K_w^\times$ has the property that $K_w^\times/\widehat{\mathcal{O}}_{K,w}^\times\cong\mathbf{Z}$ as $\mathrm{Gal}(K_w/k_v)$-modules, where the action on $\mathbf{Z}$ is trivial. The isomorphism is given by $x\mapsto v(x)$. So by Corollary 5.12,

$$Q(\mathrm{Gal}(K_w/k_v),\mathbf{Z})Q(\mathrm{Gal}(K_w,k_v),\widehat{\mathcal{O}}_{K,w}^\times)=Q(\mathrm{Gal}(K_w,k_v),K_w^\times)$$

as long as any two of the quotients are finite. Since the action on $\mathbf{Z}$ is trivial, we know $Q(\mathrm{Gal}(K_w/k_v),\mathbf{Z})=|\mathrm{Gal}(K_w/k_v)|=[K_w:k_v]$. By Lemma 5.18, $Q(\mathrm{Gal}(K_w,k_v),\widehat{\mathcal{O}}_{K,w}^\times)=1$, so the third quotient is finite and equal to $[K_w:k_v]$, as desired. □

We can also compute the norm index of the units, which we already know is finite and bounded by $[K_w:k_v]$ by the previous lemma.

Lemma 5.20. *If K_w/k_v is cyclic, then $[\widehat{\mathcal{O}}_{k,v}^\times:N_{K_w/k_v}\widehat{\mathcal{O}}_{K,w}^\times]=e(w|v)$.*

Proof. Recall from Lemma 5.18 that $Q(\mathrm{Gal}(K_w/k_v),\widehat{\mathcal{O}}_{K,w}^\times)=1$, which means it suffices to compute $|\hat{H}^1(\mathrm{Gal}(K_w/k_v),\widehat{\mathcal{O}}_{K,w}^\times)|$. By Hilbert's theorem 90,

$$(\widehat{\mathcal{O}}_{K,w}^\times)_{N_{K_w/k_v}}=\{x/\tau(x):x\in K_w^\times\},$$

which means (where $1-\tau$ is written in additive notation to make the meaning clearer; in this case it is the map $x \mapsto x/\tau(x)$)

$$\begin{aligned}|\hat{H}^1(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times)| &= [(\widehat{\mathcal{O}}_{K,w}^\times)_{N_{K_w/k_v}} : (1-\tau)\widehat{\mathcal{O}}_{K,w}^\times] \\ &= [(1-\tau)K_w^\times : (1-\tau)\widehat{\mathcal{O}}_{K,w}^\times] \\ &= [(1-\tau)K_w^\times : (1-\tau)k_v^\times\widehat{\mathcal{O}}_{K,w}^\times] \\ &= \frac{[K_w^\times : k_v^\times\widehat{\mathcal{O}}_{K,w}^\times]}{[(K_w^\times)_{1-\tau} : (k_v^\times\widehat{\mathcal{O}}_{K,w}^\times)_{1-\tau}]}\end{aligned}$$

where the third equality is because every element of $k_v^\times$ is fixed by τ, so $(1-\tau)k_v^\times = \{1\}$, and the second equality is due to the first and third isomorphism theorems. Of course, $(K_w^\times)_{1-\tau} = k_v^\times$ since the extension is Galois and cyclic ($x = \tau(x)$ means x is fixed by the whole Galois group means $x \in k_v$). For the same reason, $(k_v^\times\widehat{\mathcal{O}}_{K,w}^\times)_{1-\tau} = k_v^\times$ as well, since $k_v^\times$ is fixed by τ and $k_v^\times\widehat{\mathcal{O}}_{K,w}^\times \subseteq K_w^\times$. So the denominator is $[k_v^\times : k_v^\times] = 1$. For the numerator, Let π be a uniformizer for K_v, so that $u_0\pi^{e(w|v)}$ is a uniformizer for k_v for the appropriate choice of $u_0 \in \widehat{\mathcal{O}}_{K,w}^\times$. Then $K_w^\times = \{u\pi^n : u \in \widehat{\mathcal{O}}_{K,w}^\times, n \in \mathbf{Z}\}$ and $k_v^\times\widehat{\mathcal{O}}_{K,w}^\times = \{u\pi^{e(w|v)n} : u \in \widehat{\mathcal{O}}_{K,w}^\times, n \in \mathbf{Z}\}$, so $[K_w^\times : k_v^\times\widehat{\mathcal{O}}_{K,w}^\times] = e(w|v)$. It follows that $|\hat{H}^1(\mathrm{Gal}(K_w/k_v), \widehat{\mathcal{O}}_{K,w}^\times)| = e(w|v)$ and thus $[\widehat{\mathcal{O}}_{k,v}^\times : N_{K_w/k_v}\widehat{\mathcal{O}}_{K,w}^\times] = e(w|v)$ as desired. □

Even though we have only proved these equalities for cyclic extensions, it will turn out as a result of local Artin reciprocity that they are true for arbitrary abelian extensions of local fields (the statements for archimedean local fields are obvious using the definition $f = 1$ and $e = 2$ if v becomes complex in K). The only specific result we used is that in the abelian case, if $w|v$ is unramified, then every unit in k_v is a norm from K_w. We'll be able to prove this and its converse in the abelian case, which will take up the remainder of this section.

Lemma 5.21. *Suppose K_w/k_v is abelian. Then $[\widehat{\mathcal{O}}_{k,v} : N_{K_w/k_v}\mathcal{O}_{K,w}] \leq e(w|v)$.*

Proof. We will show a divisibility instead the inequality. Since K_w/k_v is abelian, we can inductively choose cyclic subgroups of its Galois group then pass to the quotient to get a chain of fields

$$k_v \subset E_1 \subset \cdots E_n \subset K_w$$

such that each E_i/E_{i-1} is cyclic, and so are K_w/E_n and E_1/k_v. For convenience we write $v = v_0$, $k_v = E_0$, $w = v_{n+1}$, and $K_w = E_{n+1}$. Since E_i/k_v are finite, they are all complete with respect to the unique valuation extended from v (which must be compatible with restriction from w and each other). So we really have a tower of cyclic extensions of local fields E_i with valuations v_i with compatible restrictions. Everything we have done in this section is valid abstractly for extensions of nonarchimedean fields, so there is no need to show that E_i is a completion of an intermediate field. However, even this is clearly true, as $K \cap E_i$ is dense in E_i with respect to w, which restricts to v_i on E_i. Moreover, $E_i' := K \cap E_i \subseteq E_i$ has completion with respect to v_i which is contained in E_i since E_i is complete. In fact, the completion is equal to E_i because E_i' is dense in E_i (so its completion cannot be dense and properly contained in E_i, e.g. using the equivalence of norms on finite-dimensional vector spaces over a complex field and the sup norm on E_i

over the completion of E_i'). So in fact we can match our situation exactly with the one we've dealt with so far, namely a tower of extensions

$$E_0' = k \subset E_1' \subset E_2' \subset \cdots \subset E_n' \subset K = E_{n+1}'$$

defined as described, with valuations $v = v_0 | v_1 | \cdots | v_n | v_{n+1} = w$ so that after completing with respect to these valuations we have a (Galois) tower of local fields

$$E_0 = k_v \subset E_1 \subset E_2 \subset \cdots \subset K_w = E_{n+1}$$

with the property that E_i/E_{i+1} is cyclic. Taking norms down to k_v, we have

$$N_{E_{n+1}/E_0}\mathcal{O}^\times_{E_{n+1}} \subset N_{E_n/E_0}\mathcal{O}^\times_{E_n} \subset \cdots \subset N_{E_1/E_0}\mathcal{O}^\times_{E_1} \subset \mathcal{O}^\times_{E_0}.$$

So the desired norm index is

$$\begin{aligned}
[\widehat{\mathcal{O}}^\times_{k,v} : N_{K_w/k_v}\widehat{\mathcal{O}}^\times_{K,w}] &= [\mathcal{O}^\times_{E_0} : N_{E_{n+1}/E_0}\mathcal{O}_{E_{n+1}}] \\
&= [\mathcal{O}^\times_{E_0} : N_{E_1/E_0}\mathcal{O}^\times_{E_1}][N_{E_1/E_0}\mathcal{O}^\times_{E_1} : N_{E_{n+1}/E_0}\mathcal{O}^\times_{E_{n+1}}] \\
&= e(v_1|v_0)[N_{E_1/E_0}\mathcal{O}^\times_{E_1} : N_{E_1/E_0}N_{E_{n+1}/E_1}\mathcal{O}^\times_{E_{n+1}}].
\end{aligned}$$

By the first and third isomorphism theorems, $[N_{E_1/E_0}\mathcal{O}^\times_{E_1} : N_{E_1/E_0}N_{E_{n+1}/E_1}\mathcal{O}^\times_{E_{n+1}}]$ divides $[\mathcal{O}^\times_{E_1} : N_{E_{n+1}/E_1}\mathcal{O}^\times_{E_{n+1}}]$, which divides $e(v_{n+1}|v_1)$ by induction. So the norm index we want divides $e(v_1|v_0)e(v_{n+1}|v_1) = e(v_{n+1}|v_0) = e(w|v)$, as desired. □

Corollary 5.22. *If K_w/k_v is abelian, and $w|v$ unramified, then every element of $\widehat{\mathcal{O}}^\times_{k,v}$ is a norm from $\mathcal{O}^\times_{K,w}$.*

Lemma 5.23. *If $w|v$ is ramified and K_w/k_v abelian, then $[\widehat{\mathcal{O}}^\times_{k,v} : N_{K_w/k_v}\widehat{\mathcal{O}}^\times_{K,w}] > 1$.*

Proof. Last time, the proof relied on decomposing an abelian extension into a tower of cyclic extensions, only using the fact that an subextension of an abelian extension is abelian (and in particular Galois) over the bottom field and under the top field. This time, we decompose the abelian extension as a compositum of cyclic extensions. Since $\mathrm{Gal}(K_w/k_v)$ is a finite abelian group, it is a product of cyclic groups $H_1 \times \cdots \times H_n$. Then each fixed field $K_w^{\prod_{j\neq i} H_i}$ is a Galois cyclic extension of k_v, and by the Galois correspondence the composite $K_w^{\prod_{j\neq 1} H_j} \cdots K_w^{\prod_{j\neq n} H_j}$ has Galois group $\cap_{i=1}^n \prod_{j\neq i} H_j = \{1\}$ over k_v. So K_w is a composite of cyclic subextensions. If v ramifies in K_w, then it ramifies in one of these cyclic extensions, which means that for some i,

$$N_{K_w^{\prod_{j\neq i} H_j}/k_v}\mathcal{O}^\times_{K_w^{\prod_{j\neq i} H_j}} \subsetneq \widehat{\mathcal{O}}_{k,v}$$

(because the index is equal to $e(K_w^{\prod_{j\neq i} H_j}/k_v) > 1$). Since

$$N_{K_w/k_v}\widehat{\mathcal{O}}^\times_{K,w} \subseteq N_{K_w^{\prod_{j\neq i} H_j}/k_v}\mathcal{O}^\times_{K_w^{\prod_{j\neq i} H_j}},$$

it follows that $[\widehat{\mathcal{O}}^\times_{k,v} : N_{K_w/k_v}\widehat{\mathcal{O}}^\times_{K,w}] > 1$ as desired. □

5.4. **Other applications.** Kummer theory. General statement of Hilbert 90. Using the long exact sequence to prove Hasse's local-global principal for norms in cyclic extensions. Application to quadratic forms.

6. Global Class Field Theory

Recall the original goal of class field theory, namely that if K/k is an abelian extension of number fields, then for some modulus $\mathfrak{m}$, the Artin map $I(\mathfrak{m}) \to \operatorname{Gal}(K/k)$ induces an isomorphism $I(\mathfrak{m})/P_{\mathfrak{m}}N(\mathfrak{m}) \to \operatorname{Gal}(K/k)$. The $N(\mathfrak{m})$ in the denominator is at least a minimum requirement, as it is clearly in the kernel of the Artin map (the elements of the norm group are products of $f(\mathfrak{P}|\mathfrak{p})$-th powers of primes $\mathfrak{p} \not| \mathfrak{m}_0$, and the Artin symbol $\left[\frac{K/k}{\mathfrak{p}}\right]$ has order $f(\mathfrak{P}|\mathfrak{p})$). Showing that $P_{\mathfrak{m}}$ is in the kernel is the most nontrivial part of global class field theory, but it is motivated by the desire to relate Hecke L-functions to Artin L-functions via the Artin map, as well as the fact (historically proven by Takagi [15] in the 1910s before the Artin reciprocity law was known) that $I(\mathfrak{m})/P_{\mathfrak{m}}N(\mathfrak{m})$ and $\operatorname{Gal}(K/k)$ are noncanonically isomorphic for the correct choice of $\mathfrak{m}$. Once we have shown that the kernel contains $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$, it will still be useful to know at least the equality of sizes of these two finite group. To do that, we will use the **first and second fundamental inequalities**. Both were historically proven analytically. We will follow [9], proving the first one analytically, and the second one using the cohomology of the S-units and idèles. Note that we establish the first inequality in more generality than the second one.

6.1. The first fundamental inequality.

In this section, we will use the Hecke L-functions for characters on on $I(\mathfrak{m})/P_{\mathfrak{m}}$ to derive the following inequality:

Proposition 6.1. *Let K/k be a Galois extension of number fields, and $\mathfrak{m}$ a modulus for k divisible by all the primes ramifying in K.*[28] *Then we have*

$$[I(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})] \leq [K : k].$$

Proof. We will use the usual trick of multiplying $L(s,\chi)$ together over all χ, first taking logs to simplify things. Let χ be a character of $G := I(\mathfrak{m})/P_{\mathfrak{m}}N(\mathfrak{m})$, or simply a Hecke character mod $\mathfrak{m}$ vanishing on $N(\mathfrak{m})$. We have not yet shown that $L(1,\chi) \neq 0$, but we know that $L(s,\chi)$ extends past 1 when χ is nontrivial, and that $L(s,1)$ differs from ζ_k by a finite number of entire factors which are nonzero at 1. We don't yet have access to Artin L-functions from Hecke L-functions (since we haven't proven Artin reciprocity yet), so we can't prove any relationship between $\prod_\chi L(s,\chi)$ and any zeta function. Instead, we directly analyze the definition of the log of this product.

Since $L(s,\chi)$ is not identically zero, by the identity theorem if it has a zero at $s=0$ it is of finite order. So for $\chi \neq 1$ we may write

$$L(s,\chi) = (s-1)^{m(\chi)} f(s,\chi)$$

for some integer $m(\chi)$, where f is holomorphic on the domain of definition of $L(s,\chi)$, plus $s=1$, and nonzero at $s=1$. Let $s \to 1^+$. Adding up the logs of the $L(s,\chi)$, we have (using the Euler products as usual)

$$\sum_{\chi \in \widehat{G}} \log L(s,\chi) = \log \zeta_k(s) - \sum_{1 \neq \chi \in \widehat{G}} m(\chi) \log \frac{1}{s-1}.$$

[28] These hypotheses are general enough for everything we will do. In particular, the modulus must be divisible by all the ramified primes in order for the Artin map to be well-defined anyway.

Recall that ζ_k has a simple pole at $s = 1$. Its residue does not matter since we are taking logs. As a result, we have

$$\sum_{\chi\in\widehat{G}} \log L(s,\chi) = \left(1 - \sum_{1\neq\chi\in\widehat{G}} m(\chi)\right) \log\frac{1}{s-1} + O(1)$$

as $s \to 1^+$. On the other hand, we can directly look at the Euler products and get rid of converging parts to get in the usual way[29]

$$\sum_{\chi\in\widehat{G}} \log L(s,\chi) = \sum_{\chi\in\widehat{G}} \sum_{\mathfrak{p}\nmid\mathfrak{m}} \frac{\chi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^s} + O(1).$$

Splitting the sum over the ideal classes (allowed by absolute convergence for $\Re(s) > 1$) and combining the previous two equations, we get

$$\begin{aligned}\left(1 - \sum_{1\neq\chi\in\widehat{G}} m(\chi)\right) \log\frac{1}{s-1} &= \sum_{\chi\in\widehat{G}} \sum_{\mathfrak{K}\in G} \sum_{\mathfrak{p}\in\mathfrak{K}} \frac{\chi(\mathfrak{K})}{\mathrm{N}\mathfrak{p}^s} + O(1)\\ &= \sum_{\mathfrak{K}\in G} \left(\sum_{\mathfrak{p}\in\mathfrak{K}} \mathrm{N}\mathfrak{p}^{-s}\right)\left(\sum_{\chi\in\widehat{G}} \chi(\mathfrak{p})\right) + O(1).\end{aligned}$$

The second term in the summand vanishes whenever $\mathfrak{K}$ is nontrivial and is $|\widehat{G}| = |G|$ otherwise. So the right hand side is equal to

$$|G| \sum_{\mathfrak{p}\in P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})} \mathrm{N}\mathfrak{p}^{-s} + O(1).$$

If $\mathfrak{p}$ splits completely in K, then $\mathfrak{p} = \mathrm{N}\mathfrak{P}$ for any $\mathfrak{P}|\mathfrak{p}$, so $\mathfrak{p} \in \mathfrak{N}(\mathfrak{m})$. We can also add back in the primes dividing $\mathfrak{m}$, absorbing the extra cost into the error term, so that

$$\left(1 - \sum_{1\neq\chi\in\widehat{G}} m(\chi)\right) \log\frac{1}{s-1} \geq |G| \sum_{\mathfrak{p}\in\mathrm{Spl}(K/k)} \mathrm{N}\mathfrak{p}^{-s} + O(1).$$

There are exactly $[K : k]$ primes $\mathfrak{P}$ of K lying over each $\mathfrak{p} \in \mathrm{Spl}(K/k)$, each of which having the same norm as $\mathfrak{p}$. Thus, the right hand side is equal to

$$\frac{|G|}{[K:k]} \sum_{\substack{\mathfrak{P}\\ f(\mathfrak{P}|\mathfrak{p})=1}} \mathrm{N}\mathfrak{P}^{-s} + O(1),$$

where we have added the ramified primes back into the sum at a constant cost (as there are finitely many). What we are left with is within $O(1)$ from $\zeta_K(s)$, since the primes of higher inertial degree contribute at most $[K : k]$ terms each, of the form $\mathrm{N}\mathfrak{p}^{-fs}$ for $f > 1$. These sum to something bounded $f > 1$, and there are at most $[k : \mathbf{Q}]$ of these primes lying over a given one in $\mathbf{Q}$. As a result,

$$\left(1 - \sum_{1\neq\chi\in\widehat{G}} m(\chi)\right) \log\frac{1}{s-1} \geq \frac{|G|}{[K:k]} \log\frac{1}{s-1} + O(1)$$

[29] Using the power series for $\log(1-x)$ and showing all the terms except those of degree 1 sum to something $O(1)$

because of the simple pole of ζ_K at $s = 1$. Since $|G|/[K : k] > 0$, this immediately implies that $m(\chi) = 0$ for all χ (otherwise the LHS would always be negative or zero as $s \mapsto 1^+$). This in turn implies that $|G| \leq [K : k]$, as desired. □

Remark 6.2. We have also just shown that $L(1, \chi) \neq 0$, which yields a direct proof of the fact that there are infinitely many primes in each class of $I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ as long as we can construct an extension K/k which only ramifies at primes dividing $\mathfrak{m}$. This is easy: just consider $k(\zeta_m)$ where m is divisible by the same rational primes as $\mathfrak{m}$. In general this group is smaller than the generalized ideal class group $I(\mathfrak{m})/P_{\mathfrak{m}}$, so the problem of whether there are infinitely many primes in each generalized ideal class has still not been addressed. To do that, we would need to find an extension K/k with the additional property that $\mathfrak{N}(\mathfrak{m}) \subseteq P_{\mathfrak{m}}$.

Remark 6.3. The fact that $L(1, \chi) \neq 0$ and therefore the infinitude of primes in each class of $I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ is still useful. It shows that if this group is nontrivial, then there are infinitely many primes not in $\mathfrak{N}(\mathfrak{m})$, and therefore infinitely many primes which do not split completely. In particular, the density of the set of such primes is at least $(|G| - 1)/|G|$.

If we take $\mathfrak{m}$ to be an admissible cycle, Proposition 6.1 tells us via the isomorphism of Lemma 4.33 that

$$|J_k/k^\times N_{K/k}J_K| \leq [K : k].$$

6.2. **The second fundamental inequality.** The second fundamental inequality proves that the first is an equality (as would be implied by the full statements of class field theory), but only in the case that K/k is cyclic. We will use cohomology to prove it. From now on, K/k is a cyclic Galois extension of number fields (whereas in the previous section it was an arbitrary Galois extension of number fields). The index $[J_k : k^\times N_{K/k}J_K]$ is just $|\hat{H}^0(\mathrm{Gal}(K/k), J_K)|$. Recall from Lemma 4.17 that for all sufficiently large finite $S \subseteq M_K$ containing all the archimedean absolute values, we have $J_K = K^\times J_{K,S}$. In order to allow $\mathrm{Gal}(K/k)$ to act on $J_{K,S}$, we need S to be closed under the action of $\mathrm{Gal}(K/k)$. So we enlarge S to include all $w|v$ for each $v \in M_k$ for which it already includes at least one $w|v$. In order to further simplify things, we also enlarge S to contain all the w such that $w|v$ is ramified.

Then we have an isomorphism of $\mathrm{Gal}(K/k)$-modules $J_{K,S}/K_S \to K^\times J_{K,S}/K^\times = C_K$ induced by the inclusion of $\mathrm{Gal}(K/k)$-modules $J_{K,S} \to K^\times J_{K,S}$. So by Lemma 5.12, the relevant Herbrand quotient is

$$\begin{aligned} Q(\mathrm{Gal}(K/k), C_K) &= Q(\mathrm{Gal}(K/k), K^\times J_{K,S}/K^\times) \\ &= Q(\mathrm{Gal}(K/k), J_{K,S}/K_S) \\ &= Q(\mathrm{Gal}(K/k), J_{K,S})/Q(\mathrm{Gal}(K/k), K_S). \end{aligned}$$

The first thing we need to do is therefore to compute the Herbrand quotients for $J_{K,S}$ and K_S.

Proposition 6.4. *With $S \subseteq M_K$ as above, $Q(\mathrm{Gal}(K/k), J_{K,S}) = \prod_{v \in S_k}[K_w : k_v]$, where S_k is the set of all absolute values of k lying below elements of S.*

Proof. We reduced the computation from J_K to $J_{K,S}$ because it can be written in a straightforward way as the product

$$J_{K,S} = \left(\prod_{v \in S_k} \prod_{w|v} K_w^\times \right) \times \left(\prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times \right).$$

Since $\mathrm{Gal}(K/k)$ permutes the $w|v$, it acts separately on each component of the product. Therefore, Lemma 5.12 tells us that[30]

$$Q(\mathrm{Gal}(K/k), J_{K,S}) = \prod_{v \in S_k} Q\left(\mathrm{Gal}(K/k), \prod_{w|v} K_w^\times \right) Q\left(\mathrm{Gal}(K/k), \prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times \right).$$

Since $\mathrm{Gal}(K/k)$ permutes the $w|v$ transitively, the results of Lemma 5.16 and Lemma 5.17 apply, so

$$Q\left(\mathrm{Gal}(K/k), \prod_{w|v} K_w^\times \right) = Q(\mathrm{Gal}(K_w/k_v), K_w^\times) = [K_w : k_v]$$

where the second equality is by Lemma 5.19. It remains to compute the Herbrand quotient for the product at the places not in S_k. Recall from our description in section 4 of the norm coming from the action of $\mathrm{Gal}(K/k)$ on J_K that if $(\alpha_w)_w \in \prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times$, then

$$N_{K/k}\alpha = \left(\prod_{w|v} N_{K_w/k_v} \alpha_w \right)_{v \in M_k \setminus S_k}.$$

Since v is unramified for all $v \in M_k \setminus S_k$, every element of $\widehat{\mathcal{O}}_{k,v}^\times$ is a norm from $\widehat{\mathcal{O}}_{K,w}^\times$ (see Lemma 5.20). This implies (after using it on all the coordinates) that $\hat{H}^0(\mathrm{Gal}(K/k), \prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times) = 1$. For H^1, the fact that $\hat{H}^1(\mathrm{Gal}(K/k), \widehat{\mathcal{O}}_{K,w}^\times) = 1$ implies that the same is true for $\prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times$ by Lemma 5.17. By our description of the norm, any element of $\prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times$ of norm 1 has components in $\prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times$ all of norm 1, which are therefore in $(1-\sigma)\prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times$ where σ is a generator for $\mathrm{Gal}(K/k)$ since $\hat{H}^1(\mathrm{Gal}(K/k), \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times) = 1$. Since $\mathrm{Gal}(K/k)$ acts componentwise, this implies that $\hat{H}^1(\mathrm{Gal}(K/k), \prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times) = 1$, and thus

$$Q\left(\mathrm{Gal}(K/k), \prod_{v \in M_k \setminus S_k} \prod_{w|v} \widehat{\mathcal{O}}_{K,w}^\times \right) = 1$$

which implies the desired result. □

To compute $Q(\mathrm{Gal}(K/k), K_S)$, we'll use the usual theory of the log mapping of K_S into a lattice on the trace-zero hyperplane in $\mathbf{R}^{|S|}$. Let $\mathrm{Gal}(K/k)$ act on $\mathbf{R}^{|S|}$ by permuting the coordinates in the same way that $\mathrm{Gal}(K/k)$ permutes the absolute values in S (this works because we chose S large enough to be closed under this action). To be able to use this to compute the appropriate Herbrand quotient, we

[30] N.B. There's no way to use Lemma 5.12 to take infinite direct products out of Herbrand quotients.

need $\log(K_S)$ to be closed under the action of G. This is obviously true by the definition of $\log(K_S)$ and the fact that S is closed under the action of $\mathrm{Gal}(K/k)$. Moreover, log is compatible with the action of $\mathrm{Gal}(K/k)$. In particular, for $\alpha \in K_S$ we have

$$\log(g\alpha) = (\log |g\alpha|_w)_{w\in S} = (\log |\alpha|_{g^{-1}w})_{w\in S} = g(\log |\alpha|_w)_{w\in S}.$$

But still, $\log(K_S)$ has no obvious structure that makes it easy to compute its Herbrand quotient. Luckily, we have the following technical lemma, from [9, Ch. IX, §4, Theorem 1]:

Lemma 6.5. *Let L be a lattice in $\mathbf{R}^{|S|}$ which is also a $\mathrm{Gal}(K/k)$-submodule. Then L has a $\mathrm{Gal}(K/k)$-submodule L' of finite index with a $\mathbf{Z}$-basis $\{X_w\}_{w\in S}$ with the property that $gX_w = X_{gw}$ for all $g \in \mathrm{Gal}(K/k)$.*

Proof. Let $\{e_w\}$ be the standard basis for $\mathbf{R}^{|S|}$. For one $w_0|v$ for each $v \in S_k$, we can let $Z_{w_0} \in L$ be the closest element of L to $t\cdot e_{w_0}$ for a large enough positive real number t. Since L has full rank, there is a constant b such that $|Z_{w_0} - te_{w_0}| < b$[31] for all such w_0. This makes it an exercise in linear algebra to show that the Z_{w_0} (and the lattice we will define in terms of them) are linearly independent if t is sufficiently large.

To get the desired $\mathrm{Gal}(K/k)$-submodule, for each $w|v$ let

$$X_w = \sum_{\sigma\in D_{w_0}} g_{w_0,w}\sigma Z_{w_0}$$

where $g_{w_0,w}$ is a fixed element of $\mathrm{Gal}(K/k)$ such that $g_{w_0,w}w_0 = w$. This construction guarantees that X_w has the desired action of $\mathrm{Gal}(K/k)$. Choosing t large enough makes the X_w linearly independent elements of L, thus generating a sublattice of finite index. □

So in fact by Lemma 5.12 and Lemma 5.13, all lattices in $\mathbf{R}^{|S|}$ which are $\mathrm{Gal}(K/k)$-submodules have the same Herbrand quotient, and this Herbrand quotient is equal to

$$\begin{aligned} Q\left(\mathrm{Gal}(K/k), \prod_{v\in S_k}\prod_{w|v}\mathbf{Z}\cdot X_w\right) &= \prod_{v\in S_k} Q\left(\mathrm{Gal}(K/k), \prod_{w|v}\mathbf{Z}\cdot X_w\right) \\ &= \prod_{v\in S_k} Q(\mathrm{Gal}(K_w/k_v), \mathbf{Z}\cdot X_w) \\ &= \prod_{v\in S_k} [K_w : k_v] \end{aligned}$$

by Lemma 5.12, Lemma 5.16, Lemma 5.17, and the fact that $\mathrm{Gal}(K_w/k_v)$ has trivial action on $\mathbf{Z}\cdot X_w$. Thus we have done essentially all the hard work in the proof of the following

Lemma 6.6. *If $\mathrm{Gal}(K/k)$ is cyclic, then $Q(\mathrm{Gal}(K/k), K_S) = \frac{\prod_{v\in S_k}[K_w:k_v]}{[K:k]}$.*

Proof. Since $\log : K_S \to \mathbf{R}^{|S|}$ has finite kernel and respects the action of $\mathrm{Gal}(K/k)$, it follows from Lemma 5.12 and Lemma 5.13 that

$$Q(\mathrm{Gal}(K/k), K_S) = Q(\mathrm{Gal}(K/k), \log(K_S)).$$

[31] $|\cdot|$ denotes the sup norm on $\mathbf{R}^{|S|}$

We can't directly apply Lemma 6.5, since $\log(K_S)$ does not have full rank in $\mathbf{R}^{|S|}$. By the generalized unit theorem for S-units, it does have full rank in the trace-zero hyperplane. So if we let $X \in \mathbf{R}^{|S|}$ have coordinates all equal to 1, we know $\log(K_S) + \mathbf{Z} \cdot X$ is a lattice (of full rank) in $\mathbf{R}^{|S|}$. It is also clearly a $\mathrm{Gal}(K/k)$-submodule, since $\mathrm{Gal}(K/k)$ acts trivially on the extra component. So by Lemma 5.12 and the discussion following Lemma 6.5,

$$\begin{aligned} Q(\mathrm{Gal}(K/k), K_S) &= Q(\mathrm{Gal}(K/k), \log(K_S)) \\ &= \frac{Q(\mathrm{Gal}(K/k), \log(K_S) + \mathbf{Z} \cdot X)}{Q(\mathrm{Gal}(K/k), \mathbf{Z} \cdot X)} \\ &= \frac{\prod_{v \in S_k} [K_w : k_v]}{[K : k]}, \end{aligned}$$

as desired. □

We may finally put these together to obtain the second fundamental inequality.

Proposition 6.7. *If K/k is cyclic, then $[J_k : k^\times N_{K/k} J_K] \geq [K : k]$.*

Proof. Recall from the beginning of this section that

$$Q(\mathrm{Gal}(K/k), C_K) = \frac{Q(\mathrm{Gal}(K/k), J_{K,S})}{Q(\mathrm{Gal}(K/k), K_S)}.$$

By Lemma 6.6 and Prop 6.4, it follows that

$$Q(\mathrm{Gal}(K/k), C_K) = [K : k].$$

Therefore, $[K : k]|\hat{H}^0(\mathrm{Gal}(K/k), C_K)| = [C_k : N_{K/k} C_K] = [J_k : k^\times N_{K/k} J_K]$ which implies the desired result. □

Remark 6.8. Recall from Remark 6.3 that our proof that $L(1, \chi) \neq 0$ for nontrivial Heck characters χ implies that infinitely many primes in k do not split completely in K, so long as $I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ is not trivial. Notice that the second fundamental inequality proves that this is the case as long as K/k is cyclic and nontrivial (set $\mathfrak{m}$ to any admissible cycle for K/k).

6.3. **Global Artin reciprocity.** The historical strategy for the proof of the reciprocity law follows these steps, many of which rely on the two fundamental inequalities:

(1) The Artin map is surjective
(2) If $K \subset k(\zeta)$ for some root of unity ζ, then there exists a modulus $\mathfrak{m}$ for k such that
$$\ker\left(\left[\frac{K/k}{\cdot}\right] : I(\mathfrak{m}) \to \mathrm{Gal}(K/k)\right) = P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}).$$
(3) Extend (2) to the case where K/k is cyclic.
(4) Show that (3) implies the full result in the case where $\mathfrak{m}$ is any admissible cycle for any abelian extension K/k.

Steps (1), (2), and (4) are relatively simple exercises dealing with the formal properties of the Artin map. Step (3) was the main historical difficulty of the proof, and was only accomplished by Artin after Chebotarev proved his density theorem using a similar "field crossing" argument. The key insight is the construction of an auxiliary cyclotomic extension satisfying certain properties. We present the steps in order, relegating the construction of the auxiliary extension to an appendix.

Proposition 6.9 (Step 1)**.** *Let K/k be an arbitrary abelian extension, and $\mathfrak{m}$ any modulus of k divisible by the ramified primes so that the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$ is well-defined. Then the Artin map is surjective.*

Proof 1. Recall that the Chebotarev density theorem (see Theorem 1.2) can be proved independently of the main theorems of class field theory[32]. So the Artin map is surjective (in particular the preimage of any element of $\mathrm{Gal}(K/k)$ contains infinitely many primes). □

Proof 2. In the interest of keeping these notes self-contained, we present another proof which uses the second fundamental inequality (Proposition 6.7). Let $H \subset G(K/k)$ be the image of the Artin map, and suppose it is not equal to $\mathrm{Gal}(K/k)$. Then we can take its fixed field $K^H = F/k$. Since $H \neq \mathrm{Gal}(K/k)$, we know $[F : k] > 1$. And since $\mathrm{Gal}(K/k)$ is abelian, F/k is abelian as well (it is Galois since H is normal in $\mathrm{Gal}(K/k)$ and abelian as a result of its Galois group being a quotient of an abelian Galois group). Inductively choosing elements of $\mathrm{Gal}(F/k)$ and taking the fixed field of the cyclic subgroup they generate, we eventually get a tower $k = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots E_n \subseteq E_{n+1} = F$ such that E_i/E_{i-1} is cyclic (c.f. the proof of Lemma 5.21) and nontrivial. In particular, we have a cyclic extension E_1/k contained in F. Since F is the fixed field of H, the Artin symbol (with respect to K/k) of any prime in k not dividing $\mathfrak{m}$ acts trivially on F and therefore on E_1. By the functoriality of the Artin symbol[33], this implies that all but finitely many primes of k split completely in E_0. But E_0/k is cyclic and nontrivial, so Remark 6.8 shows that the opposite is true: infinitely many primes of k must not split completely. This shows that in fact $F = k$ and thus $H = \mathrm{Gal}(K/k)$, as desired. □

Now it remains to determine the kernel of the Artin map. In each step (2)-(4), the goal is to show the kernel is $P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})$.

Remark 6.10. $\mathfrak{N}(\mathfrak{m}) \subseteq \ker \left[\frac{K/k}{\cdot}\right]$ is already true by the basic properties of the Artin map (for example because $\left[\frac{K/k}{\mathfrak{p}}\right]$ has order $f(\mathfrak{P}|\mathfrak{p})$). If we can show that $P_\mathfrak{m} \subseteq \ker \left[\frac{K/k}{\cdot}\right]$, then it follows that $P_\mathfrak{m}\mathfrak{N}(\mathfrak{m}) \subseteq \ker \left[\frac{K/k}{\cdot}\right]$ and thus by Proposition 6.9 there is a surjective induced map $I(\mathfrak{m})/P_\mathfrak{m}\mathfrak{N}(\mathfrak{m}) \to \mathrm{Gal}(K/k)$, which is an isomorphism by Proposition 6.1 (the first fundamental inequality). So to prove Artin's reciprocity law for a modulus $\mathfrak{m}$ it suffices to show that $P_\mathfrak{m}$ is in the kernel of the Artin map.

Remark 6.11. When K/k is cyclic and $\mathfrak{m}$ is admissible for K/k, the second fundamental inequality also shows that it suffices to show that $\ker \left[\frac{K/k}{\cdot}\right] \subseteq P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})$. This is because the second inequality (Proposition 6.7, combined with Proposition 6.1 and Lemma 4.33) shows via the surjectivity of the Artin map (Proposition 6.9)

$$[I(\mathfrak{m})/P_\mathfrak{m}\mathfrak{N}(\mathfrak{m})] = [J_k : k^\times N_{K/k}J_K] = [K : k] = [I(\mathfrak{m}) : \ker \left[\frac{K/k}{\cdot}\right]],$$

[32] See [6, Ch. 6] or my math 229x final project. Note that the full strength of the theorem implies that even if K/k is not abelian, every conjugacy class in $\mathrm{Gal}(K/k)$ is hit by the Artin map.

[33] Alternatively, the general fact that splitting completely means you also split completely in any intermediate extension, via the multiplicativity in towers of the ramification index and inertial degree.

so the inclusion $\ker \left[\frac{K/k}{\cdot}\right] \subseteq P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ is enough to do step (3).

Proposition 6.12 (Step 2)**.** *Suppose that K is a cyclotomic extension of k, that is $K \subseteq k(\zeta_m)$ for some primitive m-th root of unity ζ. Then there is a modulus $\mathfrak{m}$ of k whose finite part is divisible only by primes lying over m such that the kernel of the corresponding Artin map is equal to $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$.*

Proof. If $\mathfrak{p}$ ramifies in K, then it ramifies in $k(\zeta_m)$, which means that it contains the relative discriminant $d_{k(\zeta_m)/k}$. This discriminant is by definition generated by the discriminants of all the k-bases of $k(\zeta_m)$ contained in $\mathcal{O}_{k(\zeta_m)}$, so it contains $\operatorname{disc}_{k(\zeta_m)/k}(1, \dots, \zeta_m^{[k(\zeta_m):k]-1})$ which must divide a power of m because ζ_m satisfies $X^m - 1 = 0$ (the reasoning is the same as in the discussion after [10, Ch. 2, Theorem 8]). This shows that as long as $\mathfrak{m}$ is chosen to be divisible by all the primes of k containing m, the Artin map $I(\mathfrak{m}) \to \operatorname{Gal}(K/k)$ is well-defined. By Remark 6.10, it suffices to show that we can choose $\mathfrak{m}$ so that $P_{\mathfrak{m}}$ is in the kernel of the Artin map. The key (as usual with cyclotomic fields) is to exploit the fact that the elements of $\operatorname{Gal}(k(\zeta_m)/k)$ are determined by where they send ζ_m. Since $\operatorname{Gal}(k(\zeta_m)/k)$ might not be all of $(\mathbf{Z}/m\mathbf{Z})^\times$, we should reduce to the case of $\mathbf{Q}(\zeta_m)/\mathbf{Q}$ first. In particular, if $\mathfrak{p}$ is a prime of k, then

$$\left[\frac{k(\zeta_m)/k}{\mathfrak{p}}\right] = \left[\frac{\mathbf{Q}(\zeta_m)/\mathbf{Q}}{\mathrm{N}\mathfrak{p}}\right]$$

when restricted to $\mathbf{Q}(\zeta_m)$[34]. This is because[35] the left hand side satisfies $\left[\frac{k(\zeta_m)/k}{\mathfrak{p}}\right] x \equiv x^{\mathrm{N}\mathfrak{p}} \mod \mathfrak{P}$ for $x \in k(\zeta_m)$ and therefore for $x \in \mathbf{Q}(\zeta_m)$, $\left[\frac{k(\zeta_m)/k}{\mathfrak{p}}\right] x \equiv x^{\mathrm{N}\mathfrak{p}} \mod \mathfrak{p}$ which is exactly the condition that uniquely determines $\left[\frac{\mathbf{Q}(\zeta_m)/\mathbf{Q}}{\mathrm{N}\mathfrak{p}}\right]$. Now we can directly use the description of the Artin map for a cyclotomic field to see that if $\mathfrak{a} \in I_k$ is divisible only by primes unramified in $k(\zeta_m)$, then (by the discussion on generalized ideal classes from Example 3.6)

$$\mathrm{N}\mathfrak{a} \in P_{mv_\infty} \implies \left[\frac{\mathbf{Q}(\zeta_m)/\mathbf{Q}}{\mathrm{N}\mathfrak{a}}\right] = \mathrm{id} \implies \left[\frac{k(\zeta_m)/k}{\mathfrak{a}}\right] = \mathrm{id} \implies \left[\frac{K/k}{\mathfrak{a}}\right] = \mathrm{id}$$

so we just need to find a modulus $\mathfrak{m}$ of k such that $(\alpha) \in P_{\mathfrak{m}} \implies N_{k/\mathbf{Q}}(\alpha) \in P_{mv_\infty}$ for $\alpha \in k^\times$ (then we can just enlarge $\mathfrak{m}$ to be divisible by all the ramified primes if needed). The continuous local norms on each coordinate induce a continuous map

$$\prod_{\substack{w \in M_k \\ w \mid m}} k_w^\times \to \prod_{\substack{v \in M_{\mathbf{Q}} \\ v \mid m}} \mathbf{Q}_v^\times.$$

whose v-coordinate is given by $\prod_{w|v} N_{K_w/\mathbf{Q}_v}$. If $\alpha \in k^\times$ is positive with respect to all $w|v_\infty$, then $N_{k/\mathbf{Q}}\alpha = \prod_{w|v_\infty} N_{k_w/\mathbf{Q}_v}\alpha$ is positive with respect to v_∞. The continuity of the map above implies (by the same product formula) the existence of a modulus $\mathfrak{m}_0$ of k containing only places lying over m such that $\alpha \in P_{\mathfrak{m}_0} \implies$

[34] The Frobenius is uniquely determined on $k(\zeta_m)$ because of this, since it is trivial on k

[35] This argument is not specific to cyclotomic fields. It's a special case of the general (almost tautological) fact that if K/k is Galois and E/k is an arbitrary finite extension, then $\left[\frac{KE/E}{\mathfrak{p}}\right]$ restricts on K to $\left[\frac{K/k}{\mathrm{N}_{E/k}\mathfrak{p}}\right]$

$N_{k/\mathbf{Q}}\alpha \in P_m$. Taking intersections, the modulus $\mathfrak{m} = \mathfrak{m}_0 \prod_{w|v_\infty} w$ has the desired property, so we are done. □

To deduce the cyclic case (step 3) from step 2, we need the following lemma, originally due to Artin and quoted directly from [9, §X.2]. This establishes the existence of the desired auxiliary cyclotomic extensions.

Lemma 6.13. *Let K/k be a finite cyclic extension of number fields, and S a finite set of rational primes. Let $\mathfrak{p}$ be a prime in k unramified in K. Then there exists a positive integer m not divisible by any element of S and a finite extension E/k such that*

(1) $K \cap E = k$, so $\operatorname{Gal}(KE/E) \cong \operatorname{Gal}(K/k)$.
(2) $K(\zeta_m) = E(\zeta_m)$ so that KE/E is a cyclotomic extension of E.
(3) $K \cap k(\zeta_m) = k$[36]
(4) $\mathfrak{p}$ splits completely in E.

Proof. See appendix. □

Suppose K/k is cyclic. By Remark 6.11, in order to show the reciprocity law for an admissible modulus $\mathfrak{f}$ of k, it suffices to show that the kernel of the Artin map for $I(\mathfrak{f})$ is contained in $P_\mathfrak{f}\mathfrak{N}(\mathfrak{f})$. It's clear that any prime in the kernel of the Artin map must be in $\mathfrak{N}(\mathfrak{f})$ since it splits completely and it therefore equal to the norm of any prime lying over it. In the general case, if $\mathfrak{a}$ is an arbitrary fractional ideal in the kernel, its prime factors are not guaranteed to be in the kernel. This is where the auxiliary extension from Lemma 6.13 comes into play.

Proposition 6.14 (Step 3)**.** *Let K/k be a cyclic extension of number fields, and $\mathfrak{f}(K/k)$ be an admissible cycle for K/k. Then the Artin map induces an isomorphism $I(\mathfrak{f})/P_\mathfrak{f}\mathfrak{N}(\mathfrak{f}) \to \operatorname{Gal}(K/k)$.*

Proof. By Remark 6.11 it suffices to show that $\ker \left[\frac{K/k}{\cdot}\right] \subseteq P_\mathfrak{f}\mathfrak{N}(\mathfrak{f})$. So let

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \in \ker \left[\frac{K/k}{\cdot}\right].$$

Since $\operatorname{Gal}(K/k)$ is cyclic, we can write

$$\left[\frac{K/k}{\mathfrak{p}}\right] = \tau^{n_\mathfrak{p}}$$

for each $\mathfrak{p}$, where τ is a generator for $\operatorname{Gal}(K/k)$. As a result,

$$1 = \left[\frac{K/k}{\mathfrak{a}}\right] = \tau^{\sum_\mathfrak{p} n_\mathfrak{p} v_\mathfrak{p}(\mathfrak{a})}$$

which means that

$$[K:k] | \sum_\mathfrak{p} n_\mathfrak{p} v_\mathfrak{p}(\mathfrak{a}).$$

In order to write things as norms, we need $\mathfrak{p}$ to split completely somewhere. So we use Lemma 6.13 to get the extensions $E_\mathfrak{p}/k$ where $\mathfrak{p}$ splits completely and satisfying the conditions (1)-(4), where $m_\mathfrak{p}$ can be chosen (by a suitable choice of S) to be

[36] I don't think this one is necessary. It is already implied by taking m coprime to d_K (see the proof of Step 3), and this must be done anyway in order to get the full product decomposition.

coprime to $\mathfrak{f}$, $\mathfrak{p}$, the other $m_\mathfrak{p}$'s, and the absolute discriminant of K. We can also take $E_\mathfrak{a}$ to be the compositum of all the $E_\mathfrak{p}$'s for $\mathfrak{p}|\mathfrak{a}$. Then

$$K \cap \mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}) = k \cap \mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}) = \mathbf{Q}$$

since the left hand side is an unramified extension of $\mathbf{Q}$ (in particular any ramified prime must ramify in $\mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})$ and therefore divides one of the $m_\mathfrak{p}$, which is impossible since such a prime couldn't ramify in K because the $m_\mathfrak{p}$ are coprime to d_K). This in turn means we have a diagram of field extensions, in which the fields horizontally across from each other are linearly disjoint[37]. As a result, the injective restriction homomorphism

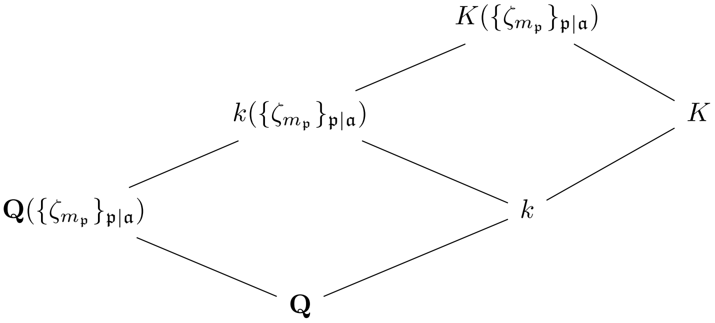
$K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})$
$k(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})$
K
$\mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})$
k
$\mathbf{Q}$

FIGURE 5.

$$\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/k) \to \mathrm{Gal}(K/k) \times \mathrm{Gal}(k(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/k) \cong \mathrm{Gal}(K/k) \times \mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/K)$$

is an isomorphism. Since the $m_\mathfrak{p}$ are pairwise coprime, the fields $\mathbf{Q}(\zeta_{m_\mathfrak{p}})$ are pairwise linearly disjoint[38], and for the same reason $\mathbf{Q}(\zeta_{m_\mathfrak{p}})$ is linearly disjoint from the compositum of any subset of the others. It follows that

$$\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/K) \cong \mathrm{Gal}(\mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/\mathbf{Q}) \cong \prod_{\mathfrak{p}} \mathrm{Gal}(\mathbf{Q}(\zeta_{m_\mathfrak{p}})/\mathbf{Q}).$$

Since the diagram in Figure 5 works just as well with only one root of unity at a time, we have $\mathrm{Gal}(\mathbf{Q}(\zeta_{m_\mathfrak{p}})/\mathbf{Q}) \cong \mathrm{Gal}(K(\zeta_{m_\mathfrak{p}})/K)$. Therefore, the restriction map

$$\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/K) \to \prod_{\mathfrak{p}} \mathrm{Gal}(K(\zeta_{m_\mathfrak{p}})/K)$$

is an isomorphism, so in fact restriction gives an isomorphism

$$\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/k) \cong \mathrm{Gal}(K/k) \times \prod_{\mathfrak{p}} \mathrm{Gal}(K(\zeta_{m_\mathfrak{p}})/K).$$

Note that $\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/E_\mathfrak{p})$ embeds into this product. Since $E_\mathfrak{p} \subseteq K(\zeta_{m_\mathfrak{p}})$, we see that fixing $E_\mathfrak{p}$ is independent of how an automorphism restricts to any of the other intermediate cyclotomic extensions, so we have (by restriction)

$$\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/E_\mathfrak{p}) \cong G \times \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathrm{Gal}(K(\zeta_{m_\mathfrak{p}})/K)$$

[37] This is because of the isomorphism $\mathrm{Gal}(K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/K) \cong \mathrm{Gal}(\mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})/(K \cap \mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}})))$, which implies (after repeating for k) $[K(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}) : K] = [k(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}) : k][\mathbf{Q}(\{\zeta_{m_\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}) : \mathbf{Q}]$.

[38] For example by the irreducibility of the cyclotomic polynomials over $\mathbf{Q}$

where $G = \mathrm{Gal}(K(\zeta_{\mathfrak{p}})/E_{\mathfrak{p}}) \subseteq \mathrm{Gal}(K/k) \times \mathrm{Gal}(K(\zeta_{\mathfrak{p}})/K) \cong \mathrm{Gal}(K(\zeta_{\mathfrak{p}})/k)$. Since $K \cap E_{\mathfrak{p}} = k$, we see that G fixing an element of K means that element must be in k. In other words, G contains an element of the form $(\tau, \tau_{\mathfrak{p}})$ where τ is a generator for $\mathrm{Gal}(K/k)$. This way, we see that

$$\mathrm{Gal}(K(\{\zeta_{m_{\mathfrak{p}}}\}_{\mathfrak{p}|\mathfrak{a}})/E_{\mathfrak{a}}) = \bigcap_{\mathfrak{p}|\mathfrak{a}} \mathrm{Gal}(K(\{\zeta_{m_{\mathfrak{p}}}\}_{\mathfrak{p}|\mathfrak{a}})/E_{\mathfrak{p}})$$

contains an element with $\mathrm{Gal}(K/k)$-coordinate τ. In particular, this Galois group restricts to K by fixing only k, which means $K \cap E_{\mathfrak{a}} = k$[39] and thus $\mathrm{Gal}(KE_{\mathfrak{a}}/E_{\mathfrak{a}}) \cong \mathrm{Gal}(K/k)$ by restriction. So by the surjectivity of the Artin map, there exists a fractional ideal $\mathfrak{b}$ of $E_{\mathfrak{a}}$ such that

$$\tau = \left[\frac{KE_{\mathfrak{a}}/E_{\mathfrak{a}}}{\mathfrak{b}}\right] = \left[\frac{K/k}{N_{E_{\mathfrak{a}}/k}\mathfrak{b}}\right]$$

and $\mathfrak{b}$, like $\mathfrak{p}$, is coprime to $\mathfrak{f}$ and all the $m_{\mathfrak{p}}$ (the first condition is there so that it has this in common with $\mathfrak{p}$; the secon is there so that its prime factors are unramified in $KE_{\mathfrak{a}} \subseteq K(\{\zeta_{m_{\mathfrak{p}}}\}_{\mathfrak{p}})$). By the transitivity of norms, $N_{E_{\mathfrak{a}}/k}\mathfrak{b} = N_{E_{\mathfrak{p}}/k}N_{E_{\mathfrak{a}}/E_{\mathfrak{p}}}\mathfrak{b}$, so this fractional ideal is a norm from $E_{\mathfrak{p}}$. Since $\mathfrak{p}$ splits completely in $E_{\mathfrak{p}}$, it is also such a norm. It follows that

$$\mathfrak{c} := \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} N_{E_{\mathfrak{p}}/k} N_{E_{\mathfrak{a}}/E_{\mathfrak{p}}} \mathfrak{b}^{-n_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{a})}$$

is a norm from $E_{\mathfrak{p}}$ as well. Since $\mathfrak{p}$ and $\mathfrak{b}$ are, we know that $\mathfrak{c}$ is coprime to $\mathfrak{f}$ and all the $m_{\mathfrak{p}}$, and thus $\mathfrak{c} = N_{E_{\mathfrak{p}}/k}\mathfrak{c}'$, where $\mathfrak{c}'$ is coprime to those as well. By definition of all this notation (dating back from the beginning of the proof), we know[40]

$$\left[\frac{KE_{\mathfrak{p}}/E_{\mathfrak{p}}}{\mathfrak{c}'}\right] = \left[\frac{K/k}{\mathfrak{c}}\right] = \left[\frac{K/k}{\mathfrak{p}}\right]^{v_{\mathfrak{p}}(\mathfrak{a})} \left[\frac{K/k}{N_{E_{\mathfrak{a}}/k}\mathfrak{b}}\right]^{-n_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{a})} = \mathrm{id}.$$

In particular, $\mathfrak{c}'$ is in the kernel of the Artin map from $I(\mathfrak{f}\prod_{\mathfrak{p}} m_{\mathfrak{p}})$. But $KE_{\mathfrak{p}} \subseteq E_{\mathfrak{p}}(\zeta_{m_{\mathfrak{p}}})$, so this extension is cyclotomic. By Step 2 (Proposition 6.12)[41], that kernel is contained in $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ [with respect to the extension $KE_{\mathfrak{p}}/E_{\mathfrak{p}}$] as long as $\mathfrak{m}$ is divisible by $\mathfrak{f}\prod m_{\mathfrak{p}}$. So we can write

$$\mathfrak{c}' = (\gamma) N_{KE_{\mathfrak{p}}/E_{\mathfrak{p}}}\mathfrak{C}$$

where $\mathfrak{C}$ is coprime to $\mathfrak{f}$ and the $m_{\mathfrak{p}}$'s, and γ is (arbitrarily) close to 1 with respect to the absolute values dividing $\mathfrak{f}$ and the $m_{\mathfrak{p}}$'s. By continuity of the local norms and the multiplicativity of the norm in towers, this means

$$\mathfrak{c} = N_{E_{\mathfrak{p}}/k}\mathfrak{c}' = (N_{E_{\mathfrak{p}}/k}\gamma) N_{KE_{\mathfrak{p}}/k}\mathfrak{C}$$

is in $P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})$ [with respect to $E_{\mathfrak{p}}/k$]. But $N_{KE_{\mathfrak{p}}/k}\mathfrak{C} = N_{K/k}N_{KE_{\mathfrak{p}}/K}\mathfrak{C}$, so we actually have $\mathfrak{c} \in P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})$ with respect to K/k. Doing this for each $\mathfrak{p}|\mathfrak{a}$ and expanding the

[39] Note that the only thing about the $E_{\mathfrak{p}}$'s that we used to conclude this was condition (1), which says the same thing for $E_{\mathfrak{p}}$, and the fact that the $m_{\mathfrak{p}}$'s are coprime to the right primes in order to make things linearly disjoint.

[40] The leftmost expression is well-defined because $\mathfrak{c}'$ is coprime to $m_{\mathfrak{p}}$ so its prime factors are unramified in $E_{\mathfrak{p}}(\zeta_{m_{\mathfrak{p}}})$.

[41] In that result, we can choose the modulus $\mathfrak{m}$ to be anything as long as it is sufficiently divisible by the primes lying over $m_{\mathfrak{p}}$; here we are somewhat more relaxed by setting $\mathfrak{m} = \mathfrak{f}\prod m_{\mathfrak{p}}$ so we only know the kernel is contained in this group

definition of $\mathfrak{c}$, we get[42]

$$\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} N_{E_{\mathfrak{a}}/k} \mathfrak{b}^{-\sum_{\mathfrak{p}} n_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{a})} \in P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{m}).$$

Of course, $\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} = \mathfrak{a}$ and $\sum_{\mathfrak{p}} n_{\mathfrak{p}} v_{\mathfrak{p}}$ is divisible by $[K : k]$, and therefore by $f(\mathfrak{P}|\mathfrak{p})$ for all primes $\mathfrak{p}$ of k. This shows $N_{E_{\mathfrak{a}}/k} \mathfrak{b}^{-\sum_{\mathfrak{p}} n_{\mathfrak{p}} v_{\mathfrak{p}}}$ is a norm from K, and thus $\mathfrak{a} \in P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{f})$ as desired. □

The full statement of the global reciprocity law follows directly from the cyclic case.

Theorem 6.15 (Step 4; Artin's global reciprocity law)**.** *Let K/k be an abelian extension, and $\mathfrak{m}$ an admissible cycle for K/k. Then the kernel of the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$ is equal to $P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})$.*

Proof. By Remark 6.10, it suffices to show that $P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})$ is contained in the kernel of the Artin map $I(\mathfrak{m}) \to \mathrm{Gal}(K/k)$. Let $\mathfrak{f}$ be the smallest admissible cycle for K/k. If we can show that $P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{f})$ is in the kernel, then so is $P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})$ since $P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m}) \subseteq P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{f})$ as $\mathfrak{f}|\mathfrak{m}$. As usual, write K as the compositum of cyclic extensions K_i/k. We can take the minimal admissible modulus $\mathfrak{f}_i$ for K_i/k, which we know by the usual norm index computations is divisible only by valuations that ramify in K_i, and thus only by $v|\mathfrak{f}$. In fact, the definition of admissible tells us that $\mathfrak{f}_i|\mathfrak{f}$, since taking norms (from completions) reverses inclusions. By Proposition 6.14, every fractional ideal of k coprime to $\mathfrak{f}$, which is therefore coprime to each $\mathfrak{f}_i$, is in the kernel of the Artin map for K_i/k if it is in $P_{\mathfrak{f}_i} \mathfrak{N}(\mathfrak{f}_i)$. If a fractional ideal $\mathfrak{a}$ is in $P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{f})$, then it is in $P_{\mathfrak{f}_i} \mathfrak{N}(\mathfrak{f}_i)$ (as $\mathfrak{f}_i|\mathfrak{f}$), and therefore in the kernel of the Artin map for all K_i/k. By the functoriality of the Artin symbol, and the fact that an automorphism of K/k is determined by its action on all the K_i's, it follows that $P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{f})$ is in the kernel of the Artin map for K/k, which completes the proof. □

Remark 6.16. The fact that $\mathfrak{m}$ is admissible, over the course of all four steps, is only used in two ways. The first is the more trivial one, which is just the fact that the admissible moduli are divisible by all the ramified primes (so the Artin map is well-defined). The second one is that the admissibility of $\mathfrak{m}$ allows for the isomorphism between $I(\mathfrak{m})/P_{\mathfrak{m}} \mathfrak{N}(\mathfrak{m})$ and $J_k/k^\times N_{K/k} J_K$, and thus the application of the second fundamental inequality to the idealic situation.

The reciprocity isomorphism has a clear interpretation as a "reciprocity law" in a sense analogous to (and far more general than) the law of quadratic reciprocity. In particular, it says that the splitting type of a prime in an abelian extension is determined (up to finitely many exceptions) by a congruence condition. As a result can obtain the classical reciprocity laws by specializing to fields of low degree. In fact, Artin conjectured the isomorphism in order to establish the equivalence between Hecke and Artin L-functions in the abelian case, and did not prove it until several years after he showed that it implied the classical reciprocity laws.

[42] This is where we use the fact that $\mathfrak{b}$ is the same ideal, in $E_{\mathfrak{a}}$, for each $\mathfrak{p}$, rather than an ideal in $E_{\mathfrak{p}}$ that depends on $\mathfrak{p}$

6.4. **The class field correspondence.** Let K/k be an abelian extension of number fields as usual. By Lemma 4.33, the global reciprocity law establishes, via the isomorphism[43]

$$\mathrm{Gal}(K/k) \cong I(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}) \cong J_k/k^{\times}N_{K/k}J_K.$$

Definition 6.17. The *idèlic Artin map* for K/k is the map[44] $\theta_{K/k} : J_k \to \mathrm{Gal}(K/k)$ defined by lifting the isomorphism $J_k/k^{\times}N_{K/k}J_K \to \mathrm{Gal}(K/k)$. It does not depend on the choice of admissible modulus $\mathfrak{m}$.

Of course, it doesn't really matter that the idèlic Artin map does not depend on $\mathfrak{m}$. We could choose a specific $\mathfrak{m}$ (for example the smallest admissible modulus), and we would still know that the idèlic Artin map has kernel $k^{\times}N_{K/k}J_K$. Of course, we require in any event the global reciprocity law for ideals in order to make the idèlic statement well-defined. The idèlic Artin map is useful because it expresses the subgroup $k^{\times}N_{K/k}J_K$ as the kernel of a map whose properties we are much more familiar with.

It also clearly satisfies the properties we expect of the "Artin map."

Lemma 6.18. *Let $k \subseteq K \subseteq K'$ be a tower of extensions of number fields such that K/k and K'/k are abelian. Then for any $a \in J_k$, $\theta_{K'/k}(a)$ restricts on K to $\theta_{K/k}$.*

Proof. Let $a \in J_k$, and take $\mathfrak{m}$ to be a modulus for k which is admissible for K/k and therefore for K'/k. Then we can select (via weak approximation) $\alpha \in k^{\times}$ such that $\alpha a \in J_{\mathfrak{m}}$, and we know (via the description of the isomorphism from Lemma 4.33) that

$$\theta_{K/k}(a) = \left[\frac{K/k}{\psi(\alpha a)}\right], \qquad \theta_{K'/k}(a) = \left[\frac{K'/k}{\psi(\alpha a)}\right]$$

since $\mathfrak{m}$ is admissible for both extensions. So it's clear from the corresponding property of the idealic Artin map that these restrict to the same automorphism of K/k. □

Remark 6.19. Notice that if $a_v = 1$ at all valuations v which ramify in K, then there is no need to multiply by an element of $k^{\times}$ to get an element of $J_{\mathfrak{m}}$, since the minimal admissible cycle is only divisible by ramified places. As a result, the local Artin map is very easy to define directly for unramified extensions.

Lemma 6.20. *Let K/k be an abelian extension, E/k an arbitrary finite extension, and $a \in J_E$. Then $\theta_{KE/E}(a) \in \mathrm{Gal}(KE/E)$ restricts on K to $\theta_{K/k}(N_{E/k}a)$.*

Proof. Let $\mathfrak{f}$ be the minimal admissible cycle for K/k, and let $\mathfrak{m}$ be an admissible modulus for KE/E with the additional property that $N_{E/k}(J_{E,\mathfrak{m}}) \subseteq J_{k,\mathfrak{f}}$ (the idèle norm is continuous). We can select $\alpha \in E^{\times}$ such that $\alpha a \in J_{E,\mathfrak{m}}$. Then

$$(N_{E/k}\alpha)(N_{E/k}a) \in J_{k,\mathfrak{f}}$$

[43] All of these isomorphisms factor through the map induced by the inclusion $I(\mathfrak{m}) \to I(\mathfrak{f}(K/k))$, so they yield the same definition of the idèlic Artin map.

[44] We will denote it by $\theta_{K/k}$ specifically to distinguish it from the idealic Artin map.

so

$$\begin{aligned}\theta_{KE/E}(a) &= \left[\frac{KE/E}{\psi(\alpha a)}\right] \\ &= \left[\frac{K/k}{N_{E/k}\psi(\alpha a)}\right] \\ &= \left[\frac{K/k}{\psi((N_{E/k}\alpha)(N_{E/k}a))}\right] \\ &= \theta_{K/k}(N_{E/k}a)\end{aligned}$$

when restricted to K, as desired. □

The fact that the idèlic Artin map has kernel $k^\times N_{K/k}J_K$ immediately implies the following correspondence:

Theorem 6.21. *Let K, K' be finite abelian extensions of a number field k. Then $K \subseteq K'$ if and only if $k^\times N_{K/k}J_K \supseteq k^\times N_{K'/k}J_{K'}$.*

Proof. If $K \subseteq K'$, then $N_{K'/k}J_{K'} \subseteq N_{K/k}J_K$ by the transitivity of the norm. So it suffices to prove the converse. Suppose that $k^\times N_{K'/k}J_{K'} \subseteq k^\times N_{K/k}J_K$. In other words,

$$\ker\theta_{K'/k} \subseteq \ker\theta_{K/k}$$

which implies by Lemma 6.18 and the fact that an element of $\mathrm{Gal}(KK'/k)$ is determined by its restrictions to K and K' that

$$\ker\theta_{KK'/k} = \ker\theta_{K'/k} \cap \ker\theta_{K/k} = \ker\theta_{K'/k}.$$

It suffices to show that $KK' = K'$, i.e. $[KK' : k] = [K' : k]$. By the global reciprocity law, we know $[KK' : k] = [J_k : \ker\theta_{KK'/k}]$ which is equal to $[J_k : \ker\theta_{K'/k}] = [K' : k]$ so we are done. □

Remark 6.22. Compare Theorem 6.21 and its proof to the consequence of the Chebotarev density theorem which says that an abelian extension is uniquely determined by the primes in the kernel of the Artin map (see Theorem 6.3).

As a result of Theorem 6.21, we have an inclusion-reversing correspondence between the abelian extensions K/k and the subgroups of J_k of the form $k^\times N_{K/k}J_K$. It immediately implies an abelian extension K/k is uniquely determined by the subgroup $k^\times N_{K/k}J_K \subseteq J_k$. In this correspondence, the field K is called the *class field* for the *class group* $k^\times N_{K/k}J_K \subseteq J_k$. It turns out that any open subgroup of J_k (which we saw is always of finite index) is actually the class group for an abelian extension of k. This is called the **existence theorem**. In the general case, the explicit construction of class fields is still an open problem. We will explain how it is done in the local setting (Lubin-Tate theory), and in the global setting over $\mathbf{Q}$ (Kronecker–Weber) and imaginary quadratic fields (elliptic curves with complex multiplication). The general global existence theorem is therefore nonconstructive. The strategy is to show that every open subgroup of J_k contains a subgroup that has a class field (so this subgroup can be chosen to have a very convenient form). This is valid due to the following lemma:

Lemma 6.23. *Let $H_1 \subseteq H_2$ be subgroups of J_k and suppose that H_1 has a class field K_1/k. Then H_2 has a class field $K_2 \subseteq K_1$, and it is equal to the fixed field of $\theta_{K_1/k}(H_2)$.*

Proof. Let $K_2 = K_1^{\theta_{K_1/k}(H_2)} \subseteq K_1$ as suggested by the statement. Recall that $\theta_{K_2/k}$ is just the restriction of $\theta_{K_1/k}$ to K_2 by Lemma 6.18. So

$$\begin{aligned}\ker\theta_{K_2/k} &= \{a \in J_k : \theta_{K_1/k}(a)|_{K_2} = \mathrm{id}\}\\ &= \{a \in J_k : \theta_{K_1/k}(a) \in \theta_{K_1/k}(H_2)\}\\ &= H_2\end{aligned}$$

since any element of this set differs from an element of H_2 by an element of $\ker\theta_{K_1/k} = H_1 \subseteq H_2$, so in fact it must be in H_2. This means K_2 is the desired class field for H_2. □

One application of this lemma is that it suffices to prove the existence theorem for some (conveniently chosen) abelian extension F/k. In particular, if J_k/H has exponent n, if H has class field K/k then we expect $\mathrm{Gal}(K/k) \cong J_k/H$ to also have exponent n. This is only useful (via Kummer theory) if k contains a primitive n-th root of unity, so we want a proof of the existence theorem for $F = k(\zeta_n)$ to imply it for k. Since any abelian extension can be decomposed into a tower of cyclic extensions, it suffices to prove the reduction for cyclic steps. It takes the following form:

Lemma 6.24. *Let H be an open subgroup of J_k containing $k^\times$, and F/k a cyclic extension. By the continuity of the idèle norm, $N_{F/k}^{-1}(H) \subseteq J_F$ is an open subgroup, and it clearly contains $k^\times$. If the existence theorem holds for F, this means that $N_{F/k}^{-1}(H)$ has a class field over F. The statement of the lemma is that this implies that H has a class field over k.*

Proof. Let K be the class field over F for $N_{F/k}^{-1}(H)$. It is an abelian extension of F. We will show that in fact K is also a class field over k for a subgroup of H (this suffices by Lemma 6.23). There are three things we need:

- K/k is Galois.[45]
- $\mathrm{Gal}(K/k)$ is abelian.[46]
- $k^\times N_{K/k}J_K \subseteq H$.

The third point is actually obvious, because $F^\times N_{K/F}J_K = N_{F/k}^{-1}(H)$, so

$$N_{F/k}F^\times N_{K/k}J_K \subseteq H.$$

This means that $N_{K/k}J_K \subseteq H$. The same is true of $k^\times$, so indeed $k^\times N_{K/k}J_K \subseteq H$. So it remains to verify that K/k is Galois with abelian Galois group. To show it is Galois, we let K' be the Galois closure of K/k and show that every element of $\mathrm{Gal}(K'/k)$ restricts to an automorphism of K. Let $\sigma \in \mathrm{Gal}(K'/k)$. Since F is Galois over k, we know that σ restricts to an automorphism of F. Since norms from F to k are invariant under applying an automorphism of F/k, we know that $\sigma N_{F/k}^{-1}(H) = N_{F/k}^{-1}(H)$. Moreover, the fact that K is a class field for $N_{F/k}^{-1}(H)$ means that

$$F^\times N_{K/F}J_K = N_{F/k}^{-1}(H)$$

[45] N.B. It isn't generally true that if L/K is Galois and K/k is Galois, then L/k is Galois. For example consider $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(2^{1/4})$. This proof needs to use the fact that K is the class field for something.

[46] This is the part where F/k being cyclic helps.

and thus after applying σ,

$$(\sigma F)^\times \sigma N_{K/F} J_K = N_{F/k}^{-1}(H).$$

Since F/k is Galois, $\sigma F = F$. And

$$\begin{aligned}\sigma N_{K/F} J_K &= \sigma \left\{ \prod_{\tau \in \mathrm{Gal}(K/F)} \tau a : a \in J_K \right\} \\ &= \left\{ \prod_{\tau \in \mathrm{Gal}(K/F)} \sigma\tau a : a \in J_K \right\} \\ &= \left\{ \prod_{\tau \in \mathrm{Gal}(\sigma K/F)} \sigma\sigma^{-1}\tau\sigma a : a \in J_K \right\} \\ &= N_{\sigma K/F} J_{\sigma K}.\end{aligned}$$

It follows that K and σK are both class fields over F for $N_{F/k}^{-1}(H)$, and thus they are equal by the uniqueness of class fields (a consequence of Theorem 6.21). this proves that K/k is Galois. We know K/F is abelian and F/k is cyclic. From the isomorphism $\mathrm{Gal}(F/k) \cong \mathrm{Gal}(K/k)/\mathrm{Gal}(K/F)$, every element of $\mathrm{Gal}(K/k)$ is equal to $\tau \circ \sigma_F^n$ where σ_F is an element of $\mathrm{Gal}(K/k)$ restricting to a generator of $\mathrm{Gal}(F/k)$ and $\tau \in \mathrm{Gal}(K/F)$. To show $\mathrm{Gal}(K/k)$ is abelian, it suffices to show that every $\tau \in \mathrm{Gal}(K/F)$ commutes with $\sigma_F \in \mathrm{Gal}(K/k)$ restricting to a generator of $\mathrm{Gal}(F/k)$. As usual we take advantage of the Artin symbol and reciprocity law to prove this. In particular, $\tau = \theta_{K/F}(a)$ for some $a \in J_F$, so

$$\sigma_F \circ \tau \circ \sigma_F^{-1} = \theta_{K/F}(\sigma_F a).$$

Furthermore, the fact that $N_{F/k}(\sigma_F a) = N_{F/k}(a)$ means that $(\sigma_f a)/a \in N_{F/k}^{-1}(H)$ and since K is the class field for that group, we know that in fact

$$\sigma_F \circ \tau \circ \sigma_F^{-1} = \theta_{K/F}(\sigma_F a) = \theta_{K/F}(a) = \tau,$$

so these two automorphisms commute as desired. □

Now let k be a number field and H an open subgroup of J_k containing $k^\times$. Then H is of finite index in J_k since $J_k/H \cong C_k/\pi(H)$ and any open subgroup of C_k has finite index. So J_k/H has some finite exponent n. By Lemma 6.24, it suffices to prove that $N_{F/k}^{-1}(H)$ has a class field over F for some cyclic extension F/k. Let $a \in J_F$. We know that $N_{F/k}a^n = (N_{F/k}a)^n \in H$, so $a^n \in N_{F/k}^{-1}H$. It follows that $J_F/N_{F/k}^{-1}H$ has exponent n[47]. By going up cyclic extensions, this means (by Lemma 6.24) we can reduce the case of J_k/H having exponent n to the case where J_F/H has exponent n and F is an arbitrary finite abelian extension of k. In particular, we can let $F = k(\zeta_n)$, so that by using Lemma 6.24 inductively on a tower of cyclic extensions from k to F, it suffices (by the previous discussion) to show that if F contains ζ_n, then every open subgroup H of J_F containing $F^\times$ with the property that J_F/H has exponent n has a class field over F. We expect to be able to use Kummer theory to construct the desired class field, since F contains ζ_n

[47] N.B. here by a group G with exponent n we just mean that $g^n = 1$ for all $g \in G$. We do not mean the smallest such n.

and if K/F is that class field, we know that $\mathrm{Gal}(K/F) \cong J_F/H$ will have exponent n. We can also assume $n > 2$, since if n is an exponent for J_k/H then so is $3n$.

Theorem 6.25 (Existence theorem, idèlic version)**.** *Suppose F is a number field containing ζ_n, and $H \subseteq J_F$ such that J_F/H has exponent n. Then H has a class field.*

Proof. Since J_F/H has exponent n, we know that for any finite set $S \subseteq M_F$ containing all the archimedean places and all v such that $1 \times \cdots \times \widehat{\mathcal{O}}_{F,v}^\times \times \cdots \nsubseteq H$ (only finitely many v have this property because of the definition of the open sets of J_F),

$$B := \prod_{v \in S} (F_v^\times)^n \times \prod_{v \in M_F \setminus S} \widehat{\mathcal{O}}_{F,v}^\times \subseteq H.$$

So by Lemma 6.23, it suffices to show that $k^\times B$ has a class field over F. This class field needs to have exponent n, so (if it exists) it will be a Kummer extension of F. Such an extension is obtains by adjoining n-th roots of elements of F. In fact, we will do it by adjoining the n-th roots of every element of F_S (which makes sense given the definition of B), taking

$$K = F(F_S^{1/n}).$$

It's easier if K/F is unramified at all v outside of S, so that all the $\widehat{\mathcal{O}}_{F,v}^\times$ are all in the norm group. To do this, we recall that $\mathfrak{p}$ ramifies in K if and only if it ramifies in at least one of the extensions $F(\alpha^{1/n})$. The relative discriminant of $F(\alpha^{1/n})/F$ divides the discriminant of the power basis generated by $\alpha^{1/n}$, which is

$$N_{F(\alpha^{1/n})/F}(n\alpha^{(n-1)n}).$$

Since $\alpha \in F_S$, this norm has trivial valuation at every valuation outside of S except those dividing n. But we might as well enlarge S to include all $\mathfrak{p}|n$, so that this norm has trivial valuation outside S and therefore K/F is unramified outside S by the properties of the relative discriminant. It follows that for all $v \in M_F \setminus S$, each element of $\widehat{\mathcal{O}}_{F,v}^\times$ (embedded in J_F by 1's at all the other places) is a norm from J_K. To show that $B \subseteq k^\times N_{K/F} J_K$, it remains to show that $(F_v^\times)^n \subseteq F^\times N_{K/F} J_K$ when embedded in the same way. Of course, the right hand side is just the kernel of the Artin map for K/F, whose Galois group has exponent n (by Kummer theory), so this is clearly true. It remains to show the opposite inclusion, which we will do by showing that

$$[J_F : F^\times B] = [J_F : k^\times N_{K/F} J_K].$$

We might as well compute them directly. The right hand side is $[K : F]$ by global class field theory. Since K was defined as a Kummer extension, we know by Kummer theory that

$$[K : F] = [(F^\times)^n F_S : (F^\times)^n].$$

By one of the "isomorphism theorems",

$$\frac{(F^\times)^n F_S}{(F^\times)^n} \cong F_S/((F^\times)^n \cap F_S) = F_S/F_S^n,$$

but by the unit theorem for the S-units,

$$F_S \cong \mathbf{Z}^{|S|-1} \times \mu_F.$$

As a result,

$$F_S/F_S^n \cong \frac{\mathbf{Z}^{|S|-1} \times \mu_F}{(n\mathbf{Z})^{|S|-1} \times \mu_F^n}.$$

The fact that F contains ζ_n means that the surjective n-th power map $\mu_F \to \mu_F^n$ has kernel equal to $\langle \zeta_n \rangle$ (this uses the fact that $\zeta_n \in F$) and thus $|\mu_F| = n|\mu_F^n|$, which means

$$[K : F] = n^{|S|}.$$

It remains to check that this agrees with $[J_F : F^\times B]$. Since J_F is too hard to deal with, we further enlarge S so that $J_F = F^\times J_{F,S}$ (see Lemma 4.17). So we may rewrite

$$[J_F : F^\times B] = [F^\times J_{F,S} : F^\times B].$$

There is also an isomorphism

$$F^\times J_{F,S}/F^\times B \cong J_{F,S}/(F^\times B \cap J_{F,S}).$$

The right hand side has size

$$\frac{[J_{F,S} : B]}{[F^\times B \cap J_{F,S} : B]} = \frac{[J_{F,S} : B]}{[F^\times \cap J_{F,S} : F^\times \cap B]}$$

which comes from the isomorphism[48] $(F^\times \cap J_{F,S})/(F^\times \cap B) \to (F^\times B \cap J_{F,S})/B$. So in the end we have

$$[J_F : F^\times B] = \frac{[J_{F,S} : B]}{[F_S : F^\times \cap B]}.$$

We compute the denominator first. We claim that $F^\times \cap B = F_S^n$ so that from our previous computation the denominator is equal to $n^{|S|}$. The inclusion $F_S^n \subseteq F^\times \cap B$ is obvious from the definition of B. So it suffices to show that $F^\times \cap B \subseteq F_S^n$. Let $\alpha \in F^\times \cap B$. Then α is a local n-th power for each $v \in S$, which means that

$$\alpha^{1/n} \in F_v^\times$$

and thus $F(\alpha^{1/n})_w = F_v$, which means that $[F(\alpha^{1/n})_w : F_v] = 1$ and so v splits completely in $F(\alpha^{1/n})$. We also know (from the fact that S contains all the archimedean valuations and the $\mathfrak{p}|n$) that $F(\alpha^{1/n})/F$ is unramified outside of S. Thus,

$$J_{F,S} \subseteq N_{F(\alpha^{1/n})/F} J_{F(\alpha^{1/n})}$$

because our analysis of the splitting of the $v \in M_F$ in $F(\alpha^{1/n})$ means that $\widehat{\mathcal{O}}_{F,v}^\times = N_{F(\alpha^{1/n})/F} \widehat{\mathcal{O}}_{F(\alpha^{1/n}),v}^\times$ for v outside of S and $F_v^\times = N_{F(\alpha^{1/n})/F} F(\alpha^{1/n})_w^\times$ for v in S. Since $J_F = F^\times J_{F,S}$, this implies that

$$J_F \subseteq F^\times N_{F(\alpha^{1/n})/F} J_{F(\alpha^{1/n})}$$

so in fact

$$J_F = F^\times N_{F(\alpha^{1/n})/F} J_{F(\alpha^{1/n})}.$$

Since $F(\alpha^{1/n})$ is an abelian extension of F, this means it is the class field for all of J_F, so it must coincide with F. Therefore, α is an n-th power in F. Since $\alpha \in B$

[48] It is an isomorphism because the natural map $F^\times \cap J_{F,S} \to (F^\times B \cap J_{F,S})/B$ has kernel $B \cap F^\times \cap J_{F,S} = B \cap F^\times$ since $B \subseteq J_{F,S}$

in fact it must be an n-th power in F_S. So we have proven the opposite inclusion $F^\times \cap B \subseteq F_S^n$, which means

$$[F_S : F^\times \cap B] = [F_S : F_S^n] = n^{|S|}$$

by our previous computation. Finally, we show that $[J_{F,S} : B] = n^{2|S|}$, which will prove that $[J_F : F^\times B] = n^{|S|} = [K : F] = [J_F : F^\times N_{K/F} J_K]$ and thus that K is the desired class field. By definition of B,

$$[J_{F,S} : B] = \prod_{v \in S} [F_v^\times : (F_v^\times)^n].$$

So we need to show that $[F_v^\times : (F_v^\times)^n] = n^2$. From the fact that $F_v^\times \cong \widehat{\mathcal{O}}_{F,v}^\times \times \mathbf{Z}$, we know that if v is nonarchimedean, then

$$[F_v^\times : (F_v^\times)^n] = n[\widehat{\mathcal{O}}_{F,v}^\times : (\widehat{\mathcal{O}}_{F,v}^\times)^n].$$

Since F contains ζ_n and $n > 2$, F has no real archimedean places. Since every element of $\mathbf{C}^\times$ is an n-th power, this means the only contribution is in fact from the nonarchimedean elements of S. Moreover, if $v = v_\mathfrak{p}$, then

$$[\widehat{\mathcal{O}}_{F,v}^\times : (\widehat{\mathcal{O}}_{F,v}^\times)^n] = \frac{1}{|n|_\mathfrak{p}} n$$

(this is easy to deduce using the same $\mathfrak{p}$-adic logarithm trick from Lemma 4.7 and the fact that F contains ζ_n). So

$$\begin{aligned}
[[J_{F,S} : B] &= \prod_{v \in S} [F_v^\times : (F_v^\times)^n] \\
&= \prod_{v \in S \setminus S_\infty} n[\widehat{\mathcal{O}}_{F,v}^\times : (\widehat{\mathcal{O}}_{F,v}^\times)^n] \\
&= n^{2|S| - 2|S_\infty|} \prod_{\mathfrak{p} \in S \setminus S_\infty} \frac{1}{|n|_\mathfrak{p}} \\
&= n^{2|S| - 2|S_\infty|} \prod_{v \in S_\infty} |m|_v \\
&= n^{2|S|},
\end{aligned}$$

where the second-to-last inequality follows from the product formula because the nonarchimedean primes outside of S all do not divide n, and the last equality is because all of these v are complex and $m \in \mathbf{Z}$. so the normalized valuation is $|m|_v = m^2$. This proves the desired result by the previous discussion. □

For the purposes of studying primes in generalized ideal classes, it might be instructive to look at what the class fields correspond to in the setting of ideal classes. Let $\mathfrak{m}$ be a modulus of K. Recall from section 4 that we have an isomorphism

$$J_K / K^\times W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m},$$

which is induced by the map $J_\mathfrak{m} \to I(\mathfrak{m})$ taking $(a_\mathfrak{p})_\mathfrak{p} \mapsto \prod \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$. Under this map, the open subgroups of J_K containing $K^\times W_\mathfrak{m}$ correspond[49] to the subgroups

[49] Indeed, $K^\times W_\mathfrak{m}$ is an open (and therefore closed) subgroup of finite index, and J_K is Hausdorff, so $J_K/K^\times W_\mathfrak{m}$ is a finite group with the discrete topology. Hence all the subgroups of $I(\mathfrak{m})/P_\mathfrak{m}$ are images of an open subgroup under the isomorphism.

of $I(\mathfrak{m})$ containing $P_{\mathfrak{m}}$. So we might as well state the existence theorem in the setting of ideals:

Theorem 6.26 (Existence theorem for ideals). *Let $\mathfrak{m}$ be a modulus for K. Then for every intermediate subgroup $P_{\mathfrak{m}} \subseteq H \subseteq I(\mathfrak{m})$, there is an abelian extension L/K such that $H = P_{\mathfrak{m}} N(\mathfrak{m})$ and $\mathfrak{m}$ is admissible for L/K.*

Proof. This is basically a direct corollary of the idèlic statement of the existence theorem and local class field theory. Let H be a subgroup between $P_{\mathfrak{m}}$ and $I(\mathfrak{m})$. Then through the (topological) isomorphism $J_K/K^\times W_{\mathfrak{m}} \cong I(\mathfrak{m})/P_{\mathfrak{m}}$, H corresponds to an open subgroup B of J_K containing $K^\times W_{\mathfrak{m}}$. The idèlic existence theorem tells us that there is a finite abelian extension L/K such that

$$K^\times N_{L/K}(J_L) = B \supseteq K^\times W_{\mathfrak{m}}.$$

In particular, $K^\times N_{L/K}(J_L) \supseteq W_{\mathfrak{m}}$, which actually implies $\mathfrak{m}$ is admissible[50] □

7. Local Class Field Theory

7.1. The local Artin map.

7.2. Local-global compatibility.

7.3. Conductors and the Artin character.

7.4. The local cyclic norm index inequality.

8. Consequences

8.1. Computation of Ray Class fields.

Let K be a number field. Since $K^\times N_{L/K}(J_L)$ is open in J_K, any abelian extension L/K has the property that

$$K^\times N_{L/K}(J_L) \supseteq K^\times W_{\mathfrak{m}}$$

for some modulus $\mathfrak{m}$ of K (in fact we saw from local class field theory that this is true if and only if $\mathfrak{m}$ is admissible for L/K). Then the inclusion-reversing class field correspondence (which we proved in Theorems 6.21 and 6.25) says that L is contained in the class field of $\mathfrak{m}$. So if we can compute the ray class field for an arbitrary modulus (or any set of moduli with the property that every modulus divides one of them), then we can prove a theorem analogous to Kronecker–Weber along the lines of "every abelian extension of K is contained in an extension of the form [...]", where in this case [...] is the class field corresponding to $K^\times W_{\mathfrak{m}}$. Such a class field is called a *ray class field* because of the isomorphism $J_K/K^\times W_{\mathfrak{m}} \cong I(\mathfrak{m})/P_{\mathfrak{m}}$ which means that in terms of ideals it is the class field corresponding to $P_{\mathfrak{m}} \subseteq I(\mathfrak{m})$, with Galois group equal to the ray class group $I(\mathfrak{m})/P_{\mathfrak{m}}$.

Theorem 8.1 (Global Kronecker–Weber). *Let L be an abelian extension of $\mathbf{Q}$. Then $L \subseteq \mathbf{Q}(\zeta_f)$ for some positive integer f.*

[50] This is where the use of local class field theory comes in. In particular, from the corollary to Theorem 3 of Chapter XI of Lang, taking intersections with $K_v^\times$, for all $v \in M_K$ we get $N_{L_w/L_v} L_w^\times = K^\times N_{L/K} J_L \cap K_v^\times \supseteq W_{\mathfrak{m}}(v)$ which is the definition of $\mathfrak{m}$ being admissible.

Proof. By the previous remarks, it suffices to compute the ray class field corresponding to nv_∞ for any positive integer n. Here we are assuming that the class group for L contains $K^\times W_{nv\infty}$ and therefore that nv_∞ is admissible for $L/\mathbf{Q}$. By the uniqueness of class fields (a consequence of the inclusion-reversing part of the correspondence), it suffices to show that $\mathbf{Q}^\times W_{nv_\infty}$ is the kernel H of the Artin map $J_\mathbf{Q} \to \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. First of all, we know that

$$J_\mathbf{Q}/\mathbf{Q}^\times W_{nv_\infty} \cong I_\mathbf{Q}(nv_\infty)/P_{\mathfrak{n}\mathfrak{v}_\infty} \cong (\mathbf{Z}/n\mathbf{Z})^\times$$

(this was one of the two examples of ray class groups I actually know how to compute). On the other hand, by the surjectivity of the Artin map

$$J_\mathbf{Q}/H \cong \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$$

as well, so we only need to prove one inclusion, say

$$K^\times W_{nv\infty} \subseteq H.$$

In fact in the definition of the idèlic Artin map we know $K^\times$ maps to $\mathrm{id} \in \mathrm{Gal}(L/K)$, we just need to show that $W_{nv_\infty} \subseteq H$. The problem is that we don't know that nv_∞ is admissible for $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ yet, so we need to choose some $n|m$ such that mv_∞ is admissible for $\mathbf{Q}(\zeta_n)/\mathbf{Q}$. Now let $\alpha \in W_{nv_\infty}$. To take the corresponding ideal, we need to multiply by an element of $K^\times$ to put α in W_{mv_∞}. By the Chinese remainder theorem, there is a positive integer a such that $a \equiv \alpha_p^{-1} \mod p^{v_p(m)}$, so that $a\alpha \in W_{mv_\infty}$. Since $n|m$, outside of mv_∞, $a\alpha$ has valuation $v(a)$, which means the corresponding ideal in $\mathbf{Q}$ is (a), and thus the Artin symbol is $a \in (\mathbf{Z}/n\mathbf{Z}) = \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. This only depends on the residue class of a mod n, and since $\alpha \in W_{nv_\infty}$, the definition of a means $a \equiv 1 \mod p^{v_p(n)}$ for all $p|n$, and so we have proved α has trivial Artin symbol in $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}$ as desired. □

In general, the ray class groups are more complicated and there are few other cases where the ray class fields have such a simple form (though in practice algorithms like those in [2, Ch. 4–5] can be used to compute the ray class field for a given modulus using the same Kummer theory procedure as in the proof of the existence theorem).

8.2. **The Hilbert class field.** Let K be a number field. From local class field theory and the fact that the class field correspondence is inclusion-reversing, the class field corresponding to

$$K^\times J_{S_\infty}$$

is the maximal unramified abelian extension of K (if L'/K is an abelian extension of K with class group $H' \subseteq J_K$, then $H' \cap \mathcal{O}_{K,v}^\times = N_{L'_w/K_v}\mathcal{O}_{L',v}^\times$, so L'/K is unramified if and only if H' contains $\mathcal{O}_{K,v}^\times$ for all nonarchimedean v and it contains $K_v^\times$ for all $v \in S_\infty$, i.e. if and only if H' contains $K^\times J_{S_\infty}$, i.e. if and only if $L' \subseteq L$). In general local class field theory lets you read off the ramification phenomena of a class field L/K from the corresponding class group in J_K, and you can define things like the "narrow class field" which is the same thing except it doesn't need to be unramified at the infinite places.

In any event, the global reciprocity law says that if L is the Hilbert class field for K, then

$$J_K/K^\times J_{S_\infty} \cong \mathrm{Gal}(L/K).$$

But the left hand side is isomorphic to the ideal class group of K (I proved this somewhere in here). In fact, the image of a fractional ideal of K under the reciprocity map is just its ideal class in $\mathrm{Cl}(K)$. So a prime in K splits completely in the Hilbert class field if and only if it is principal in K. By taking the Hilbert class field of the Hilbert class field, it's possible to get another interesting property:

Theorem 8.2 (Principal ideal theorem)**.** *Let $\mathfrak{p}$ be a prime in K, and let L be the Hilbert class field of K. Then $\mathfrak{p}\mathcal{O}_L$ is principal.*

Beginning of the proof. The full proof requires some group-theoretic input which I don't know how to do. I will explain the general idea of what needs to be done before that.

Let K' be the Hilbert class field of K, and K'' the Hilbert class field of K'. Whether $\mathfrak{p}$ becomes principal in K' is the same thing as whether it splits completely in K''. We know that K''/K is unramified (ramification is multiplicative in towers), but to apply the theory of the Artin symbol we need it to be Galois (it definitely won't be abelian because K' is the maximal abelian subextension of K''). This is actually true in general: let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Since K'/K is Galois, we know $\sigma K' = K'$. Therefore, since K''/K' is unramified and abelian, so is $\sigma K''/K'$, but since K''/K' is the maximal abelian unramified extension of K', this implies

$$\sigma K'' \subset K'',$$

and therefore $\sigma K'' = K''$ and K''/K is Galois.

Since K' is the maximal abelian subextension of K''/K, we have

$$\mathrm{Gal}(K'/K) = \mathrm{Gal}(K''/K)^{\mathrm{ab}}$$

and

$$\mathrm{Gal}(K''/K') = [\mathrm{Gal}(K''/K), \mathrm{Gal}(K''/K)].$$

Since K'/K is unramified, $\mathfrak{p}\mathcal{O}_L$ factors as a product of single powers of primes

$$\mathfrak{p}\mathcal{O}_L = \prod_i \mathfrak{q}_i$$

so that actually the element of $\mathrm{Gal}(K''/K)$ we need to show is trivial is

$$\left[\frac{K''/K}{\mathfrak{p}}\right] = \prod_i \left[\frac{K''/K'}{\mathfrak{q}_i}\right] = \prod_i \sigma_i \left[\frac{K''/K'}{\mathfrak{q}}\right] \sigma_i^{-1}$$

where $\mathfrak{q}$ is a fixed prime in K' lying over $\mathfrak{p}$ and the σ_i's are elements of $\mathrm{Gal}(K''/K)$ taking $\mathfrak{q}$ to $\mathfrak{q}_i$. So the principal ideal theorem amounts to showing that this product is trivial. □

Independently of the principal ideal theorem, if one can actually compute the Hilbert class field (which can be done by ad-hoc methods in small cases or by the theory of complex multiplication for imaginary quadratic fields), then just the simpler fact that splitting completely in the Hilbert class field is the same thing as being principal is very useful for proving more concrete facts, most notably regarding the primes of the form $x^2 + ny^2$ for $x, y \in \mathbf{Z}$ (though in general this definitely works for primes represented by arbitrary binary quadratic forms):

Lemma 8.3. *Let $n \in \mathbf{N}$ be squarefree and not 3 mod 4, $K = \mathbf{Q}(\sqrt{-n})$, and L the Hilbert class field of K. A positive rational prime p not dividing $2n$ is of the form $x^2 + ny^2$ if and only if p splits completely in L.*

Proof. p is of the form $x^2 + ny^2$ if and only if p splits in $\mathcal{O}_K = \mathbf{Z}[\sqrt{-n}]$ into two distinct principal primes[51]. This is equivalent to these two primes (or equivalently just one of them since they are conjugate) splitting completely in L, and therefore to p splitting completely in L. □

As a result, even if we can't compute the Hilbert class field of $\mathbf{Q}(\sqrt{-n})$, this gives an interesting density statement: p is of the form $x^2 + ny^2$ if and only if p splits in this field L, which has degree $|\mathrm{Cl}(\mathbf{Q}(\sqrt{-n}))|$ over $\mathbf{Q}(\sqrt{(\sqrt{-n})})$, and therefore degree $2|\mathrm{Cl}(\mathbf{Q}(\sqrt{-n}))|$ over $\mathbf{Q}$, which means that the set of primes of the form $x^2 + ny^2$ (still under the hypothesis[52] that $n \not\equiv 3 \mod 4$) has density $1/(2|\mathrm{Cl}(\mathbf{Q}(\sqrt{-n}))|)$ in the positive rational primes.

When the class group is small it's sometimes easy to tell what the Hilbert class field is.

Example 8.4. If $\mathbf{Q}(\sqrt{-n})$ has trivial class group, then it is equal to its own Hilbert class field, so p coprime to $2n$ is of the form $x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$.

Example 8.5. Let $n = 5$. Then (from the Minkowski bound) one can see that $|\mathrm{Cl}(\mathbf{Q}(\sqrt{-5}))| = 2$ and therefore the Hilbert class field of $\mathbf{Q}(\sqrt{-5})$ is equal to any unramified quadratic extension we can find. I claim that this extension is $\mathbf{Q}(\sqrt{-5}, \sqrt{-1})$. That is because $\mathbf{Q}(\sqrt{-5}, \sqrt{-1}) = \mathbf{Q}(\sqrt{5}, \sqrt{-1})$ so 2 and 5, which both ramify in $\mathbf{Q}(\sqrt{-5})$, both have ramification index 2 in $\mathbf{Q}(\sqrt{5}, \sqrt{-1})$, so $\mathbf{Q}(\sqrt{-5}, \sqrt{-1})/\mathbf{Q}(\sqrt{-5})$ is unramified as desired. This shows that a positive rational prime p not equal to 2 or 5 is of the form $x^2 + 5y^2$ if and only if $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) = 1$, which is equivalent to $p \equiv 1, 9 \mod 20$.

8.3. **Classical reciprocity laws.** Artin originally conjectured his reciprocity law as a correspondence between abelain Artin L-functions and Hecke L-functions (see section 3). Before he proved it, Artin also noticed that the classical reciprocity laws of Gauss, etc. could be derived from the reciprocity law. Recall the "standard" proof of quadratic reciprocity e.g. from the later chapters of Samuel [12], which uses the a priori knowledge that $\mathbf{Q}(\sqrt{\pm p}) \subseteq \mathbf{Q}(\zeta_p)$, and therefore the Artin symbol of q with respect to $\mathbf{Q}(\sqrt{\pm p})/\mathbf{Q}$ only depends on q mod p. Even though the characterization of the unique quadratic subfield of a cyclotomic extension of $\mathbf{Q}$ is elementary and can be done using Gauss sums or by looking at discriminants, it is easy to suspect that there should be a proof involving class field theory as well (since the computation of class fields over $\mathbf{Q}$ is really what lets you put the quadratic extension inside a cyclotomic one in the first place). In fact, independently of this metamathematical reason, the actual statement of the global reciprocity isomorphism

$$I(\mathfrak{f})/P_{\mathfrak{f}} \to \mathrm{Gal}(L/K)$$

tells you that the splitting type of a prime of K in L (as determined by its Artin symbol) depends only on a congruence condition modulo the conductor $\mathfrak{f}(L/K)$.

[51] If $p = x^2+ny^2$ then clearly p splits as the product of primes $(x-y\sqrt{-n})(x+y\sqrt{-n})$. Conversely, if $p\mathbf{Z}[\sqrt{-n}]$ factors as a product of distinct principal primes, which must be conjugates of each other, which just translates as $p\mathbf{Z}[\sqrt{-n}] = (x - y\sqrt{-n})(x + y\sqrt{-n})$, and thus $p = a(x^2 + ny^2)$ for some unit a in $\mathbf{Z}[\sqrt{-n}]$. But $a \in \mathbf{Q}$, so actually $a = \pm 1$ and if we assume $p > 0$ we get $p = x^2 + ny^2$.

[52] To deal with the case where $\mathcal{O}_K \neq \mathbf{Z}[\sqrt{-n}]$, we need to consider a certain order in the ring of integers. This is probably done somewhere in [3]

Taking $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{p})$, this basically (up to checking that this still works when $p \equiv 1 \mod 4$, which we had as an exercise in Math 123) says that whether p is a perfect square mod q (i.e. the splitting type of $X^2 - p$ mod q) depends only on a congruence condition on q mod $\mathfrak{f}(\mathbf{Q}(\sqrt{p})/\mathbf{Q})$, which depends only on q. So one way to prove quadratic reciprocity would be to actually compute the conductor $\mathfrak{f}(\mathbf{Q}(\sqrt{p})/\mathbf{Q})$. Suppose for simplicity that p is odd. The discriminant of this extension is $4p$ if $p \equiv 1 \mod 4$ and p otherwise. Since we have the best understanding of what the ray class groups of $\mathbf{Q}$ look like at moduli divisible by the infinite prime, we assume that $p < 0$, so that v_∞ is ramified in $\mathbf{Q}(\sqrt{p})$ and $v_\infty | \mathfrak{f}(\mathbf{Q}(\sqrt{p})/\mathbf{Q})$. For the finite places, the only ramified ones are p and possibly 2 if $p \equiv 3 \mod 4$. In the case $p \equiv 1 \mod 4$, we could just use the conductor-discriminant formula to show that the conductor divides the discriminant and is therefore equal to p (since it must be divisible by the ramified primes). Alternatively, we know $\mathbf{Q}_p(\sqrt{p})/\mathbf{Q}_p$ is quadratic (for example because p is ramified with index 2 in $\mathbf{Q}(\sqrt{p})$ so after taking completions the degree is still at least 2) and totally ramified of ramification index 2. Therefore it is tamely ramified (as $p \neq 2$), so its first ramification group is trivial. It follows that $\mathfrak{f}(\mathbf{Q}(\sqrt{p})/\mathbf{Q})$ is divisible by p exactly once (this works just as well when $p \equiv 1 \mod 4$). At the prime 2, when $p \equiv 3 \mod 4$ so that 2 is ramified at all, we see that the quadratic extension

$$\mathbf{Q}_2(\sqrt{p})/\mathbf{Q}_2$$

is not tamely ramified (2 divides the degree), so it has lower ramification groups $G_{-1} = G_0 = G_1 = \mathbf{Z}/2\mathbf{Z}$. So the valuation of the different is

$$v_{\mathfrak{q}|2}(\mathcal{D}(\mathbf{Q}_2(\sqrt{p})/\mathbf{Q}_2)) = \sum_{i \geq 0}(|G_i| - 1) \geq 2.$$

Since the norm of the different equals the absolute discriminant which we know is $4p$, and there is no inertia at 2, actually equality must hold, and the higher ramification groups are all trivial after G_1. As a result (after converting to the upper numbering which actually does nothing in this case), we have computed for odd primes p,

$$\mathfrak{f}(\mathbf{Q}(\sqrt{p})/\mathbf{Q}) = \begin{cases} 4pv_\infty, & \text{if } p \equiv 3 \mod 4 \\ pv_\infty, & \text{if } p \equiv 1 \mod 4 \end{cases}$$

which is just the discriminant plus the infinite prime. Remember that we assumed that $p < 0$ to force the infinite prime to show up. Now we can prove quadratic reciprocity just by looking at the two cases for p mod 4. If q is an odd rational prime, then the Legendre symbol

$$\left(\frac{p}{q}\right)$$

is the same as the image of q under the reciprocity map $I_{\mathbf{Q}} \to \mathbf{Z}/2\mathbf{Z} = \mathrm{Gal}(\mathbf{Q}(\sqrt{p})/\mathbf{Q})$ (the Artin symbol is trivial if and only if q splits completely, which is equivalent to $X^2 - p$ having a root mod q). Moreover, the reciprocity map at least restricts and descends to a surjective map

$$I_{\mathbf{Q}}(\mathfrak{f}(\mathbf{Q}(\sqrt{p})\mathbf{Q}))/P_{\mathbf{Q},\mathfrak{f}(\mathbf{Q}(\sqrt{p})\mathbf{Q})} \to \{\pm 1\}$$

whose kernel has index 2. If $p \equiv 1 \mod 4$, then the left hand side is just

$$I_{\mathbf{Q}}(pv_\infty)/P_{\mathbf{Q},pv_\infty} \cong (\mathbf{Z}/p\mathbf{Z})^\times$$

which has a unique subgroup of index 2, namely the squares (this is because it is cyclic), so a rational prime q coprime to p has $\left(\frac{p}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1$. On the other hand, when $p \equiv 1 \mod 4$, Artin reciprocity tells us that the reciprocity maps factors through $P_{\mathfrak{f}(\mathbf{Q}(\sqrt{p})/\mathbf{Q})}$ to get a well-defined map

$$(\mathbf{Z}/4\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$$

defined by

$$[q] \mapsto \left(\frac{p}{q}\right)$$

with kernel of index 2. Since $q \cdot \mathbf{Z} = (-q) \cdot \mathbf{Z}$ and this Legendre symbol is just the Artin symbol of the ideal $q \cdot \mathbf{Z}$, we can always multiply q by $(-1)^{(q-1)/2}$ to force it to be $1 \mod 4$. Let $q^* = (-1)^{\frac{q-1}{2}} q$. We know the map above is the same as the map

$$(\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$$

given by

$$q \mapsto q^* \mapsto \left(\frac{p}{q^*}\right)$$

the kernel of which is just the squares in $(\mathbf{Z}/p\mathbf{Z})^\times$, which proves that

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

when $p \equiv 3 \mod 4$, as desired.

In general, the situation we exploited here was that $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$ happens to be Galois, so the Legendre symbol could be directly studied using the Artin symbol. For the higher classical reciprocity laws, it's harder to do this because an extension like $\mathbf{Q}(p^{1/m})/\mathbf{Q}$ won't be Galois. So the standard thing to do is to pass to the obvious Kummer extension $\mathbf{Q}(p^{1/m})/\mathbf{Q}(\zeta_m)$. Taking $m = 3$ and directly computing the conductor of this extension as we did in the quadratic case, it's possible to prove cubic reciprocity. Even if we were to do it this way, we would need to first establish a connection between the Artin symbol of $\mathbf{Q}(p^{1/m})/\mathbf{Q}(\zeta_m)$ and whether primes are m-th powers mod other primes (when $m = 2$ this is easy because we know the ring of integers of $\mathbf{Q}(\sqrt{p})$ is monogenic and have a reasonable expression for its defining polynomial). To do this, we need to develop some small part of the theory of the *power residue residue symbol*, so I'll just follow that to its logical conclusion. What follows essentially consists of solutions to the first two sets of exercises in [1].

Let K be a number field containing ζ_m.

Definition 8.6. Let $a \in K$ and $\mathfrak{b}$ a fractional ideal of K coprime to m and a. Then the primes dividing $\mathfrak{b}$ are unramified in the Kummer extension $K(a^{1/m})/K$, so the Artin symbol $\left[\frac{K(a^{1/m})/K}{\mathfrak{b}}\right]$ is well-defined. It is determined by its action on $a^{1/m}$, so we define the *power residue symbol*

$$\left(\frac{a}{\mathfrak{b}}\right)_m \in \mu_m$$

to be the unique root of unity ζ_m^i such that

$$\left[\frac{K(a^{1/m})/K}{\mathfrak{b}}\right](a^{1/m}) = \zeta_m^i a^{1/m}.$$

Lemma 8.7. *The power residue symbol is independent of the choice of m-th root of a.*

Proof. Choose two distinct m-th roots of a, $a^{1/m}$ and $\zeta_m^j a^{1/m}$. The lemma is proved just by noticing that if

$$\left[\frac{K(a^{1/m})/K}{\mathfrak{b}}\right](a^{1/m}) = \zeta^i a^{1/m},$$

then

$$\left[\frac{K(a^{1/m})/K}{\mathfrak{b}}\right](\zeta_m^j a^{1/m}) = \zeta_m^{j+i} a^{1/m} = \zeta_m^i(\zeta_m^j a^{1/m})$$

(where the second line is because the Galois group acts trivially on the roots of unity, for example because they are in K). □

Lemma 8.8. *If $\mathfrak{b}$ is coprime to a and a' and m, then*

$$\left(\frac{aa'}{\mathfrak{b}}\right)_m = \left(\frac{a}{\mathfrak{b}}\right)_m \left(\frac{a'}{\mathfrak{b}}\right)_m .$$

Proof. Consider the extension $L = K(a^{1/m}, (a')^{1/m})$. The usual restriction property of the Artin symbol says that

$$\begin{aligned}\left[\frac{K(a^{1/m},(a')^{1/m})/K}{\mathfrak{b}}\right]((aa')^{1/m}) &= \left(\left[\frac{K((aa')^{1/m})/K}{\mathfrak{b}}\right](a^{1/m})\right)\left(\left[\frac{K((aa')^{1/m})/K}{\mathfrak{b}}\right]((a')^{1/m})\right)\\ &= \left(\left[\frac{K(a^{1/m})/K}{\mathfrak{b}}\right](a^{1/m})\right)\left(\left[\frac{K(a^{1/m})/K}{\mathfrak{b}}\right]((a')^{1/m})\right)\\ &= \left(\frac{a}{\mathfrak{b}}\right)_m \left(\frac{a'}{\mathfrak{b}}\right)_m\end{aligned}$$

as desired. □

Lemma 8.9. *If a fractional ideal $\mathfrak{b}$ of K is coprime to a and $a' \in K$, then*

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right)_m = \left(\frac{a}{\mathfrak{b}}\right)_m \left(\frac{a}{\mathfrak{b}'}\right)_m .$$

Proof. This follows from the definition of the Artin symbol (it is defined to be multiplicative in the ideal downstairs). □

Lemma 8.10. *Let $\mathfrak{p}$ be a prime in K coprime to $a \in K$ and m. Then $m|(\mathrm{N}\mathfrak{p} - 1)$ and*

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{N\mathfrak{p}-1}{m}} \mod \mathfrak{p}.$$

Proof. Since $\zeta_m \in K$ and $\mathfrak{p}$ is coprime to m, actually $\kappa\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ must contain a primitive m-th root of unity, since the polynomial $X^m - 1$ remains separable[53] over $\kappa(p)$. So $\mu_m \subseteq \kappa(\mathfrak{p})^\times$ is a multiplicative subgroup, so by Lagrange's theorem we have the desired

$$m||\kappa(\mathfrak{p})^\times| = \mathrm{N}\mathfrak{p} - 1.$$

[53] Let $f(X) = X^m - 1 \in K[X]$. By Hensel's lemma, any root of f in $\kappa(\mathfrak{p})$ can be lifted to a root of f in $K_\mathfrak{p}$, which must actually be a power of $\zeta_m \in K$ since there are already m of them, so all the roots are of the form $\zeta_m^i \mod \mathfrak{p}$. But (using the fact that m and $\mathfrak{p}$ are coprime for the second time) $v_\mathfrak{p}(f'(\zeta_m)) = 0$ so f remains separable in $\kappa(\mathfrak{p})[X]$, and hence $\kappa(\mathfrak{p})$ contains m distinct m-th roots of unity.

The definition of the Artin symbol also mandates that

$$\left(\frac{a}{\mathfrak{p}}\right) a^{1/m} \equiv (a^{1/m})^{\mathrm{N}\mathfrak{p}} \mod \mathfrak{P},$$

for some $\mathfrak{P}|\mathfrak{p}$, so after rearranging we see that

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{\mathrm{N}\mathfrak{p}-1}{m}} \mod \mathfrak{P}.$$

Since both sides are actually in K, this congruence is true mod $\mathfrak{p}$ as well, which is the desired statement. □

Lemma 8.11. *For $\mathfrak{p}$ in K coprime to a and m, the following are equivalent:*

(i) $\left(\frac{a}{\mathfrak{p}}\right) = 1$.

(ii) There exists an $x \in \mathcal{O}_K$ such that $x^m \equiv a \mod \mathfrak{p}$.

(iii) There exists an $x \in K_{\mathfrak{p}}$ such that $x^m = a$.

Proof. Assume (ii). Then we know from the previous lemma that

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv x^{\mathrm{N}\mathfrak{p}-1} \mod \mathfrak{p}.$$

Since $\mathrm{N}\mathfrak{p} - 1 = |\kappa(\mathfrak{p})^\times|$, this is $1 \mod \mathfrak{p}$. Since the norm residue symbol is an m-th root of unity, which we saw earlier remain distinct mod $\mathfrak{p}$, this proves (i).

Conversely, assume (i). Using the previous lemma, (i) implies that

$$a^{\frac{\mathrm{N}\mathfrak{p}-1}{m}} \equiv 1 \mod \mathfrak{p}.$$

The reduction of a mod $\mathfrak{p}$ is therefore an m-th power, since this shows it has order dividing m and $\kappa(\mathfrak{p})$ is cyclic. It remains to show that (i) and (ii) are equivalent to (iii).

The fact that (iii) implies (ii) is obvious just by taking projecting onto the residue field.

The fact that (ii) implies (iii) is a consequence of the trivial case of Hensel's lemma: If $f(X) = X^m - a$ has a root x in $\kappa(\mathfrak{p})$, then this root is not zero $\mod \mathfrak{p}$ (since $a \not\equiv 0$), so $f'(x) = mx^{m-1} \not\equiv 0 \mod \mathfrak{p}$ and so x lifts to a root in $K_{\mathfrak{p}}$. □

Lemma 8.12. *If $\mathfrak{p}$ is an integral ideal coprime to m, then (N.B. ζ_m is coprime to $\mathfrak{p}$ since it is a unit)*

$$\left(\frac{\zeta_m}{\mathfrak{p}}\right)_m = \zeta_m^{\frac{\mathrm{N}\mathfrak{p}-1}{m}}.$$

Proof. If $\mathfrak{b}$ is prime, this is obvious because then

$$\left(\frac{\zeta_m}{\mathfrak{b}}\right)_m \equiv \zeta_m^{\frac{\mathrm{N}\mathfrak{b}-1}{m}} \mod \mathfrak{p}$$

and the m-th roots of unity are all distinct mod $\mathfrak{p}$, so this must be an equality in K. Now suppose $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$. We know that $\mathrm{N}\mathfrak{p} \equiv 1 \mod m$, so we can write

$$\mathrm{N}\mathfrak{p} = 1 + mr_{\mathfrak{p}}$$

for some choice of integers $r_{\mathfrak{p}} \in \mathbf{N}$, and thus

$$\mathrm{N}\mathfrak{b} = \prod_{\mathfrak{p}} (1 + mr_{\mathfrak{p}})^{n_{\mathfrak{p}}} \equiv 1 + m \sum_{\mathfrak{p}} n_{\mathfrak{p}} r_{\mathfrak{p}} \mod m^2,$$

which means

$$\begin{aligned}\left(\frac{\zeta_m}{\mathfrak{b}}\right) &= \prod_{\mathfrak{p}} \left(\frac{\zeta_m}{\mathfrak{p}}\right)^{n_\mathfrak{p}} \\ &= \prod_{\mathfrak{p}} \left(\zeta_m^{\frac{\mathrm{N}\mathfrak{p}-1}{m}}\right)^{n_\mathfrak{p}} \\ &= \zeta_m^{\sum_\mathfrak{p} r_\mathfrak{p} n_\mathfrak{p}} \\ &= \zeta_m^{\frac{\mathrm{N}\mathfrak{b}-1}{m}}\end{aligned}$$

as desired. □

Lemma 8.13. *If $a, a' \in K$ are nonzero, and $\mathfrak{b}$ is an integral ideal of K coprime to a, a' and m such that $a \equiv a' \mod \mathfrak{b}$, then*

$$\left(\frac{a}{\mathfrak{b}}\right)_m = \left(\frac{a'}{\mathfrak{b}}\right)_m.$$

Proof. The condition $a \equiv a' \mod \mathfrak{b}$ means that

$$a - a' \in \mathfrak{b} \subseteq \mathfrak{p}$$

for all $\mathfrak{p}|\mathfrak{b}$ (this is where we use the fact that $\mathfrak{b}$ is integral). The point is that this implies $a \equiv a' \mod \mathfrak{p}$ for all $\mathfrak{p}|\mathfrak{b}$, and thus

$$\left(\frac{a}{\mathfrak{p}}\right) = \left(\frac{a'}{\mathfrak{p}}\right)$$

since by a previous lemma $\left(\frac{a}{\mathfrak{p}}\right)$ depends only on $a \mod \mathfrak{p}$. Multiplying this over all the powers of primes dividing $\mathfrak{b}$, we recover the desired equality. □

Rephrased in the language of the power residue symbol, a crude estimation of the conductor of this Kummer extension also results in quadratic reciprocity without needing to justify the exact value of the conductor.

Proposition 8.14. *Let $a \in K^\times$, and $\mathfrak{b}$ and $\mathfrak{b}'$ be fractional ideals of K coprime to a. If $\mathfrak{b}(\mathfrak{b}')^{-1}$ is principally generated by $c \in K^\times$ which is an m-th power in $K_\mathfrak{p}^\times$ for all $\mathfrak{p}$ dividing m or a, then*

$$\left(\frac{a}{\mathfrak{b}}\right)_m = \left(\frac{a}{\mathfrak{b}'}\right)_m.$$

Proof. By one of the previous lemmas,

$$\left(\frac{a}{\mathfrak{b}}\right)_m \left(\frac{a}{\mathfrak{b}'}\right)_m^{-1} = \left(\frac{a}{c \cdot \mathcal{O}_K}\right)_m.$$

We know that $[K_\mathfrak{p}(a^{1/m}) : K_\mathfrak{p}]|m$, so

$$N_{K_\mathfrak{p}(a^{1/m})/K_\mathfrak{p}}(K_\mathfrak{p}(a^{1/m})^\times) \supseteq (K_\mathfrak{p}^\times)^{[K_\mathfrak{p}(a^{1/m}):K_\mathfrak{p}]} \supseteq (K_\mathfrak{p}^\times)^m$$

which means c is a local norm at all $\mathfrak{p}$ which ramify in $K(a^{1/m})$. Local class field theory implies that the local Artin symbol of c is trivial at all these ramified primes. On the other hand, c is not divisible by the ramified primes because of how it was defined, so its local Artin symbol at those primes is also trivial. As a result, the global Artin symbol is trivial, as desired. □

This turns out to be good enough to deduce quadratic reciprocity.

Lemma 8.15. *Let $a \in \mathbf{N}$, and let a_0 be an (odd) integer such that $a = 2^{v_2(a)}a_0$. Also let P be a positive odd integer coprime to a. Then*

$$\left(\frac{a}{(P)}\right)_2 = \left(\frac{a}{(Q)}\right)_2$$

if $P \equiv Q \mod 8a_0$.

Proof. Most of this is just specializing the previous lemma. If $P \equiv Q \mod 8a_0$, then since P and Q are odd and coprime to a, we actually know

$$(P)(Q)^{-1} \equiv 1 \mod 8a_0.$$

Since the squares in $\mathbf{Q}_2^\times$ contain the elements congruent to 1 mod 8, and the squares in $\mathbf{Q}_p^\times$ when p is odd contain $U_p^{(1)}$ (both of these are easy consequences of Hensel's lemma), the hypotheses of the previous lemma show the conclusion of this one. □

Theorem 8.16 (Quadratic Reciprocity)**.** *If P and Q are odd distinct rational primes, then*

$$\left(\frac{-1}{(P)}\right)_2 = (-1)^{\frac{P-1}{2}}, \qquad \left(\frac{2}{(P)}\right)_2 = (-1)^{\frac{P^2-1}{8}}, \qquad \left(\frac{Q}{(P)}\right)_2\left(\frac{P}{(Q)}\right)_2 = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

Proof. The first part is a direct consequence of Euler's criterion (lemma 8.12), since $\zeta_2 = -1$. For the second one, just use the previous lemma with $a = 2$. This implies that $\left(\frac{2}{(P)}\right)$ depends only on P mod 8. So we can just check one odd rational prime in each odd congruence class mod 8: 2 is a perfect square mod 17 since $6^2 \equiv 2$ mod 17, and 2 is a perfect square mod 7, but not mod 3 or mod 5.

The last one requires more work before it can be reduced to a finite computation, but luckily I am armed with the hint in Cassels–Frohlich. Let

$$\langle P, Q\rangle = \left(\frac{P}{(Q)}\right)_2\left(\frac{Q}{(P)}\right)_2,$$

which we know only depends on P mod $8Q$ and Q mod $8P$.

Suppose $P \equiv Q \mod 8$, so that $Q \equiv 8a \mod (P)$ and $8a \equiv -P \mod (Q)$ for some integer a, and therefore by three previous lemmas and the fact that $P \equiv Q$ mod 8 and $P \equiv Q \mod a$,

$$\left(\frac{Q}{(P)}\right)_2 = \left(\frac{8a}{(P)}\right)_2 = \left(\frac{8a}{(Q)}\right)_2 = \left(\frac{-P}{(Q)}\right)_2 = (-1)^{\frac{Q-1}{2}}\left(\frac{P}{(Q)}\right)_2$$

as desired. One convenient way to rephrase this is that

$$\langle P, Q\rangle = \left(\frac{-1}{(Q)}\right)_2.$$

For arbitrary P, Q, take $R \equiv 1 \mod Q$ to be an odd integer such that

$$RP \equiv Q \mod 8,$$

which implies

$$\langle P, Q\rangle\langle R, Q\rangle = \langle PR, Q\rangle = \left(\frac{-1}{(Q)}\right)_2.$$

This means that if you fix R and Q and vary P while keeping $(P, Q) = 1$ and $RP \equiv Q \mod 8$, it follows that $\langle R, Q\rangle$ never changes, and neither does the right hand side, so $\langle P, Q\rangle$ never changes. But doing this is the same thing as changing P to anything congruent to it mod 8 and coprime to Q, so this shows that $\langle P, Q\rangle$

depends only on $P \mod 8$. By symmetry this also only depends on Q mod 8, so after checking a finite number of cases we can verify the last part of the reciprocity law. □

8.4. **Local-global principles.** For now I'll just write about a local-global principle for norms in cyclic extensions. Maybe later I'll add in Grunwald-Wang or something about the Brauer–Manin obstruction. Actually this has been made trivial by the theory we already developed for the purposes of doing global class field theory. If L/K is a finite cyclic extension of number fields, then the short exact sequence of multiplicative $\mathrm{Gal}(L/K)$-modules

$$1 \to L^\times \to J_L \to C_L \to 1$$

induces a long exact sequence on cohomology, a part of which is

$$H^1(\mathrm{Gal}(L/K), C_L) \to H^2(\mathrm{Gal}(L/K), L^\times) \to H^2(\mathrm{Gal}(L/K), J_L).$$

Since $\mathrm{Gal}(L/K)$ is cyclic, the long exact sequence on Tate cohomology is periodic, and we know that this is the same as the exact sequence

$$H^1(\mathrm{Gal}(L/K), C_L) \to \hat{H}^0(\mathrm{Gal}(L/K), L^\times) \to \hat{H}^0(\mathrm{Gal}(L/K), J_L).$$

We proved earlier in the course of proving one of the fundamental inequalities that

$$Q(\mathrm{Gal}(L/K), C_L) = [L : K],$$

but also $|\hat{H}^0(\mathrm{Gal}(L/K), C_L)| = [C_K : N_{L/K}C_L] = [L : K]$ (by the class field theory isomorphism), so actually $H^1(\mathrm{Gal}(L/K), C_L)$ is trivial, and we are left with an injective group homomorphism

$$K^\times/N_{L/K}L^\times \to J_K/N_{L/K}J_L$$

which we know is really induced by the inclusion of $K^\times \to J_K$. The local-global principle for norms follows:

Theorem 8.17. *Let L/K be a cyclic extension of number fields. An element $\alpha \in K^\times$ is a norm from $L_w^\times$ in $K_v^\times$ for all $v \in M_K$ if and only if α is a norm from $L^\times$.*

Specializing to the case where L is a quadratic extension, we can recover the Hasse–Minkowski theorem in the special case of binary quadratic forms.

9. Explicit Class Field Theory

9.1. **Lubin-Tate Theory.**

9.2. **Complex Multiplication.**

References

[1] J.W.S. Cassels and A. Frölich. *Algebraic number theory: proceedings of an instructional conference*. Academic Pr, 1967.

[2] Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

[3] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[4] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, pages 143–316. Springer, 1973.

[5] N.D. Elkies. Math 229: Introduction to analytic number theory. URL: http://www.math.harvard.edu/~elkies/M229.18/index.html.

[6] M.D. Fried and M. Jarden. *Field arithmetic*, volume 11. Springer Science & Business Media, 2006.

[7] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. Princeton University Press, 1985.

[8] E. Landau. Neuer beweis des primzahlsatzes und beweis des primidealsatzes. *Mathematische Annalen*, 56(4):645–670, 1903.

[9] S. Lang. *Algebraic number theory*, volume 110. Springer Science & Business Media, 2013.

[10] Daniel Marcus. *Number Fields*. Springer, 1977.

[11] J. Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[12] Pierre Samuel. *Théorie Algébrique des Nombres*. Hermann, 1967.

[13] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[14] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 2013.

[15] T. Takagi, K. Iwasawa, S. Iyanaga, and K. Kodaira. *Teiji Takagi Collected Papers*. Springer, 1990.

[16] R. Vakil. The rising sea: Foundations of algebraic geometry. *preprint*, 2017.