Class Field Theory

Abstract

These notes are based on a course in class field theory given by Freydoon Shahidi at Purdue University in the fall of 2014. The notes were typed by graduate students Daniel Shankman and Dongming She. The approach to class field theory in this course is very global: one first defines the ideles and adeles, then uses L-functions and cohomology, respectively, to prove the first and second norm index inequalities. One can then prove the main theorem of global class field theory, which is essentially the existence of a well defined idelic Artin map. Local class field theory and the lower reciprocity laws are proved as corollaries of this.

The logical progression is in many ways similar to Lang's *Algebraic Number Theory*. For example, the section on cohomology is nearly identical. However, we make use of more powerful machinery to prove the first inequality (the theory of locally compact groups, the Haar measure, some harmonic analysis). Also, Lang's notes are more balanced in describing things in terms of ideals or ideles, while these notes favor the ideles. Finally, the last section on lower reciprocity laws was neither in Lang's book nor the course; we added the section later with the intention of describing how Artin reciprocity is related to the 19th century results.

Contents

Preliminary Material

In order to acquaint the reader with our (more or less standard) notation and vocabulary, we will give a brief review of algebraic number theory.

0.1 Places, primes, and valuations

Let K be a number field, $A = \mathcal{O}_K$, and $\mathfrak{p}$ a prime ideal of K. The localization $A_\mathfrak{p}$ is a discrete valuation ring whose normalized valuation we denote by $\mathrm{ord}_\mathfrak{p}$ or $\nu_\mathfrak{p}$. To describe this valuation more explicitly, let π be a generator of the unique maximal ideal of $A_\mathfrak{p}$. Then every $x \in K^*$ can be uniquely written as $u\pi^n$, where u is a unit in $A_\mathfrak{p}$ and n is an integer. We then define $\mathrm{ord}_\mathfrak{p}(x) = n$ (and set $\mathrm{ord}_\mathfrak{p}(0) = \infty$). This valuation extends uniquely to K^*, and it induces a nonarchimedean absolute value $|\cdot|$ on K by setting $|x| = \rho^{-\mathrm{ord}_\mathfrak{p}(x)}$, where ρ is a fixed real number in $(1, \infty)$. As far as topology is concerned, the choice of ρ does not matter, for if $|\cdot|_1, |\cdot|_2$ are absolute values, then they induce the same topology if and only if there is a $c > 0$ for which $|\cdot|_1 = |\cdot|_2^c$. The completion of K with respect to this absolute value is a nonarchimedean local field, whose ring of integers is the completion of $A_\mathfrak{p}$. In this way the absolute value $|\cdot|$, and the valuation $\mathrm{ord}_\mathfrak{p}$, extend uniquely to this completion.

By a **place** of K we mean an equivalence class of absolute values on K, two absolute values being equivalent if they induce the same topology. The **finite places** are those which are induced by the prime ideals in the ring of integers of K. There is one for each prime. Thus if v is a finite place, we denote the corresponding prime by $\mathfrak{p}_v$. The **infinite places** are those which are induced by embeddings of K into the complex numbers. There is one for each embedding into $\mathbb{R}$, and one for each pair of conjugate complex embeddings (embeddings of K into $\mathbb{C}$ which are not contained in $\mathbb{R}$ come in pairs). To describe these places explicitly, consider an embedding $\sigma : K \to \mathbb{C}$. Such an embedding gives an absolute value $|\cdot|_1$ on K by setting $|x|_1 = |\sigma(x)|$, where $|\cdot|$ denotes the usual absolute value on $\mathbb{C}$. These are all the places of K. Some authors treat infinite places as coming from "infinite primes," and moreover distinguish between ramified and unramified infinite primes, but we will always use the word "prime" to refer to an honest prime ideal.

For a given place w of K, there are two absolute values corresponding to w, denoted $|\cdot|_w$ and $||\cdot||_w$, which will be of use. First, let v be the place of $\mathbb{Q}$ over which w lies (that is, pick any absolute value corresponding to w, and let v be the place corresponding to the absolute value induced by restriction to $\mathbb{Q}$). If v is finite (say v corresponds to the prime number p), then we have the canonical absolute value $|\cdot|_p$ on $\mathbb{Q}$ given by $|x|_p = p^{-\mathrm{ord}_p(x)}$. Otherwise v corresponds to the canonical archimedean absolute value on $\mathbb{Q}$. Either way, let $|\cdot|_v$ denote the canonical absolute value

on $\mathbb{Q}$. It is then trivial to verify that the *product formula*

$$\prod_v |x|_v = 1$$

holds for any $x \in \mathbb{Q}^*$ (v running through all the *rational places*, i.e. the places of $\mathbb{Q}$). Note that this is a finite product. For the completions $\mathbb{Q}_v \subseteq K_w$, the absolute value $|\cdot|_v$ on $\mathbb{Q}_v$ will extend uniquely to an absolute value $|\cdot|_w$ on K_w by the formula

$$|x|_w = |N_{w/v}(x)|_v^{\frac{1}{[K_w:\mathbb{Q}_v]}}$$

where we write $N_{w/v}$ to denote the local norm $N_{K_w/\mathbb{Q}_v}$. Restricting $|\cdot|_w$ to K gives us an absolute value on K corresponding to the place w. But of course this is seldom the only absolute value on K which extends $|\cdot|_v$.

On the other hand, we can scale $|\cdot|_w$ to obtain an absolute value $||\cdot||_w$ for which the product formula holds for K. We do this by setting $||x||_w = |x|_w^{[K_w:\mathbb{Q}_v]}$, where v is the rational place over which w lies. We know that for a given rational place v, the norm $N_{K/\mathbb{Q}}$ is the product of the local norms $N_{w/v}$. Thus as w runs through all the places of K, v runs through all the rational places, we have

$$\prod_w ||x||_w = \prod_v \prod_{w|v} ||x||_w = \prod_v \prod_{w|v} |x|_w^{[K_w:\mathbb{Q}_v]}$$

$$= \prod_v \prod_{w|v} |N_{w/v}(x)|_v = \prod_v |N_{K/\mathbb{Q}}(x)|_v = 1$$

In general, we will interchange valuations, places, and primes when the context is clear, for example writing ord_w instead of $\mathrm{ord}_\mathfrak{p}$ when $\mathfrak{p}$ is the place corresponding to w, or writing $||\cdot||_\mathfrak{p}$ instead of $||\cdot||_w$.

0.2 Nonarchimedean local fields

Let K be a field of characteristic zero. We say K is a *local field* if it is a topological field whose topology is locally compact and not discrete. Necessarily then K will be isomorphic (as a topological field) to $\mathbb{R}, \mathbb{C}$, or a finite extension of $\mathbb{Q}_p$ for some prime number p. If $K \cong \mathbb{R}$ or $\mathbb{C}$, then K is called *archimedean*, otherwise *nonarchimedean*.

Let E be a number field, and K a finite extension of $\mathbb{Q}_p$. We can imagine all the number fields to be contained in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and also imagine all p-adic fields to be contained in a fixed algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. We can also fix a canonical isometric embedding $\mathbb{Q} \to \mathbb{Q}_p$.

Proposition. *Every finite extension K of $\mathbb{Q}_p$ is the completion of a number field E, and furthermore E can be chosen so that $[E:\mathbb{Q}] = [K:\mathbb{Q}_p]$.*

Proof. (Sketch) Let $K = \mathbb{Q}_p(\alpha)$, with f the minimal polynomial of α over $\mathbb{Q}_p$. Approximate the coefficients of f closely enough (p-adically speaking) by a polynomial $g \in \mathbb{Q}[X]$, and it will follow that there exists a root $\beta \in \mathbb{C}_p$ of g such that $K = \mathbb{Q}_p(\beta)$ (Krasner's lemma). Since $[K : \mathbb{Q}_p] = deg(f) = deg(g)$, it follows that g is irreducible over $\mathbb{Q}_p$, hence over $\mathbb{Q}$.

Since g is irreducible over $\mathbb{Q}_p$, this tells us that if $b \in \overline{\mathbb{Q}}$ is any root of g, then p has only one prime ideal $\mathfrak{p}$ lying over it in $E := \mathbb{Q}(b)$ (see the appendix on topological tensor products). Thus the p-adic absolute value on $\mathbb{Q}$ extends uniquely to a $\mathfrak{p}$-adic absolute value on E. Now the map $b \mapsto \beta$ gives an isometric $\mathbb{Q}$-embedding of E into $\mathbb{C}_p$, and the completion of this field with respect to the p-adic absolute value is exactly $\mathbb{Q}_p(\beta) = K$. □

Note that different embeddings of different number fields into $\mathbb{C}_p$ are in general not compatible with each other (except for a given number field and the canonical embedding $\mathbb{Q} \to \mathbb{Q}_p$), and the specific embedding is rather arbitrary. In this case, for example, there could be several roots β, b to choose from. Also a given p-adic field could be the completion of infinitely many distinct number fields in the sense above, and an arbitrary number field admits several different topologies coming from the p-adic absolute value, one for each prime lying over p.

However, for every finite extension of local fields K'/K, one can argue as above that there exists an extension of number fields E'/E, as well as an extension of places w/v, such that (in the sense of the proposition) K' is the completion of E' with respect to w, K is the completion of E_v with respect to v , and the diagram

$$\begin{array}{ccc} E' & \to & K' \\ \cup & & \cup \\ E & \to & K \\ \cup & & \cup \\ \mathbb{Q} & \to & \mathbb{Q}_p \end{array}$$

commutes. So the point of the above proposition is *not* to view local fields as being canonically induced by global fields; rather, it is to permit the use of global machinery in the investigation of local phenomena.

Let $\mathcal{O}$ be K's ring of integers, with unique maximal ideal $\mathfrak{p}$, and let π be a uniformizer for K ($\mathfrak{p} = \pi\mathcal{O}$). Let $|\cdot| = |\cdot|_p$ denote the p-adic absolute value, uniquely extended to K.

We state the following facts. Proofs can be found in any good book on algebraic or p-adic number theory.

- Two open balls in K are either disjoint, or one contains the other.
- Given $x \in K, r > 0$, if $|y - x| < r$, then the ball with center x and radius r is the same thing as the ball with center y and radius r.
- Every open set in K is a disjoint union of open balls.

- Open balls are also closed, and moreover compact. Hence K is locally compact.
- $\mathcal{O}$ is the unique maximal compact subgroup of K with respect to addition. $\mathcal{O}^*$ is the unique maximal compact subgroup of K^* with respect to multiplication.
- $\mathfrak{p}^i$, that is the ball of center 0 and radius $|\pi^i|_p$, is a compact open subgroup with respect to addition, and these subgroups form a fundamental system of neighborhoods of 0 (any given neighborhood of 0 will contain $\mathfrak{p}^i$ for sufficiently large i)
- $1+\mathfrak{p}^i$, that is the ball of center 1 and radius $|\pi^i|_p$, is a compact open subgroup with respect to multiplication, and these subgroups form a fundamental system of neighborhoods of 1.

Most of the above properties are straightforward to prove. For example, the topological properties of $1+\mathfrak{p}^i$ follow from those of $\mathfrak{p}^i$, since the map $x \mapsto 1+x$ is a homeomorphism of these subspaces. To show that $1+\mathfrak{p}^i$ is closed under inverses, one need only observe that if $1+x\pi^i$ is a member of this set, then its inverse is the infinite sum $1 - x\pi^i + x^2\pi^{2i} - \cdots$, with $-x\pi^i + x^2\pi^{2i} - \cdots \in \mathfrak{p}^i$. This series converges because $|x\pi^i|_p$ goes to 0.

We also state, but do not prove, a general version of Hensel's lemma (again, see any good number theory textbook).

Hensel's lemma. *Let K be a p-adic field with absolute value $|\cdot|$. Suppose $f \in \mathcal{O}[X], a_0 \in \mathcal{O}$, and $|f(a_0)| < |f'(a_0)|^2$. Then there is a unique root $a \in \mathcal{O}$ of f such that*

$$|a - a_0| < \left|\frac{f(a_0)}{f'(a_0)^2}\right| < 1$$

Corollary. *Let $m \in \mathbb{N}$. There exists a $\delta > 0$ such that for any $u \in \mathcal{O}^*$ satisfying $|u-1| < \delta$, u has an mth root in $\mathcal{O}^*$.*

Proof. Apply Hensel's lemma with $f(X) = X^m - u$ and $a_0 = 1$. □

Let K'/K be an extension of p-adic fields with primes $\mathfrak{p}', \mathfrak{p}$. We regard the residue field $\mathcal{O}_K/\mathfrak{p}$ as a subfield of $\mathcal{O}_{K'}/\mathfrak{p}'$, and denote the index by $f = f(\mathfrak{p}'/\mathfrak{p})$. Usually, $\mathfrak{p}$ will not remain prime in $\mathcal{O}_{K'}$, but will be a prime power. Let $e = e(\mathfrak{p}'/\mathfrak{p}) \geq 1$ be the number for which $\mathfrak{p}\mathcal{O}_{K'} = \mathfrak{p}'^e$. We call e and f the **ramification index** and **inertial degree**. We always have

$$ef = [K' : K]$$

For a tower of fields, both ramification and inertia are multiplicative. We call K'/K **unramified** if $e = 1$. Let b run through all the elements of $\mathcal{O}_{K'}$ such that $K' = K(b)$, and let $g_b \in \mathcal{O}_K[X]$ be

the minimal polynomial of b over K. The **different** is the ideal

$$\mathscr{D}(K'/K) = \sum_b g_b'(b)\mathcal{O}_K$$

of $\mathcal{O}_{K'}$. Actually, there always exists a b_0 among the b such that $\mathcal{O}_{K'} = \mathcal{O}_K[b]$, so $\mathscr{D}(K'/K) = g_{b_0}'(b_0)\mathcal{O}_K$. The different is all of $\mathcal{O}_{K'}$ if and only if K'/K is unramified.

Let us briefly describe unramified extensions. There is a unique unramified extension of K of each degree, and these extensions are in bijection with the extensions of the residue field $\mathcal{O}_K/\mathfrak{p}$. If K'/K is unramified, then it is Galois, and the Galois group is isomorphic to the Galois group of the extension of residue fields. In particular this group is cyclic. If E/K is finite, then EK'/E is unramified. Hence a compositum of unramified extensions is unramified.

0.3 Number Fields

Let L/K be a finite extension of number fields. If $\mathfrak{p}$ is a prime of K, then the ideal in $\mathcal{O}_L$ generated by $\mathfrak{p}$ will be a product of primes

$$\mathfrak{p}\mathcal{O}_L = \mathscr{P}_1^{e_1} \cdots \mathscr{P}_g^{e_g}, e_i \geq 1$$

where $\mathscr{P}_1, ..., \mathscr{P}_g$ are all the primes lying over $\mathfrak{p}$. If v is the place of K corresponding to $\mathfrak{p}$, and w_i is the place of L corresponding to $\mathscr{P}$, then $w_1, ..., w_g$ are all the extensions of v to L. The number $e(\mathscr{P}_i/\mathfrak{p}) := e_i$ is called the ramification index of $\mathscr{P}_i$ over $\mathfrak{p}$, and $f(\mathscr{P}_i/\mathfrak{p}) = f_i := [\mathcal{O}_L/\mathscr{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is called the inertial degree of $\mathscr{P}_i$ over $\mathfrak{p}$. We always have

$$[L : K] = e_1 f_1 + \cdots + e_g f_g$$

We call a prime $\mathscr{P}_i$ **ramified** over K if $e(\mathscr{P}_i/\mathfrak{p}) > 1$, otherwise we say it is unramified. We call $\mathfrak{p}$ ramified if some prime lying over it is ramified. If L/K is Galois, then $e_i = e_j$ and $f_i = f_j$ for all i, j, so we just write the above formula as $[L : K] = efg$.

Let $\mathscr{P} \mid \mathfrak{p}$ be an extenion of primes, corresponding to an extension of places $w \mid v$. If $\mathcal{O}_w, \mathcal{O}_v, \mathscr{P}_w, \mathfrak{p}_v$ are the completions of $\mathcal{O}_L, \mathcal{O}_K, \mathscr{P}, \mathfrak{p}$ with respect to w and v, then ramification and inertia are unchanged after completion. We have

$$e(L_w/K_v) = e(\mathscr{P}_w/\mathfrak{p}_v) = e(\mathscr{P}/\mathfrak{p})$$

and the residue field extensions $\mathcal{O}_w/\mathscr{P}_w$ over $\mathcal{O}_v/\mathfrak{p}_v$; $(\mathcal{O}_L)_{\mathscr{P}}/\mathscr{P}(\mathcal{O}_L)_{\mathscr{P}}$ over $(\mathcal{O}_K)_{\mathfrak{p}}/\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$; and $\mathcal{O}_L/\mathscr{P}$ over $\mathcal{O}_K/\mathfrak{p}$ are all isomorphic to each other. Thus

$$f(L_w/K_v) = f(\mathscr{P}_w/\mathfrak{p}_v) = f(\mathscr{P}/\mathfrak{p})$$

The **different** ideal $\mathscr{D}(L/K)$ of L/K can be defined in exactly the same way as in the local case. One can show that global different is in a sense the product of the local differents:

$$\mathscr{D}(L/K)_{\mathfrak{p}} = \prod_{w|v} \mathscr{P}_w^{\mathrm{ord}_w \mathscr{D}(L_w/K_v)}$$

Thus a prime of L divides the different if and only if it is ramified over K. The **discriminant** of L/K is the (ideal) norm of the different $N_{L/K}(\mathscr{D}(L/K))$. A prime of K is ramified in L if and only if it divides the discriminant.

Now assume L/K is Galois. The Galois group of L/K acts transitively on the places (or the primes in the finite case) lying over any place of K (or prime of K). If $\mathfrak{p}$ is a prime of K, and $\mathscr{P}$ is a prime of L lying over $\mathfrak{p}$, the **decomposition group** $\mathrm{Gal}(L/K)_{\mathscr{P}}$ of $\mathscr{P}$ is the set of $\sigma \in \mathrm{Gal}(L/K)$ for which $\sigma\mathscr{P} = \mathscr{P}$.

Assume L/K is abelian (that is, $\mathrm{Gal}(L/K)$ is abelian). The abelian case is what class field theory is all about. Then the decomposition groups $\mathrm{Gal}(L/K)_{\mathscr{P}} : \mathscr{P} \mid \mathfrak{p}$ are all the same, so we just refer to all of them as $\mathrm{Gal}(L/K)_{\mathfrak{p}}$, *the decompositon group of* $\mathfrak{p}$.

We have a homomorphism

$$\mathrm{Gal}(L/K)_{\mathfrak{p}} \to \mathrm{Gal}((\mathcal{O}_L/\mathscr{P})/(\mathcal{O}_K/\mathfrak{p}))$$

(the choice of $\mathscr{P} \mid p$ doesn't matter; the residue fields are all isomorphic) given by $\sigma \mapsto \overline{\sigma}$, where $\overline{\sigma}(x + \mathscr{P}) = \sigma(x) + \mathscr{P}$. This is well defined. The kernel of this homomorphism is called the **inertia group**. Let Z, T be the fixed fields under L of the decomposition and inertia groups, respectively. We call Z, T the **decomposition** and **inertia fields**, respectively. Since $\mathrm{Gal}(L/T) \subseteq \mathrm{Gal}(L/Z) = \mathrm{Gal}(L/K)_{\mathfrak{p}}$, we have $Z \subseteq T$. When we factor $\mathfrak{p}\mathcal{O}_L$ as a product of prime ideals:

$$\mathfrak{p}\mathcal{O}_L = \mathscr{P}_1^e \cdots \mathscr{P}_g^e$$

there are three things happening which we seek to understand: the ramification e, the inertia f, and the number of primes g lying over $\mathfrak{p}$. They are related and balanced by the formula $[L : K] = efg$. The decomposition and inertia fields allow us to isolate each of these constants.

Proposition. *(i) The index of the decomposition group* $\mathrm{Gal}(L/K)_{\mathfrak{p}}$ *in* $\mathrm{Gal}(L/K)$ *is the number of primes lying over* $\mathfrak{p}$*. The index of the inertia group in* $\mathrm{Gal}(L/K)_{\mathfrak{p}}$ *is the ramification index of* p*.*

(ii) The decomposition group, Z*, is the unique maximal subfield of* L/K *in which* $\mathfrak{p}$ *splits completely. Here* $\mathfrak{p}$ *has ramification index and inertial constant one in* Z/K*.*

(iii) If P *is a prime of* Z *lying over* $\mathfrak{p}$*, then there is only one prime* $\mathfrak{P}$ *of* T *lying over* $\mathfrak{p}$*. Here* $\mathfrak{p}$ *is unramified and with inertial degree* $[T : Z] = f(\mathscr{P}/\mathfrak{p})$*, where* $\mathscr{P}$ *is any prime of* L *lying over* $\mathfrak{p}$*.*

(iv) If $\mathfrak{P}$ *is any prime of* T *lying over* $\mathfrak{p}$*, then there is only one prime* $\mathscr{P}$ *of* L *lying over* $\mathfrak{P}$*.*

Here $\mathfrak{P}$ has inertial degree one and ramification index $[L:T] = e(\mathscr{P}/\mathfrak{p})$.

Thus all the splitting of $\mathfrak{p}$ happens in the extension Z/K, all the inertia in T/Z, and all the ramification in L/T. Almost all primes $\mathfrak{p}$ are unramified in L, so most of the time we will have $T = L$.

We should also mention the connection of the decomposition group to the local fields. If w/v is an extension of places of L/K, then the decomposition group $\mathrm{Gal}(L/K)_v$ is 'really' the Galois group of L_w/K_v. Every K-isomorphism of L in $\mathrm{Gal}(L/K)_v$ will extend uniquely to a K_v-isomorphism of L_w, and every such isomorphism of L_w is obtained this way.

Last we mention the Frobenius. We are still assuming that L/K is abelian. If $\mathfrak{p}$ is a prime of K which is unramified in L, then the decomposition group of $\mathfrak{p}$ is isomorphic to the Galois group of residue fields. Now the Galois group of a finite extension of finite fields is cyclic, and it has a particularly nice generator, called the *Frobenius element*. The element σ of the decomposition group corresponding to that generator is also called the Frobenius element. It is the unique element of $\mathrm{Gal}(L/K)$ with the following property: for any prime $\mathscr{P}$ of L lying over $\mathfrak{p}$, and any $x \in \mathcal{O}_L$, σ has the effect

$$\sigma(x) - x^{\mathcal{N}\mathfrak{p}} \pmod{\mathscr{P}}$$

Here $\mathcal{N}\mathfrak{p}$ is the norm (cardinality of the residue field $\mathcal{O}_K/\mathfrak{p}$).

0.4 Cyclotomic extensions of $\mathbb{Q}$

We will discuss some properties of cyclotomic extensions which will be used later. Let m be an integer, and $\zeta = \zeta_m$ a primitive mth root of unity. The field $K := \mathbb{Q}(\zeta)$ is called the mth cyclotomic extension of $\mathbb{Q}$. The extension $K/\mathbb{Q}$ is abelian with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$. The isomorphism is the following: an integer a, relatively prime to m, is associated with the map $(\zeta \mapsto \zeta^a)$.

The ring of integers of K is $\mathbb{Z}[\zeta]$. A prime p of $\mathbb{Q}$ ramifies in K if and only if p divides m. If p is unramified, then the Frobenius element at p is the map $\zeta \mapsto \zeta^p$. It follow that for $p \nmid m$, the inertial degree of p is the multiplicative order of p modulo m.

Let K be any number field. A fundamental problem in algebraic number theory is the following: given a Galois extension L of K, produce an algorithm which determines how primes of K split in L. Class field theory more or less solves this problem for L/K abelian. That is, the main result of class field theory implies the existence of such an algorithm for any given abelian extension. Actually producing the algorithm is another problem entirely; conceivably one *could* do this by following the proofs in Section 4, but this would in general be a computational nightmare.

For the special case $K = \mathbb{Q}$, we can already describe how prime ideals split in abelian extensions if we assume the *Kronecker-Weber theorem* (which will be a corollary of the main theorems of class

field theory). The Kronecker-Weber theorem says that every abelian extesion of $\mathbb{Q}$ is contained in a cyclotomic extension. If L is an abelian extension of $\mathbb{Q}$, we can describe how primes split in L as follows:

1. Find (somehow) an integer m such that $L \subseteq \mathbb{Q}(\zeta)$, where ζ is a primitive mth root of unity.
2. Determine how the prime divisors of m split in L on your own. Don't complain, there are only finitely many of them.
3. Identify $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^*$ in the natural way, and under this identification regard $H := \mathrm{Gal}(\mathbb{Q}(\zeta)/L)$ as a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$.
4. For any prime number p not dividing m, let f be the smallest number for which $p^f \in H$. Then p splits into $\frac{[L:\mathbb{Q}]}{f}$ primes in L.

0.5 Haar measures on local fields

If G is a locally compact topological group (which we will always assume to be abelian and Hausdorff), then G admits a translation invariant Radon measure, called a *Haar measure*, which is unique up to scaling. For an introduction to locally compact topological groups, see the first chapter of *Fourier Analysis on Number Fields* by Ramakrishnan and Valenza. For more on the Haar measure, see the appendix.

Let us deduce the Haar measures on several locally compact groups. First we consider the additive locally compact groups $\mathbb{R}, \mathbb{C}$, and finite extensions of $\mathbb{Q}_p$. All these groups can be realized as a completion K_v, where K is a number field and v is a place of K.

First let v be finite. Then $\mathcal{O}_v$ is a compact subgroup of K_v. Therefore, there exists a Haar measure μ_v on K_v for which $\mu_v(\mathcal{O}_v) = 1$. If $\mathfrak{p} = \mathfrak{p}_v$ is the unique maximal ideal of $\mathcal{O}_v$ with generator $\pi = \pi_v$, and $k \geq 1$, then $[\mathcal{O}_v : \mathfrak{p}^k] = (\mathcal{N}\mathfrak{p})^k$.

Thus $\mathcal{O}_v$ is the disjoint union of $(\mathfrak{N}\mathfrak{p})^k = \frac{1}{||\pi||_v^k}$ cosets $a + \mathfrak{p}^k$, all of which have the same measure by translation invariance. Therefore $\mu_v(\mathfrak{p}^k) = \frac{\mu_v(\mathcal{O}_v)}{(\mathcal{N}\mathfrak{p})^k} = \frac{1}{(\mathcal{N}\mathfrak{p})^k} = ||\pi^k||_v$. Similarly when $k < 0$, the fractional ideal $\mathfrak{p}^k$ is the disjoint union of $(\mathfrak{N}\mathfrak{p})^{-k} = ||\pi^k||$ sets of the form $a + \mathcal{O}_v$ for $a \in K_v$. To see this, use the fact that every element of $\mathfrak{p}^k$ can be uniquely written as $a_k\pi^k + a_{k+1}\pi^{k+1} + \cdots$, where a_i are a distinct set of coset representatives for $\mathcal{O}_v/\mathfrak{p}$. Thus the Haar measure of $\mathfrak{p}_v$ is still equal to $||\pi||_v^k$.

What we have just shown is that for any $x \in K_v^*$

$$\mu_v(x\mathcal{O}_v) = ||x||_v \mu_v(\mathcal{O}_v) = ||x||_v$$

We contend that $\mu_v(xE) = ||x||_v \mu_v(E)$ for any $x \in K_v^*$ and any measurable set E. To see this, fix x and define a new Haar measure λ on K_v by letting $\lambda(E) = \mu_v(xE)$ for any μ_v-measurable set E (it is not too difficult to see that λ is indeed a Haar measure from the fact that μ_v is a Haar measure). By the uniqueness theorem for Haar measures, there exists a $\rho > 0$ such that $\lambda(E) = \rho\mu_v(E)$ for all measurable sets E. But we can compute

$$\lambda(\mathcal{O}_v) = \mu_v(x\mathcal{O}_v) = ||x||_v \mu_v(\mathcal{O}_v)$$

and by uniqueness we get $\rho = ||x||_v$. Thus

$$\mu_v(xE) = \lambda(E) = \rho\mu_v(E) = ||x||_v \mu_V(E)$$

If $K_v = \mathbb{R}$, then the Haar measure μ_v is just a scale of the Lebesgue measure on $\mathbb{R}$. Normalize μ_v to be the actual Lebesgue measure, so $\mu_v[0,1] = 1$.

If $K_v = \mathbb{C}$, then μ_v is again a scale of the Lebesgue measure, this time on $\mathbb{R} \times \mathbb{R}$. Normalize μ_v to be twice the ordinary Lebesgue measure here.

Note that for v complex, $[K_v : \mathbb{R}] = 2$, so $||a + bi||_v = a^2 + b^2$. *By the way we have chosen the Haar measures μ_v and the absolute values $||\cdot||_v$, we see that for any place v, any $x \in K_v^*$ and any measurable set $E \subseteq K_v$:*

$$\mu_v(xE) = ||x||_v \mu_v(E)$$

This will be important later when we introduce the ring of adeles.

1 Adeles and Ideles

1.1 The direct limit topology

Let $\mathcal{S}$ be an ordered set, with the property that for any $x, y \in \mathcal{S}$, there exists a $z \in \mathcal{S}$ such that $z \geq x$ and y. Let also X be a set, $X_s : s \in \mathcal{S}$ a collection of subsets of X. Assume that:

- Each X_s is a topological space.
- $s_1 \leq s_2$ if and only if $X_{s_1} \subseteq X_{s_2}$, in which case the topology on X_{s_1} is induced by that of X_{s_2} (that is, the open sets of X_{s_1} consist of all intersections $V \cap X_{s_1}$, where V is an open set of X_{s_2}).
- $X = \bigcup_{s \in \mathcal{S}} X_s$

We will then define a topology on X, by saying that $V \subseteq X$ is open in X if and only if $V \cap X_s$ is open in X_s for each $s \in \mathcal{S}$. We call this the **direct limit topology**, and write $X = \lim X_s$ to refer to X as a topological space.

Lemma 1. *Let Y be another topological space, and $f : X \to Y$ a function. Then f is continuous if and only if $f_{|X_s} : X_s \to Y$ is continuous for all $s \in \mathcal{S}$.*

Proof. Let U be any open set of Y. To say that $f_{|X_s}$ is continuous is to say that $f^{-1}_{|X_s}(U)$ is always open in X_s. But $f^{-1}_{|X_s}(U) = f^{-1}(U) \cap X_s$, and $f^{-1}(U)$ is open in X if and only if $f^{-1}(U) \cap X_s$ is open in X_s for all $s \in \mathcal{S}$. So the assertion is obvious. □

Proposition 2. *If each X_s is open in X, then the topology on X_s is induced by the topology on X. Otherwise, the topology on X_s may be finer than the topology thereon induced by X.*

Proof. Consider the topology on X_s induced by X. If U is an open set of X, then $U \cap X_{s'}$ is open in $X_{s'}$ for all s', in particular for s. So, the existing topology on X_s is no coarser as fine as that induced by X.

Suppose that $X_{s'}$ is open in X for all s'. Let V be an open set of X_s. We claim that $V = U \cap X_s$ for some open set U of X. Of course, it is sufficient to show that V itself is open in X, i.e. $V \cap X_{s'}$ is open in $X_{s'}$ for all s'. To do this, let s'' be a member of $\mathcal{S}$ which is $\geq s$ and s'. Then $V = W \cap X_s$ for some open set W of $X_{s''}$. We have

$$V \cap X_{s'} = (W \cap X_{s''}) \cap (X_{s'} \cap X_{s''})$$

where $W \cap X_{s''}$ and $X_{s'} \cap X_{s''}$ are both open in $X_{s'}$. Thus $V \cap X_{s'}$ is open in $X_{s'}$, as required. □

Under the assumption that each X_s is open in X (which is not always true), we have that direct limits commute with direct products.

Proposition 3. *Suppose each X_s is open in X. Let X_1 be the set $X \times X$ endowed with the product topology, and X_2 the topological space $\lim X_s \times X_s$, where each $X_s \times X_s$ is given the product topology. Then $X_1 = X_2$, as sets and topological spaces.*

Proof. First let's establish that X_1 and X_2 are the same set:

$$X_1 = (\bigcup_{s \in \mathcal{S}} X_s) \times (\bigcup_{s \in \mathcal{S}} X_s)$$

$$X_2 = \bigcup_{s \in \mathcal{S}} X_s \times X_s$$

It is clear that $X_2 \subseteq X_1$. Conversely let $(a, b) \in X_1$ with, say, $a \in X_{s_1}$ and $b \in X_{s_2}$. Then there is a set X_{s_3} containing X_{s_1} and X_{s_2}, so $(a, b) \in X_{s_3} \times X_{s_3} \subseteq X_2$.

Now let $O \subseteq X \times X$ be open in X_1. To show O is open in X_2, we may assume that O is equal to a product $A \times B$, where A, B are both open in X (for O is a union of such things). To show that O is open in X_2, we must show that $O \cap (X_s \times X_s)$ is open in $X_s \times X_s$ for each s. But the intersection of $O = A \times B$ and $X_s \times X_s$ is just $A \cap X_s \times B \cap X_s$, which is open in $X_s \times X_s$ as a product of open sets.

Conversely suppose O is open in X_2. So $O \cap (X_s \times X_s)$ is open in $X_s \times X_s$ for each s. So this latter intersection is a union of products $A \times B$, where A, B are open in X_s. But since X_s is open in X, so are A and B. So $O \cap (X_s \times X_s)$ is open in $X \times X = X_1$.

Finally since $X \times X = \bigcup_{s \in S} X_s \times X_s$, we have that

$$O = \bigcup_{s \in S} O \cap (X_s \times X_s)$$

So O is open in X_1. □

We will assume from now on that each X_s is open in X.

Corollary 4. *Suppose X is a group, with each X_s a subgroup. If each X_s is a topological group, i.e. the mapping $X_s \times X_s \to X_s$ given by*

$$(x, y) \to xy^{-1}$$

is continuous, then X will also be a topological group.

Proof. This follows from Proposition 3 and Lemma 1.

□

Recall that a topological space is *locally compact* if every point therein has a compact neighborhood. $\mathbb{R}, \mathbb{C}$, $\mathbb{Q}_p$ are examples of locally compact spaces. A finite product of locally compact spaces is locally compact (hence so is any finite extension of $\mathbb{Q}_p$).

Lemma 5. *If K is a compact subset of X_s, then it is also a compact subset of X. Also if each X_s is locally compact, then so is X.*

Proof. We assumed that X_s was open in X, so X_s inherits the subspace topology from X by Proposition 2. Compactness does not depend on the ambient space, so K being compact in X_s means that it is also compact in X. So a set $O \subseteq X_s$ is open, or compact, in X_s if and only if it is so in X. From this observation the second assertion is obvious.

□

We will now describe a slightly more concrete scenario of which the preceding theory is a generalization. Let $G_v : v \in \mathcal{T}$ be a collection of topological groups. Then the product

$$\mathscr{G} = \prod_{v \in \mathcal{T}} G_v$$

will also be a topological group. Let us assume that the G_v are also locally compact. However, even with this assumption $\mathscr{G}$ will not be locally compact in general: a product of topological spaces $\prod X_i$ is locally compact if and only if each X_i is locally compact and all but finitely many X_i are compact. Our goal will be to identify a certain subgroup of $\mathscr{G}$ and place upon it a topology which *is* locally compact.

Suppose the indexing set $\mathcal{T}$ is equal to a union $\mathcal{A} \cup \mathcal{B}$, where $\mathcal{B}$ is finite, and H_v is a compact open subgroup of G_v for each $v \in \mathcal{A}$. For a finite subset $S \subseteq \mathcal{T}$ containing $\mathcal{B}$, let

$$G_S = \prod_{v \in S} G_v \prod_{v \notin S} H_v$$

Then G_S in the product topology is a locally compact topological group by the criterion we just mentioned. If we let $\mathcal{S}$ be the set of subsets $S \subseteq \mathcal{T}$ which contain $\mathcal{B}$, then we define

$$G = \bigcup_{S \in \mathcal{S}} G_S$$

and we give G the direct limit topology. So G consists of those $(x_v) \in \mathscr{G}$ for which $x_v \in H_v$ for all but finitely many v.

Proposition 6. *Each G_S is open in G. Hence G is a locally compact topological group.*

Proof. Let S' be another member of $\mathcal{S}$. We want to show that $G_S \cap G_{S'}$ is open in $G_{S'}$. We have

$$G_S \cap G_{S'} = \prod_{v \in S \cap S'} G_v \prod_{v \in S' \setminus S} H_v \prod_{v \in S \setminus S'} H_v \prod_{v \notin S \cup S'} H_v$$

which differs from $G_{S'}$ only where $v \in S' \setminus S$, in which place we have H_v instead of G_v. But H_v is open, so $G_S \cap G_{S'}$ is a product of open sets, almost all of which are not proper, so this intersection is open in $G_{S'}$ under the product topology. □

We finally make the observation that the map $\tau : G_v \to G$, which sends an x to the element whose vth place is x, and all of whose other places are the identity, is a topological embedding. By this I mean it is a group monomorphism whose domain is homeomorphic to its image. Furthermore the image of τ is closed in G_S. This is obvious, because if $S = \{v\} \cup \mathcal{B}$, then G_S contains a homeomorphic copy of G_v as a closed subgroup.

The discussion above has the following application to number theory. Let K be a finite extension of $\mathbb{Q}$, with ring of integers $\mathcal{O}$. A *place* of K is an equivalence class of absolute values on K, two absolute values being equivalent if they induce the same topology on K. We may identify each place with a choice of absolute value v of which the place is an equivalence class. We will call a place *finite* if it is nonarchimedean. There is one place for each prime of $\mathcal{O}$. Otherwise we will call the place *infinite*, in which case it is induced from a real or nonreal-complex embedding of K (and is called *real* or *complex* respectively).

If v is a finite place, denote by K_v the completion of K with respect to v. If v is real or complex, then K_v will mean $\mathbb{R}$ or $\mathbb{C}$. In any case K_v is a locally compact group with respect to addition. If v is finite, let $\mathcal{O}_v$ be the completion of $\mathcal{O}$ with respect to v; it is a compact, open subgroup of K_v. All this was described in more detail in the introduction.

We may analogously consider the operation of multiplication: K_v^* is a locally compact topological group, and for v finite, $\mathcal{O}_v^*$ is a compact open subgroup of K_v^*.

Let S be a finite set of places of K which include the infinite places (of which there are at most $[K : \mathbb{Q}]$, the collection of which we denote by S_∞). Let $\mathcal{S}$ be the set of all such S.

For each place v, we take $G_v = K_v$, and $H_v = \mathcal{O}_v$ when $v \notin S_\infty$. We define the set $\mathbb{A}_K$ of **adeles** to be the direct limit G as defined above. So

$$\mathbb{A}_K = \bigcup_{S \in \mathcal{S}} \mathbb{A}_K^S$$

where we set

$$\mathbb{A}_K^S = G_S = \prod_{v \in S} K_v \prod_{v \notin S} \mathcal{O}_v$$

On the other hand, we can let $G_v = K_v^*$, and $H_v = \mathcal{O}_v^*$ when v is finite. We define the set $\mathbb{I}_K$ of **ideles** to again be the direct limit with the G_v so defined. So

$$\mathbb{I}_K = \bigcup_{S \in \mathcal{S}} \mathbb{I}_K^S$$

where

$$\mathbb{I}_K^S = \prod_{v \in S} K_v^* \prod_{v \notin S} \mathcal{O}_v^*$$

Thus $\mathbb{A}_K$ is a topological group with respect to addition, and $\mathbb{I}_K$ is a topological group with respect to multiplication.

A *topological ring* is a ring with a topology with respect to which addition and multiplication are continuous. For example, K_v is a topological ring, and so is $\mathcal{O}_v$ for $v < \infty$. Any product of topological rings is a topological ring in the product topology. Unlike topological groups, we usually do not care whether or not the ring is Hausdorff or not. But we will not encounter any non-Hausdorff spaces in these notes anyway.

Lemma 7. *Multiplication is a continuous function $\mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$. Hence $\mathbb{A}_K$ is a topological ring.*

Proof. For each S (containing the infinite places), $\mathbb{A}_K^S$ is a topological ring in the product topology, so the multiplication function $\mathbb{A}_K^S \times \mathbb{A}_K^S \to \mathbb{A}_K^S$ is continuous. And $\mathbb{A}_K^S$, being open in $\mathbb{A}_K$, inherits its topology from the subspace topology of $\mathbb{A}_K$ (Proposition 2). Thus multiplication is a continuous function

$$\mathbb{A}_K^S \times \mathbb{A}_K^S \to \mathbb{A}_K^S \to \mathbb{A}_K$$

Since this map is continuous for each S, and $\mathbb{A}_K \times \mathbb{A}_K$ is topologically the direct limit of the spaces $\mathbb{A}_K^S \times \mathbb{A}_K^S$ (Proposition 3), our conclusion follows from Lemma 1.

□

Many topological properties from $\mathbb{A}_K^S$ and $\mathbb{I}_K^S$ are transferred to their respective direct limits. But direct limits in general do not preserve topological interactions between these sets. Algebraically, each $\mathbb{I}_K^S$ is the group of units of $\mathbb{A}_K^S$, and therefore $\mathbb{I}_K$ is the group of units of $\mathbb{A}_K$. However, while it is true that $\mathbb{I}_K^S$ inherits its topology as a subspace of $\mathbb{A}_K^S$ (for both spaces are taken in the product topology), it is *not* true that the topology of $\mathbb{I}_K$ is the subspace topology from $\mathbb{A}_K$. Moreover, $\mathbb{I}_K^S$ is open in $\mathbb{A}_K^S$ (each multiplicand is open), but $\mathbb{I}_K$ is not open in $\mathbb{A}_K$.

There is a more natural way to see the idelic topology as a natural consequence of the adelic. Let $j : \mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K$ be the injective function $x \mapsto (x, x^{-1})$, and T the image of $\mathbb{I}_K$ under j. Then T inherits the subspace topology from $\mathbb{A}_K \times \mathbb{A}_K$ (taken in the product topology), which induces a topology on $\mathbb{I}_K$.

Proposition 8. *This topology is the same as the direct limit topology on $\mathbb{I}_K$.*

Proof. Let Z_1 denote the ideles in the direct limit topology, and Z_2 the ideles in the topology we just introduced above. Remember that $\mathbb{A}_K \times \mathbb{A}_K$ is the topological direct limit of the products $\mathbb{A}_K^S \times \mathbb{A}_K^S$.

Let $M \subseteq \mathbb{I}_K$. If M is open in Z_1, so is M^{-1} (Z_1 is a topological group, inversion is a homeomorphism), so $M \cap \mathbb{I}_K^S$ is open in $\mathbb{I}_K^S$ for each S, and so is M^{-1}. Hence

$$(M \times M^{-1}) \cap (\mathbb{I}_K^S \times \mathbb{I}_K^S) = (M \cap \mathbb{I}_K^S) \times (M^{-1} \cap \mathbb{I}_K^S)$$

is open in $\mathbb{I}_K^S \times \mathbb{I}_K^S$. But $\mathbb{I}_K^S$ is open in $\mathbb{A}_K^S$, so

$$(M \times M^{-1}) \cap (\mathbb{A}_K^S \times \mathbb{A}_K^S) = (M \cap \mathbb{A}_K^S) \times (M^{-1} \cap \mathbb{A}_K^S)$$

is open in $\mathbb{A}_K^S \times \mathbb{A}_K^S$. Hence $M \times M^{-1}$ is open in $\mathbb{A}_K \times \mathbb{A}_K$, giving us that $(M \times M^{-1}) \cap T = j(M)$ is open in T. Thus M must be open in Z_2.

For the converse, observe that the map $x \mapsto (x, x^{-1})$ is a continuous function $\mathbb{I}_K^S \to \mathbb{I}_K^S \times \mathbb{I}_K^S$, since it is continuous into each component. We have inclusions in the subspace topology $\mathbb{I}_K^S \times \mathbb{I}_K^S \subseteq \mathbb{A}_K^S \times \mathbb{A}_K^S \subseteq \mathbb{A}_K \times \mathbb{A}$, so we really have described a continuous function

$$\mathbb{I}_K^S \to \mathbb{A}_K \times \mathbb{A}_K$$

This is continuous for each S, so the same function $Z_1 \to \mathbb{A}_K \times \mathbb{A}_K$ is continuous. The image of this map $x \mapsto (x, x^{-1})$ is T, and by the very definition of T the inverse map $T \to Z_2$ is a homeomorphism. Thus the identity map on $\mathbb{I}_K$ is a continuous composition

$$Z_1 \to T \to Z_2$$

which shows that the open sets of Z_2 are contained in the open sets of Z_1.

□

The above characterization of the idele topology is inspired by the more general situation of a (commutative) topological ring R with group of units R^*. Even though the multiplication is a continuous function $R^* \times R^* \to R$, inversion $x \mapsto x^{-1}$ need not be continuous. The topology on

R^* resulting from the inclusion $R^* \to R \times R, x \mapsto (x, x^{-1})$ is such that multiplication and inversion are continuous in R^*.

1.2 Algebraic and Topological Embeddings

Each $\mathbb{A}_K^S$ is an open, hence closed, subgroup of $\mathbb{A}_K$. Thus a subset E of $\mathbb{A}_K^S$ is open, or closed, there if and only if it is the same in $\mathbb{A}_K$. Remember also that properties like compactness, discreteness, and connectedness do not depend on the ambient space: if E is a compact, discrete, or connected etc. subset of $\mathbb{A}_K^S$, it is also a compact, discrete etc. subset of $\mathbb{A}_K$. The same principle holds for ideles, since $\mathbb{I}_K^S$ is an open, hence closed, subgroup of $\mathbb{I}_K$.

Lemma 9. *The diagonal embedding*

$$K \to \prod_v K_v$$

maps K into $\mathbb{A}_K$, and is a ring monomorphism. The image of K is discrete in the adele topology. Similarly we have a diagonal embedding $K^* \to \mathbb{I}_K$ which is a group monomorphism. The image of K^* is discrete in the idele topology.

Proof. For $0 \neq x \in K$, we know that x is a unit at almost all places. So it is clear that the diagonal embeddings send K (resp. $K^* = K \setminus \{0\}$) into the adeles (resp. ideles).

Let T be the image of K under the diagonal embedding. To say that T is discrete means that for any $x \in T$, the singleton set $\{x\}$ is open in T, i.e. there exists a neighborhood V of x which does not contain any other element of T. We do this first when $x = 0$. Let

$$V = \prod_{v|\infty} B_v(0, \frac{1}{2}) \prod_{v<\infty} \mathcal{O}_v$$

where $B_v(0, \frac{1}{2})$ is the ball of center 0 and radius $\frac{1}{2}$ in K_v. Clearly V is open in $\mathbb{A}_K^{S_\infty}$, hence in $\mathbb{A}_K$, and is a neighborhood of 0. And V cannot contain any other element $0 \neq y$ of K, since then $\prod_v ||y||_v$ is strictly less than 0, and it is supposed to be 1.

So V is a neighborhood of 0 which does not contain any other elements in the image of K. Since $\mathbb{A}_K$ is a topological group with respect to addition, proving the case $x = 0$ implies the result for all x: if x is any element of K, then $x + V$ is a neighborhood of x which is disjoint from all other $y \in K$.

Thus the image of K under the diagonal embedding is discrete in $\mathbb{A}_K$. The argument for ideles is almost identical, just use $x = 1$ instead of 0.

□

Warning: the diagonal embedding of K into $\mathbb{A}_K$ is not *really* a diagonal embedding, if at the infinite places we identify K_v as a subfield of $\mathbb{C}$. For example, if $K = \mathbb{Q}(\sqrt{2})$, the embedding of K

into $\mathbb{C}$ are given by the inclusion map and the map $\sqrt{2} \mapsto -\sqrt{2}$. We would inject $1+\sqrt{2}$ into the adeles as

$$(1+\sqrt{2}, 1-\sqrt{2}, 1+\sqrt{2}, 1+\sqrt{2}, ...)$$

From now on we will usually identify K (resp. K^*) with its image in $\mathbb{A}_K$ (resp. $\mathbb{I}_K$). In particular K and K^* will be taken as topological groups in the discrete topology, unless otherwise stated.

Since K^* is a discrete subgroup of $\mathbb{I}_K$, it is closed, so the quotient $C_K := \mathbb{I}_K/K^*$ is a topological group. We call C_K the **idele class group**.

For $x \in \prod_v K_v$, let x_v denote the vth component of x. If $x \in \mathbb{I}_K$, then $x \in \mathbb{I}_K^S$ for some S, and hence $||x_v||_v$ (or just $||x||_v$) is equal to 1 for almost all v, i.e. all $v \notin S$. Thus

$$||x|| := \prod_v ||x||_v$$

is a finite product, which we call the **idele norm** of x. Since each map $||-||_v : K_v \to \mathbb{R}$ is continuous, so is the idele norm on $\mathbb{I}_K^S$ as a finite product of continuous functions. Thus the idele norm on $\mathbb{I}_K$ is continuous (Lemma 1). We let

$$\mathbb{I}_K^1 = \{x \in \mathbb{I}_K : ||x|| = 1\}$$

which is a closed subgroup of $\mathbb{I}_K$, since it is the preimage of the closed set $\{1\}$. By the product formula, K^* is contained in $\mathbb{I}_K^1$, so $\mathbb{I}_K^1$ is a saturated closed set with respect to the quotient $\mathbb{I}_K \to \mathbb{I}_K/K^*$. Thus $C_K^1 := \mathbb{I}_K^1/K^*$ is a closed subgroup of C_K.

Lemma 10. *$\mathbb{I}_K^1$ is also closed as a subset of the adeles.*

Proof. Let $\alpha \in \mathbb{A}_K \setminus \mathbb{I}_K^1$. We must find a neighborhood W of α which is disjoint from $\mathbb{I}_K^1$.

Case 1: $\prod_v ||\alpha||_v < 1$.

The set S consisting of archimedean places as well as those v for which $||\alpha_v|| > 1$ is finite. Adjoin finitely many places to S to ensure that $\prod_{v \in S} ||\alpha||_v < 1$. For $\epsilon > 0$ and small, let $W_v = \{x \in K_v : ||x - \alpha_v||_v < \epsilon$ and define

$$W = \prod_{v \in S} W_v \prod_{v \notin S} \mathcal{O}_v$$

Then W is a neighborhood of α, and as long as ϵ is chosen small enough, we will have $\prod_v ||\beta||_v < 1$ for any $\beta \in W$.

Case 2: $\prod_v ||\alpha||_v > 1$.

Let $C = \prod_v ||\alpha||_v$. I claim all but finitely many places v satisfy the following property: if $x \in K_v$ and $||x||_v < 1$, then $||x||_v < \frac{1}{2C}$. This is true because for $\mathfrak{p}_v$ lying over p, we have $||x||_v < 1$ implies $||x||_v \leq ||\mathfrak{p}||_v = |p^{f(\mathfrak{p}/p)}|_p \leq \frac{1}{p}$, and there are only finitely many prime numbers p satisfying $\frac{1}{p} \geq \frac{1}{2C}$.

So, take S to include all the archimedean places, all those places v for which $||\alpha||_v > 1$, all those places for which $||\alpha||_v < 1$ (there must be only finitely many, otherwise $\prod_v ||\alpha||_v$ converges to 0) and all those places which do *not* satisfy the property we just mentioned. For small $\epsilon > 0$, set $W_v = \{x \in K_v : ||x - \alpha_v||_v < \epsilon\}$, and define

$$W = \prod_{v \in S} W_v \prod_{v \notin S} \mathcal{O}_v$$

just as we have above. Then W is a neighborhood of α, and as long as ϵ is small enough, we can ensure that any $\beta \in W$ will have $\prod_v ||\beta||_v \neq 1$. As long as we choose ϵ to be very small, if $\beta \in W$ and $||\beta||_v = 1$ for $v \notin S$, then $\prod_{v \in S} ||\beta||_v = \prod_v ||\beta||_v$ will be strictly between 1 and $2C$.

On the other hand, if $\beta \in W$ and $||\beta||_{v_0} < 1$ for some $v_0 \notin S$, then $||\beta||_{v_0} < \frac{1}{2C}$, so

$$\prod_v ||\beta||_v \leq ||\beta||_{v_0} \prod_{v \in S} ||\beta||_v < \frac{1}{2C} \cdot 2C = 1$$

□

Suppose C, X, Y are subsets of a set Z, and C is contained in both X and Y. If X and Y are topological spaces, when is the induced topology on C from Y finer than the induced topology from X? By the definition of the subspace topology, this happens if and only if for any open set W of X, there exists an open set V of Y such that $V \cap C = W \cap C$. An equivalent and more easily applicable condition is that for any open set W of X and any $\alpha \in W \cap C$, there exists an open neighborhood V of α such that $V \cap C \subseteq W$.

Lemma 11. *The subspace topologies which $\mathbb{I}_K^1$ inherits from the ideles and the adeles are the same.*

Proof. Let W be an open set of the adeles, and $\alpha \in W \cap \mathbb{I}_K^1$. To show that the idele topology on $\mathbb{I}_K^1$ is finer than the adele topology, we must find an idele-open neighborhood V of α such that $V \cap \mathbb{I}_K^1 \subseteq W$. Actually, we will just find a V so that $V \subseteq W$.

Now $||\alpha||_v = 1$ for almost all v, say all $v \notin S$. Any neighborhood of α in the adele topology contains a neighborhood of the form

$$W' = \prod_{v \in S} W_v \prod_{v \notin S} \mathcal{O}_v$$

where W_v is a neighborhood of α_v not containing 0. We may suppose S contains all the archimedean places; if not, it is fine to shrink W' further. But then W' contains

$$V := \prod_{v \in S} W_v \prod_{v \notin S} \mathcal{O}_v^*$$

which is an open neighborhood of α in the idele topology.

Conversely suppose V is open in the ideles, and $\alpha \in V \cap \mathbb{I}_K^1$. To show that the adele topology on $\mathbb{I}_K^1$ is finer than the idele topology, we must find an adele-open neighborhood W of α such that $W \cap \mathbb{I}_K^1 \subseteq V$.

Now V contains an idele-open neighborhood of α of the form

$$V' = \prod_{v \in S} E_v \prod_{v \notin S} \mathcal{O}_v^*$$

where S contains all the archimedean places as well as all those places v for which $\alpha_v \notin \mathcal{O}_v^*$, and

$$E_v = \{x \in K_v : ||x - \alpha_v||_v < \epsilon\}$$

where $\epsilon > 0$ is very small. In order for V' to be open in the ideles, ϵ would in any case have to be small enough to exclude 0 from E_v. We can also make ϵ small enough so that for any $\beta \in V'$,

$$\prod_{v \notin S} ||\beta||_v$$

is extremely close to 1 (as close as we like). Let

$$W = \prod_{v \in S} E_v \prod_{v \notin S} \mathcal{O}_v$$

so W is an open set of the adeles containing α. Now the reciprocals of the prime numbers $\frac{1}{2}, \frac{1}{3}, ...$, hence the absolute values $||x||_v$ for v finite and $x \in \mathfrak{p}_v$, are bounded away from 1. We can use this fact to argue that if ϵ is chosen small enough, then $W \cap \mathbb{I}_K^1 \subseteq V'$. For suppose $\beta \in W \cap \mathbb{I}_K^1$. To show $\beta \in V'$, we have to show that $\beta \in \mathcal{O}_v^*$ for $v \notin S$. Already $\prod_{v \in S} ||\beta||_v$ is extremely close to 1. If $v_0 \notin S$ is a place for which $\beta_{v_0} \notin \mathcal{O}_v^*$ (which means $\beta_{v_0} \in \mathfrak{p}_{v_0}$), $||\beta||_{v_0}$ will be small enough so that $||\beta||_{v_0} \cdot \prod_{v \in S} ||\beta||_v$, and hence $||\beta||$ (for $||\beta||_v \leq 1$ for all $v \notin S$), is strictly less than 1.

□

We define the **S-units**, K_S, to be the group of $x \in K^*$ which are units at all $v \notin S$. In particular $K_{S_\infty} = \mathcal{O}_K^*$. Identifying the elements of K^* as ideles, we have $K_S = \mathbb{I}_K^S \cap K^*$. Since K^* is discrete, so is K_S, so K_S is closed. Hence $\mathbb{I}_K^S / K_S$ is a topological group. Also

$$\mathbb{I}_K^{S,1} = \{x \in \mathbb{I}_K^S : ||x|| = 1\} = \mathbb{I}_K^S \cap \mathbb{I}_K^1$$

is closed (in $\mathbb{I}_K^S, \mathbb{I}_K$, same thing) and contains K_S, so $\mathbb{I}_K^{S,1} / K_S$ is a closed subgroup of $\mathbb{I}_K^S / K_S$.

Lemma 12. *There are embeddings of topological groups*

$$\mathbb{I}_K^S/K_S \to \mathbb{I}_K/K^*$$

$$\mathbb{I}_K^{S,1}/K_S \to \mathbb{I}_K^1/K^*$$

where the image of the group on the left is an open and closed subgroup on the right.

To prove the next proposition, we will rely on some technical details of direct limits, which we leave as exercises:

Exercise: Suppose $X = \lim_{s\in\mathcal{S}} X_s$ in the sense we defined earlier, and $\mathcal{S}_1 \subsetneq \mathcal{S}$. Find a sufficient condition for which we still have $X = \lim_{s\in\mathcal{S}_1} X_s$.

Exercise: Let $X = \lim_{s\in\mathcal{S}} X_s, Y = \lim_{t\in\mathcal{T}} Y_t$, and assume each X_s, Y_t is open in X, Y. Let $\tau : \mathcal{S} \to \mathcal{T}$ be an order preserving bijection, and $f : X \to Y$ a function such that for each s the restriction $X_s \to Y_{\tau(s)}$ is a homeomorphism. Show that f is a homeomorphism. If the X_s, Y_t, X, Y are all topological groups, and each $f_{|X_s}$ is a topological group isomorphism, show that f is as well.

Theorem 13. *Let L be a finite extension of K. There is an isomorphism of topological groups*

$$\prod_{i=1}^n \mathbb{A}_K \to \mathbb{A}_L$$

where $n = [L : K]$. Under this isomorphism $\prod_{i=1}^n K$ corresponds to L.

Proof. Let S_0 be a finite set of places of K, containing all the archimedean ones. Then one can argue, as in the first exercise, that $\mathbb{A}_K = \lim_{S\supseteq S_0} \mathbb{A}_K^S$. Proposition 3 extends to finitely many products, giving us

$$\prod_{i=1}^n \mathbb{A}_K = \lim_S \prod_{i=1}^n \mathbb{A}_K^S$$

Here we are only taking those S which contain S_0. Given such an S, let T be the set of places of L which lie over all the places in S. Again, we can argue that $\mathbb{A}_L = \lim_T \mathbb{A}_L^T$. Fix a basis for L/K. For each place of K, we know there is a homeomorphism (in fact, an isomorphism of topological groups)

$$\Phi_v : \prod_v K_v \to \prod_{w|v} L_w$$

which is defined using this basis. It sends $\prod_{i=1}^n K$ to $\prod_{w|v} L$. For almost all v (say, all those which are

not in S_0), restriction induces another topological group isomorphism

$$\Phi_v : \prod_{i=1}^{n} \mathcal{O}_v \to \prod_{w|v} \mathcal{O}_w$$

(see the last part of the appendix on the topological tensor product). Now a collection of isomorphisms $A_i \to B_i$ induces an isomorphism on the product $\prod A_i \to \prod B_i$, so we obtain a topological group isomorphism

$$\prod_{v \in S_0} \prod_{i=1}^{n} K_v \cdot \prod_{v \notin S_0} \prod_{i=1}^{n} \mathcal{O}_v \to \prod_{w \in T} \prod_{w|v} L_w \cdot \prod_{w \notin T} \prod_{w|v} \mathcal{O}_w$$

The product topology is commutative/associative, so we have actually described an isomorphism

$$\prod_{i=1}^{n} \mathbb{A}_K^S \to \mathbb{A}_L^T$$

Our claim then follows from the second exercise.

□

1.3 Compactness theorems

Theorem 14. *$\mathbb{A}_K/K$ is compact.*

Proof. By Theorem 13 we have an isomorphism of topological groups

$$\mathbb{A}_K/K \cong \frac{\mathbb{A}_{\mathbb{Q}} \oplus \cdots \oplus \mathbb{A}_{\mathbb{Q}}}{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}} \cong \mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \oplus \cdots \oplus \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$$

so it suffices to just prove the case where $K = \mathbb{Q}$.

To do this, we let

$$W = [-\frac{1}{2}, \frac{1}{2}] \times \prod_p \mathbb{Z}_p$$

where W is clearly a compact subset of $\mathbb{A}_{\mathbb{Q}}$. We have a continuous composition $W \to \mathbb{A}_{\mathbb{Q}} \to \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$, so it suffices to show that this composition is surjective. In other words, given any adele $\alpha \in \mathbb{A}_{\mathbb{Q}}$, find an $x \in \mathbb{Q}$ such that $\alpha - x \in W$.

For each prime p, $\alpha_p \in \mathbb{Q}_p$ can be written as a sum

$$\frac{a_k}{p^k} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + \cdots$$

where $a_i \in \{0, 1, ..., p-1\}$. If we let $b_p := \frac{a_k}{p^k} + \cdots + \frac{a_{-1}}{p}$, then $\alpha_p - b_p \in \mathbb{Z}_p$.

Actually, $b := \sum_p b_p$ is a finite sum, because $\alpha_p \in \mathbb{Z}_p$ for almost all p, in which case $b_p = 0$ from

the way it is defined. And, for any prime number q, $b_q \in \mathbb{Z}_p$ for every $p \neq q$ (because $\frac{1}{q}$ will be a unit). Thus $b - b_p \in \mathbb{Z}_p$ for every p, and hence

$$|\alpha_p - b|_p = |(\alpha_p - b_p) + (b_p - b)|_p \leq \text{Max}\{|\alpha_p - b_p|_p, |b - b_p|_p\} \leq 1$$

We have found a rational number b such that

$$\alpha - b \in \mathbb{A}_{\mathbb{Q}}^{S_\infty} = \mathbb{R} \times \prod_p \mathbb{Z}_p$$

Let v be the unique infinite place of $\mathbb{Q}$. The fact that $[-\frac{1}{2}, \frac{1}{2}]$ has length 1 means that we can find an integer s such that $(\alpha_v - b) - s \in [-\frac{1}{2}, \frac{1}{2}]$. Since $\alpha_p - b \in \mathbb{Z}_p$ for all p, so is $\alpha_p - b - s$. Thus $\alpha - x \in W$, where $x = b + s$. □

Corollary 15. *There exists a sequence of positive numbers δ_v, with $\delta_v = 1$ for almost all v, such that $\mathbb{A}_K = W + K$, where*

$$W = \prod_v \{x \in K_v : |x|_v \leq \delta_v\}$$

Proof. Suppose by way of contradiction that $W + K \subsetneq \mathbb{A}_K$ for every set W of that form. Then $\pi(W) = \pi(W + K)$ is properly contained in $\mathbb{A}_K/K$, where π is the quotient map $\mathbb{A}_K \to \mathbb{A}_K/K$. We can modify W to make it an open set: just replace $\leq$ by $<$ when v is an infinite place. Still we will have $\pi(W) \subsetneq \mathbb{A}_K/K$. Furthermore, we can find a sequence of these sets W, say $W_1 \subsetneq W_2 \subsetneq \cdots$ for which

$$\mathbb{A}_K = \bigcup_n W_n$$

by increasing the δ_v, finitely many at a time. Hence $\mathbb{A}_K/K = \bigcup_n \pi(W_n)$. And quotient maps of topological groups are open maps, so we have produced an open cover with no finite subcover, contradicting the fact that $\mathbb{A}_K/K$ is compact. □

The compactness theorem we just proved can be used to produce two powerful results. First, there is another compactness result, this time for the ideles, which is equivalent to the classical unit theorem. Second, there is the strong approximation theorem, which generalizes the existing approximation theorem.

Let μ_v be a Haar measure on K_v. As indicated in the introduction, it is possible to normalize μ_v so that $\mu_v(xE) = ||x||_v \mu_v(E)$ for any $0 \neq x \in K_v$ and $E \subseteq K_v$ measurable. For example if v is finite, all we have to do is normalize μ_v so that $\mathcal{O}_v$ has measure 1. Since $\mathbb{A}_K$ is a locally compact topological group, it also has a Haar measure μ. It is possible to normalize μ to be the product of the local Haar measures, in the sense that if S is a finite set of places containing all archimedean

ones, and $E_v \subseteq K_v : v \in S$ is μ_v-measurable, then

$$\mu(\prod_{v\in S} E_v \prod_{v\notin S} \mathcal{O}_v) = \prod_{v\in S} \mu_v(E_v)$$

It follows, by an identical argument as the one given in the introduction for $\mu_v, v < \infty$, that if $x \in \mathbb{I}_K$ and $E \subseteq \mathbb{A}_K$ is μ-measurable, then $\mu(xE) = ||x||\mu(E)$.

A complete justification for why μ can be normalized as we have claimed would be too long to include in this chapter. The approach we are familiar with depends on the Riesz representation theorem and a special version of Fubini's theorem. In the appendix on Haar measures, we sketch the proof and give references on where to find more rigorous justifications of certain claims.

Lemma 16. *(Minkowski-Chevalley-Weil) There exists a $\delta > 0$, depending only on the field K, such that for any $\eta \in \mathbb{I}_K$ with $||\eta|| > \delta$, there exists an $x \in K^*$ with $|x|_v \leq |\eta_v|_v$ for all v.*

Proof. For an infinite place v, let U_v denote the closed ball of center 0 and radius 1 in K_v. Also let

$$M = \prod_{v|\infty} U_v \prod_{v<\infty} \mathcal{O}_v \subseteq \mathbb{A}_K$$

M is a compact neighborhood of 0, so there exists another compact neighborhood V of 0 such that $V - V \subseteq M$, where $V - V$ is the set of all possible differences $v - v'$ (see the appendix on topological groups). Now K being discrete in $\mathbb{A}_K$, let λ be the counting measure on K. By the theorem mentioned in the section on Haar measures, it is possible to choose a Haar measure $\bar{\mu}$ on $\mathbb{A}_K/K$ such that for any measurable function $f : \mathbb{A}_K \to \mathbb{C}$

$$\int_{\mathbb{A}_K/K} \bar{f} d\bar{\mu} = \int_{\mathbb{A}_K} f d\mu$$

where

$$\bar{f}(\alpha + K) = \int_K f(\alpha + a) d\lambda(a) = \sum_{a\in K} f(\alpha + a)$$

Given this Haar measure, set

$$\delta = \frac{\bar{\mu}(\mathbb{A}_K/K)}{\mu(V)}$$

Remember that V and $\mathbb{A}_K/K$ are compact, so δ is finite and nonzero. We will prove the contrapositive of our theorem: suppose η is an idele, but there is no $x \in K^*$ with the property that $||x||_v \leq ||\eta_v||_v$ for each place v. We will show that $||\eta|| \leq \delta$.

Now $\eta M \cap K$ must be 0: for otherwise, there is a $\alpha \in \mathbb{I}_K, ||\alpha_v|| \leq 1$ for each place v, and there is an $x \in K^*$ such that $\eta\alpha = x$. Then $||\eta_v||_v = ||\alpha_v||^{-1}||x||_v \geq ||x||_v$, contrary to what we assumed about η.

Also, given any $\alpha \in \mathbb{A}_K$, there is at most one $a \in K$ such that $\alpha + a \in \eta V$. For if $\alpha + a_1 = \eta v_1$ and $\alpha + a_2 = \eta v_2$ for $a_1, a_2 \in K$ and $v_1, v_2 \in V$, then

$$a_2 - a_1 = (\alpha + a_1) - (\alpha + a_2) = \eta(v_1 - v_2) \in \eta(V - V) \cap K \subseteq \eta M \cap K = 0$$

which implies $a_1 = a_2$. If we set $f : \mathbb{A}_K \to \mathbb{C}$ to be the characteristic function of ηV, this shows that $\bar{f} \leq 1$, where $\bar{f}$ is as we defined it above. Thus

$$||\eta||\mu(V) = \mu(\alpha V) = \int\limits_{\mathbb{A}_K} f d\mu = \int\limits_{\mathbb{A}_K/K} \bar{f} d\bar{\mu} \leq \int\limits_{\mathbb{A}_K/K} d\bar{\mu} = \bar{\mu}(\mathbb{A}_K/K)$$

so $||\eta|| \leq \delta$, as required. □

Proposition 17. *$\mathbb{I}_K^1/K^*$ is compact, and so is $\mathbb{I}_K^{S,1}/K_S$ for any S containing the infinite places.*

Proof. The second statement follows from the first because $\mathbb{I}_K^{S,1}/K_S$ is homeomorphic to a closed subset of $\mathbb{I}_K^1/K^*$.

Take δ as in the previous lemma, and fix an idele η for which $||\eta|| > \delta$. Let

$$W = \prod_v \{x \in K_v : ||x||_v \leq ||\eta_v||_v\}$$

Then W is a compact subset of $\mathbb{A}_K$, hence a compact subset of $\mathbb{I}_K$ by (?). Therefore $W \cap \mathbb{I}_K^1$ is compact, as a closed subset of a compact space. It is enough to show that the quotient map

$$W \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^*$$

is surjective. In other words, given $\alpha in \mathbb{I}_K^1$, find an $x \in K^*$ such that $\alpha x \in W$. Since $||\eta|| > \delta$, so is $||\alpha^{-1}\eta||$. The Minkowski-Chevalley-Weil lemma says there is an $x \in K^*$ for which $||x||_v \leq ||\alpha_v^{-1}\eta_v||_v$ for all v, which is exactly what we need. □

Theorem 18. *(Strong approximation theorem) Let v_0 be a place. Given a finite set of places S not containing v_0, elements $a_v \in K_v : v \in S$, and $\epsilon > 0$, there exists an $x \in K$ such that $||a_i - x||_v < \epsilon$ for $v \in S$ and $||x||_v \leq 1$ for $v \notin S$ and $v \neq v_0$.*

Proof. By Corollary (?), there is a sequence of positive integers δ_v, with $\delta_v = 1$ for almost all v, such that $\mathbb{A}_K = W + K$, where

$$W = \prod_v \{x \in K_v : ||x||_v \leq \delta_v\}$$

Let η be an idele for which $0 < ||\eta_v||_v < \delta_v^{-1}\epsilon$ for $v \in S$, $||\eta_v||_v < \delta_v^{-1}$ for $v \notin S$ and $v \neq v_0$

(remember that $\delta_v^{-1} = 1$ for almost all v), and $||\eta_{v_0}||_{v_0}$ is very large. As long as $||\eta_{v_0}||_{v_0}$ is large enough, the norm $||\eta||$ will be greater than the number δ described in the Minkowski-Chevalley-Weil lemma. So there will exist a $\lambda \in K^*$ such that $||\lambda||_v \leq ||\eta_v||_v$ for all v.

Now let α be an adele for which $\alpha_v = a_v$ for $v \in S$, and $\alpha_v = 0$ for $v \notin S$. We can write $\alpha\lambda^{-1}$ as $\beta + b$ for $\beta \in W$ and $b \in K$. We claim that $x := \lambda b$ does what is required. For $v \in S$:

$$||a_v - x||_v = ||\alpha_v - x||_v = ||\lambda\beta_v||_v \leq ||\lambda||_v \delta_v < (\delta_v^{-1}\epsilon)\delta_v = \epsilon$$

and for $v \notin S, v \neq v_0$:

$$||x||_v = ||\lambda\beta_v||_v \leq ||\lambda||_v \delta_v \leq \delta_v^{-1}\delta_v = 1$$

□

1.4 The Unit Theorem

The Dirichlet unit theorem is a classical result which describes the structure of the group K_S. The hardest part of the unit theorem involves calculating the rank of a certain lattice. The compactness of $\mathbb{I}_K^{S,1}/K_S$ is actually equivalent to the determination of this rank (some treatments of algebraic number theory, e.g. by Neukirch, determine the rank first and use it to deduce compactness).

The proof of the unit theorem will rely on the following idea: if V is a vector space over $\mathbb{R}$, and G is an additive subgroup of V, then G and V are topological groups with respect to addition. We will be interested in looking at the *subspace* W generated by G, and in particular the vector space (and topological group with respect to addition) V/W.

Let $S = \{v_1, ..., v_s\}$ be a finite set of places containing all the infinite ones, and assume v_s is infinite. Take the vector space $\mathbb{R}^s$ in the product topology, so it is a topological group with respect to addition. Let

$$H = \{(x_1, ..., x_s) \in \mathbb{R}^s : x_1 + \cdots + x_s = 0\}$$

Then H is an $(s-1)$-dimensional subspace of V: it has as a basis $e_1 - e_n, e_2 - e_n, ..., e_{n-1} - e_n$, where e_k is the vector whose ith coordinate is δ_{ik}. Now, define

$$\Phi : \mathbb{I}_K^{S,1} \to \mathbb{R}^s$$

by the formula

$$\Phi(x_1, ..., x_s) = (\log ||x_1||_{v_1}, ..., \log ||x_s||_{v_s})$$

By the product formula, it is clear that Φ maps $\mathbb{I}_K^{S,1}$ into H.

Lemma 19. *Φ is continuous. Also, the subspace (that is, the $\mathbb{R}$-vector space) spanned by the image of Φ is all of H.*

Proof. A map into a product of topological spaces is continuous if the corresponding map into each component is continuous. In other words, we need to show that the mapping $(x_1, ..., x_s) \mapsto \log ||x_i||_{v_i}$ is continuous for each i. But we already know this to be the case. Thus Φ is continuous.

We already remarked that the image of Φ is contained in H, so all we have to do is find $s-1$ linearly independent vectors in the image of Φ. Let $x \in K^*_{v_1}$ be any element for which $||x||_{v_1} \neq 1$. Since v_s is archimedean, we can find a $y \in K^*_{v_s}$ for which $||y||_{v_s} = ||x||^{-1}_{v_1}$. Then

$$(x, 1, ..., y) \in \mathbb{I}_K^{S,1}$$

and this element is mapped by Φ to

$$(\log ||x||_{v_1}, 0, ..., 0, -\log ||x||_{v_1})$$

This is just a scale of the basis vector $e_1 - e_n$ we mentioned earlier. Similarly we can find scales of the vectors $e_2 - e_n, e_3 - e_n$ etc.in the image of Φ.

□

Proposition 20. *The image of K_S under Φ is a lattice, and the kernel of K_S is the set of all roots of unity in K.*

Proof. We first make the following claim: if $N, n \geq 1$, there are only finitely many algebraic integers x for which:

- The minimal polynomial of x over $\mathbb{Q}$ has degree $\leq n$.
- $|\sigma(x)| \leq N$ for all embeddings of K into $\mathbb{C}$.

For if x is such an algebraic integer, and μ is its minimal polynomial of degree, say, $t \leq n$, then the coefficients of μ, being symmetric functions of $\sigma(x)$, will also be bounded in terms of N. For example, the next to leading coefficient of μ is the trace of x in $\mathbb{Q}(x)/\mathbb{Q}$, and this is bounded in absolute value by $t \cdot N \leq n \cdot N$.

Also, the coefficients of these minimal polynomials are rational integers. Thus there are only finitely many minimal polynomials to consider, hence only finitely many algebraic integers which satisfy the given description. This establishes the claim.

Remember that the canonical absolute values $|| \cdot ||_v$ induced by infinite places v are directly carried from the embeddings of K into $\mathbb{C}$.

Now to show that the image of K_S is a lattice, it suffices by (?) to show that if D is a bounded subset of $\mathbb{R}^s$, then $\Phi(K_S)$ intersects D at only finitely many points. We will actually show something stronger: that only finitely many points of K_S map into D. Since D is bounded, there exists an

$M > 0$ such that $|x_i| \leq M$ for all $(x_1, ..., x_s) \in D$. Now if $\Phi(x) \in D$ for some $x \in K_S$, then $\log ||x||_{v_i} \leq M$ for all i, and hence $||x||_{v_i} \leq e^M$. In particular this holds for the archimedean places, so we see there is an $N > 0$ such that $|\sigma(x)| \leq N$ for all embeddings $\sigma : K \to \mathbb{C}$.

And the minimal polynomials of the $x \in K_S$ have degree $\leq [K : \mathbb{Q}]$. By the claim at the beginning of the proof, there are only finitely many $x \in K_S$ for which $\Phi(x) \in D$. Thus $\Phi(K_S) \cap D$ is finite.

The last thing we have to show is that the kernel of Φ is the set of roots of unity in K. If $x \in \operatorname{Ker} K_S$, so is $x^2, x^3, ...$ and all of these powers lie in a bounded set, namely $\{(0, ..., 0)\}$. Hence there are only finitely many distinct powers of x, giving us $x^i = x^j$ for $i < j$, hence $x^{j-i} = 1$. Conversely if x is a root of unity, then $x^m = 1$ for some $m \geq 1$. Then

$$(0, ..., 0) = \Phi(x^m) = m \cdot \Phi(x)$$

which implies $\Phi(x) = (0, ..., 0)$.

□

So the image of K_S is a lattice which is contained in a space of dimension $s - 1$. To complete the proof of the unit theorem, we need to show that this lattice has rank exactly $s - 1$. Here we give a slick proof which uses the compactness of $\mathbb{I}_K^{S,1}/K_S$.

Theorem 21. *The rank of the image of K_S is $s - 1$.*

Proof. Let W be the subspace spanned by the image of K_S. Then the rank of this image is the dimension of W. Since $W \subseteq H$, the dimension of W is $\leq s - 1$, and equality of dimensions is equivalent to saying that $W = H$. We have by composition a topological group homomorphism

$$f : \mathbb{I}_K^{S,1} \xrightarrow{\Phi} H \to H/W$$

whose kernel contains K_S. By the universal mapping property, there is an induced topological group homomorphism

$$\bar{f} : \mathbb{I}_K^{S,1}/K_S \to H/W$$

Now, suppose by way of contradiction that W is a proper subset of H. Then f, and hence $\bar{f}$, cannot be the zero mapping: this would assert that every vector $\Phi(x), x \in \mathbb{I}_K^{S,1}$ is a linear combination of elements in ΦK_S, and hence every element in H is a linear combination of elements of ΦK_S (for H is equal to the span of the image of Φ). Thus f being the zero mapping implies $W = H$.

Now H/W can be identified (as topological groups) with $\mathbb{R}^k$ for some $k \geq 1$. Since $\bar{f}$ is not the zero mapping, and $\mathbb{I}_K^{S,1}/K_S$ is compact, the image of $\bar{f}$ must be a nontrivial compact subgroup of

H/W. But there are no nontrivial compact subgroups of $\mathbb{R}^k$. We have reached a contradiction, so we must have $W = H$.

□

Corollary 22. *K_S modulo the roots of unity in K is a free abelian group of rank $s-1$. Hence there exist elements $c_1, ..., c_{s-1} \in K_S$ such that every element of K_S can be uniquely expressed as*

$$\zeta c_1^{n_1} \cdots c_{s-1}^{n_{s-1}}$$

where n_i are integers and ζ is a root of unity.

This corollary also describes the structure of the units of K, since $K_S = \mathcal{O}_K^*$ when S consists only of infinite places.

Corollary 23. *Suppose K contains all the nth roots of unity, and S contains s elements. Then $[K_S : K_S^n] = n^s$, where K_S^n is the group of $x^n : x \in K$.*

Proof. If C is a finite cyclic group with order divisible by n, then C/nC has exactly n elements. If T is free abelian of rank k, then T/nT is isomorphic to $\bigoplus_{i=1}^{k} \mathbb{Z}/n\mathbb{Z}$, and hence has k^n elements.

Now take C and T as multiplicative abelian groups: C is the group of roots of unity in K, and T is free abelian of rank $s-1$. The previous corollary tells us that $K_S = C \oplus T$ as an internal direct sum.

□

1.5 More on C_K

Define a map $(0, \infty) \to \prod_{v|\infty} K_v^* \prod_{v<\infty} \{1\}$ by the formula

$$\rho \mapsto a_\rho := (\sqrt[n]{\rho}, ..., \sqrt[n]{\rho}, 1, 1, ...)$$

where $n = [K : \mathbb{Q}]$. Since $||a_\rho||_v = \rho^{\frac{2}{n}}$ when v is complex, it is easy to see that $||a_\rho|| = \rho$. This map is continuous (continuous into each component), and the codomain inherits its topology from $\mathbb{I}_K^{S_\infty}$, hence from $\mathbb{I}_K$. We have by composition a continuous function $(0, \infty) \to C_K$.

Proposition 24. *The map*

$$C_K^1 \times (0, \infty) \to C_K$$

$$(\alpha K^*, \rho) \mapsto \alpha a_\rho K^*$$

is a topological group isomorphism.

Proof. Let us first establish the algebraic properties. Obviously this map is a homomorphism. To show injectivity, suppose that $\alpha a_\rho \in K^*$. Then $1 = ||\alpha a_\rho|| = \rho$, hence $a_\rho = 1$. But then $\alpha \in K^*$. For surjectivity, βK^* is mapped to by $(\beta\rho^{-1}_{||\beta||}K^*, ||\beta||)$.

The given map is continuous, as a product of continuous functions. The inverse mapping is given as we mentioned by the formula

$$\beta K^* \mapsto (\beta\rho^{-1}_{||\beta||}K^*, ||\beta||)$$

Since the inverse maps C_K into a product, we just have to show the mapping into each component is continuous. But this is just as clear.

□

2 Towards the first inequality

2.1 L-function and convergence theorem

Let $\mathbb{I}_K$ denote the idele group of the the number field K, d^*x denote the normalized Haar measure on $\mathbb{I}_K$, a continuous character on $\mathbb{I}_K$ is a continuous function $\chi : \mathbb{I}_K \longrightarrow \mathbb{C}^1$, such that $\chi(xy) = \chi(x)\chi(y)$, for $\forall x, y \in \mathbb{I}_K$

An **Adelic Bruhat-Schwartz function** is a finite linear combination of functions of the form $f_\infty \otimes f_0$, where $f_\infty \in C_c^\infty(\mathbb{A}_\infty)$, $\mathbb{A}_\infty = \prod_{v|\infty} K_v$, (here a function is smooth is in the usual sense that it is infinitely differentiable), $f_0 \in C_c^\infty(\mathbb{A}_0)$, $\mathbb{A}_0 = \prod_{v<\infty}{}' K_v$, the restricted direct product, meaning $K_v = O_v$ for almost all finite places v. where $f_0 = \otimes_{v<\infty} f_{0_v}$, $f_{0_v} \in C_c^\infty(K_v)$, meaning compactly supported and locally constant, and $f_{o_v} = 1_{O_v}$ for almost all v. We note such a function by $f \in C_c^\infty(\mathbb{A}_K)$.

Lemma 1. ('No Small Subgroup Argument'). *There exists an open neighborhood U of 1 in $\mathbb{C}$, which contains no non-trivial subgroup of $\mathbb{C}^*$.*

Proof. The existence of such U is guaranteed since otherwise suppose some non-trivial $e^{i\theta} \in U$, then if U contains a non-trivial subgroup that contains $e^{i\theta}$, then $e^{in\theta} \in U$ for all natural numbers n, this is impossible if we pick U small enough. □

By the 'No Small Subgroup Argument', $Ker(\chi)$ is open in $\mathbb{I}_K$, since $\chi(\mathbb{I}_K) \cap U = \{1\}$, therefore $Ker(\chi) = \chi^{-1}(U)$ if we pick U to be an open neighborhood of $1 \in \mathbb{C}$ which contains no non-trivial subgroup. Moreover, we have $\chi^{-1}(U) \supset \prod_{v\in S} U_v \times \prod_{v\notin S} O_v^*$, for some S a finite set of places, since such sets form a basis of open sets in $\mathbb{I}_K$. This implies $\chi_v(O_v^*) = 1$ for $\forall v \notin S$, where χ_v is the character of K_v^* induced by the imbedding $K_v^* \simeq (1, \cdots, 1, K_v^*, 1, \cdots, 1) \subset \mathbb{I}_K$. If $\chi_v|_{O_v^*} = 1$, we say χ_v is **unramified** at v.

Let $S_1 = \{v < \infty | \ \forall v \notin S_1, \chi_v \ \ unramified, \ \ and \ \ f_v = 1_{O_v}\}$. Let

$$I_v(f_v, \chi_v) = \int_{K_v^*} f_v(x)\chi_v(x)|x|_v^s d^*x_v.$$

For any S, a finite set of places, $S \supset S_1$, define

$$L^S(s, f, \chi) = \int_{\mathbb{I}_K^S} f(x)\chi(x)\|x\|^s d^*x = \prod_{v|\infty} I_v(f_v, \chi_v) \prod_{v\in S-S_1} I_v(f_v, \chi_v) \prod_{v\in S_1} I_v(f_v, \chi_v).$$

Lemma 2. *Suppose χ_v is a continuous character on K_v^*, then $\chi_v = 1$ on some small open neighborhood of 1 in O_v^**

Proof. By 'No Small Subgroup Argument', there exists an open neighborhood U of $1 \in \mathbb{C}$, such that U contains no non-trivial subgroup of $\mathbb{C}^*$, then $\chi^{-1}(U)$ is an open neighborhood of 1 in K_v^*. Choose m large enough such that $1 + \mathfrak{p}_v^m \subset \chi^{-1}(U)$, then $\chi_v(1 + \mathfrak{p}_v^m) = 1$. The smallest such m is called the **conductor** of χ_v. □

For $v \in S_1$, without loss of generality(cover $supp(f_v)$ by open sets of the form $1+\mathfrak{p}_v^m$, we can write f_v as a finite linear combination of characteristic functions $1_{1+\mathfrak{p}_v^m}$), we may assume $f_v = 1_{1+\mathfrak{p}_v^m}$, then $I_v(f_v, \chi_v) = \int\limits_{1+\mathfrak{p}_v^m} d^*x_v = \mu_v(1 + \mathfrak{p}_v^m) < \infty$. This implies that $|\prod\limits_{v\in S_1} I_v(f_v, \chi_v)| < \infty$. Also there are only finitely many $v|\infty$, and for those places, since f_v is smooth and compactly supported, we also have $|\prod\limits_{v|\infty} I_v(f_v, \chi_v)| < \infty$.

Now we only care about

$$\prod_{v\in S-S_1} I_v(f_v, \chi_v).$$

Since now $f_v = 1_{O_v}$, we have

$$I_v(f_v, \chi_v) = \int\limits_{O_v} \chi_v(x)|x|_v^s d^*x_v.$$

Write $O_v = \amalg_{n\geq 0}(\mathfrak{p}_v^n - \mathfrak{p}_v^{n+1})$, then

$$I_v(f_v, \chi_v) = \sum_{n\geq 0} \int\limits_{\varepsilon\in O_v^*} \chi_v(\varepsilon\pi_v^n)|\pi_v|_v^{ns} d^*x_v = \sum_{n\geq 0} \int\limits_{O_v^*} \chi_v(\pi_v^n)|\pi_v|_v^{ns} d^*x_v$$

$$= \sum_{n\geq 0} \chi_v(\pi_v^n) q_v^{-ns} \int\limits_{O_v^*} d^*x_v = \sum_{n\geq 0} \chi_v(\pi_v)^n q_v^{-ns} = \frac{1}{1 - \chi_v(\pi_v)q_v^{-s}}.$$

We conclude that

$$\prod_{v\in S-S_1} I_v(f_v, \chi_v) = \prod_{v\in S-S_1} (1 - \chi_v(\pi_v)q_v^{-s})^{-1}.$$

Note that

$$|\frac{\chi_v(\pi_v)}{q_v^s}| \leq \frac{1}{q_v^\sigma} < 1,$$

for $\sigma \geq 1$, we have

$$\prod_{v\in S-S_1} (1 - \chi_v(\pi_v)q_v^{-s})^{-1} = exp(\sum_{v\in S-S_1} \sum_{m\geq 1} \frac{\chi_v(\pi_v)^m}{mq_v^{ms}}).$$

Here we use the fact that

$$\frac{1}{1-z} = exp(-\sum_{m\geq 1} \frac{z^m}{m}),$$

when $|z| < 1$.

Lemma 3.

$$\sum_{v \notin S_1} \sum_{m \geq 1} \frac{1}{m q_v^{ms}}$$

converges for $Re(s) > 1$.

Proof.

$$T = \sum_{v \notin S_1} \sum_{m \geq 1} \frac{1}{m q_v^{ms}} = \sum_{v \notin S_1} (\frac{1}{q_v^s} + \sum_{m \geq 2} \frac{1}{m q_v^{ms}}),$$

therefore

$$|T| \leq \sum_{v \notin S_1} (\frac{1}{q_v^\sigma} + \sum_{m \geq 2} \frac{1}{m q_v^{m\sigma}})$$

$$\leq n \sum_p \frac{1}{p^\sigma} + n \sum_p (\frac{1}{2p^{2\sigma}} + \frac{1}{3p^{3\sigma}} + \cdots)$$

$$\leq n \sum_p \frac{1}{p^\sigma} + n \sum_p (\frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + \cdots)$$

$$\leq n \sum_p \frac{1}{p^\sigma} + n \sum_p p^{-2\sigma} \frac{1}{1 - p^\sigma}$$

$$\leq \sum_p \frac{1}{p^\sigma} + \frac{n}{1 - 2^{-\sigma}} \sum_p \frac{1}{p^{2\sigma}}.$$

Here $\sigma = Re(s)$, $n =$ the number of imbeddings from the number field K to $\mathbb{C}$. Note that the first sum on the right hand side converges for $\sigma > 1$, the second sum converges for $\sigma > \frac{1}{2}$ □

We conclude the above results as follows:

Theorem 4. *Let*

$$L_K(s, \chi) = \prod_{v \notin S_1} (1 - \chi_v(\pi_v) q_v^{-s})^{-1},$$

then we have the product $\prod_{v \notin S_1} (1 - \chi_v(\pi_v) q_v^{-s})^{-1}$ *converges for* $Re(s) > 1$, *and thus* $L_K(s, \chi)$ *defines a holomorphic function for* $Re(s) > 1$. *Moreover, we can write*

$$L_K(s, \chi) = exp(\sum_{v \notin S_1} \chi_v(\pi_v) q_v^{-s}) \cdot exp(g_0(s, \chi)),$$

where $g_0(s, \chi)$ *is a holomorphic function for* $Re(s) > \frac{1}{2}$.

Proof.

$$\prod_{v\in S-S_1}(1-\chi_v(\pi_v)q_v^{-s})^{-1}=exp(\sum_{v\in S-S_1}\sum_{m\geq 1}\frac{\chi_v(\pi_v)^m}{mq_v^{ms}})$$

$$=exp(\sum_{v\in S-S_1}\frac{\chi_v(\pi_v)}{q_v^s})\cdot exp(\sum_{v\in S-S_1}\sum_{m\geq 2}\frac{\chi_v(\pi_v)^m}{mq_v^{ms}}),$$

order the finite sets of places S which contains S_1 by inclusion, let S goes to infinity, we have

$$L_K(s,\chi)=\prod_{v\notin S_1}(1-\chi_v(\pi_v)q_v^{-s})^{-1}=exp(\sum_{v\notin S_1}\sum_{m\geq 1}\frac{\chi_v(\pi_v)^m}{mq_v^{ms}})$$

$$=exp(\sum_{v\notin S_1}\frac{\chi_v(\pi_v)}{q_v^s})\cdot exp(\sum_{v\notin S_1}\sum_{m\geq 2}\frac{\chi_v(\pi_v)^m}{mq_v^{ms}})=exp(\sum_{v\notin S_1}\frac{\chi_v(\pi_v)}{q_v^s})\cdot exp(g_0(s,\chi)),$$

where

$$g_0(s,\chi)=\sum_{v\notin S_1}\sum_{m\geq 2}\frac{\chi_v(\pi_v)^m}{mq_v^{ms}}.$$

The claimed convergence is guaranteed by the above lemma. □

Theorem 5.

$$L(s,f,\chi)=\int_{\mathbb{I}_K}f(x)\chi(x)\|x\|^s d^*x$$

converges for $Re(s)>1$, and therefore defines a holomorphic function on $\{s\in\mathbb{C}|Re(s)>1\}$.

Proof. The partial L-function

$$L^S(s,f,\chi)=\int_{\mathbb{I}_K^S}f(x)\chi(x)\|x\|^s d^*x$$

$$=\prod_{v|\infty}I_v(f_v,\chi_v)\prod_{v\in S-S_1}I_v(f_v,\chi_v)\prod_{v\in S_1}I_v(f_v,\chi_v),$$

We showed that both $\prod_{v|\infty}I_v(f_v,\chi_v)$ and $\prod_{v\in S_1}I_v(f_v,\chi_v)$ have finite absolute value. Moreover,

$$\lim_S\prod_{v\in S-S_1}I_v(f_v,\chi_v)=L(s,\chi).$$

Therefore there exists a constant $M>0$, depending only on $\prod_{v|\infty}I_v(f_v,\chi_v)$ and $\prod_{v\in S_1}I_v(f_v,\chi_v)$, such that

$$|L^S(s,f,\chi)|\leq M\cdot|\prod_{v\in S-S_1}I_v(f_v,\chi_v)|.$$

Then taking limits on both sides, we have

$$\lim_S |L^S(s,f,\chi)| \leq M \cdot |L_K(s,\chi)|.$$

Since $L(s,\chi)$ is holomorphic for $Re(s) > 1$ by Theorem 1, we have $|L^S(s,f,\chi)| < \infty$ for $Re(s) > 1$, and $\forall S \supset S_1$, the bound does not depend on S. By monotone convergence theorem,

$$L(s,f,\chi) = \int_{\mathbb{I}_K} f(x)\chi(x)\|x\|^s d^*x = \lim_S \int_{\mathbb{I}_K^S} f(x)\chi(x)\|x\|^s d^*x$$

exists for $Re(s) > 1$. Thus $L(s,f,\chi)$ is holomorphic when $Re(s) > 1$. □

2.2 Analytic continuation of L-function

A function $F : \mathbb{A}_K \to \mathbb{C}$ is **factorizable** if there exists local functions $F_v : K_v \to \mathbb{C}(\forall v \leq \infty)$, where $F_v = 1_{O_v}$ for almost all $v \leq \infty$. such that we can write F as a product $F(x) = \prod_v F_v(x_v)$ for all $x \in \mathbb{A}_K$.

Let $f \in C_c^\infty(\mathbb{A}_K)$ be an Adelic Bruhat-Schwartz function, F is a bounded factorizable function on $\mathbb{A}_K$, define $L(s,f,F) = \int_{\mathbb{I}_K} f(x)F(x)\|x\|^s d^*x$. Note that the integral converges for $Re(s) > 1$(since F is bounded, using the same argument as before). We say F is **automorphic** if $F(x\xi) = F(\xi x) = F(x)$, for $\forall \xi \in K^*, x \in \mathbb{I}_K$. Then if F is automorphic, F can be regarded as a function on $\mathbb{I}_K/K^*$.

Proposition 6. $\mathbb{I}_K/K^* \simeq \mathbb{I}_K^1/K^* \times \mathbb{R}_+^*$

Proof. Note that $\mathbb{I}_K \simeq \mathbb{I}_K^1 \cdot \mathbb{R}_+^*$, which sends α to $\alpha^1 \cdot \tilde{t}$, where $\tilde{t} = (1, \cdots, 1, t^{1/n}, \cdots, t^{1/n}) \in \mathbb{I}_K, t = \|\alpha\| = \prod_v |\alpha_v|_v, \alpha^1 = \frac{\alpha}{\|\alpha\|}$. Let $\Phi : \mathbb{I}_K/K^* \to \mathbb{I}_K^1/K^* \times \mathbb{R}_+^*$ be defined as $\Phi(\bar{\alpha}) = (\bar{\alpha^1}, t)$, if $\alpha = \alpha^1 \cdot \tilde{t}$.

First, Φ is well-defined: if $\bar{\alpha} = \bar{\beta}$, then $\alpha = \beta \cdot \xi$, for some $\xi \in K^*$. $\Rightarrow t = \|\alpha\| = \|\beta \cdot \xi\| = \|\beta\| \cdot \|\xi\| = \|\beta\|$, by product formula.$\Rightarrow \alpha^1 = \frac{\alpha}{\|\alpha\|} = \frac{\beta \cdot \xi}{\|\beta\|} \Rightarrow \bar{\alpha^1} = \frac{\bar{\beta \cdot \xi}}{\|\beta\|} = \bar{\beta^1} \Rightarrow (\bar{\alpha^1}, t) = (\bar{\beta^1}, t) \Rightarrow \Phi(\bar{\alpha}) = \Phi(\bar{\beta})$.

Second, Φ is injective: if $(\bar{\alpha^1}, t) = (\bar{\beta^1}, t)$, write $\beta = \beta^1 \cdot \tilde{s}$, then $t = s, \bar{\alpha^1} = \bar{\beta^1} \Rightarrow t = s, \alpha^1 \cdot \beta^{1^{-1}} \in K^* \Rightarrow \alpha\beta^{-1} = (\alpha^1\tilde{t})(\beta^1\tilde{s})^{-1} = (\alpha^1\beta^{1^{-1}})(\tilde{t}\tilde{s})^{-1} = (\alpha^1\beta^{1^{-1}}) \in K^* \Rightarrow \bar{\alpha} = \bar{\beta}$.

Next, Φ is surjective: take $(\bar{\alpha^1}, t) \in \mathbb{I}_K^1/K^* \times \mathbb{R}_+^*$, let $\alpha = \alpha^1 \cdot \tilde{t}$, then $\Phi(\bar{\alpha}) = (\bar{\alpha^1}, t)$.

Finally, since Φ is obviously a homomorphism of abelian groups, and both Φ and Φ^{-1} are continuous, we see that Φ is an isomorphism of locally compact abelian groups. □

Lemma 7. *Let G be a locally compact abelian group, Γ be a discrete subgroup of G, d^*x denotes the Haar measure on G, then there exists a unique Haar measure d_0^*x on the quotient group G/Γ, such that $\int_G f(x)d^*x = \int_{G/\Gamma} \sum_{\gamma \in \Gamma} f(x\gamma)d_0^*x$*

Proof. We write $f_\Gamma(x) = \sum_{\gamma\in\Gamma} f(x\gamma) = \int_\Gamma f(x\gamma)d\mu_\Gamma$, where $d\mu_\Gamma$ is the Haar measure on Γ, since Γ is discrete, one can see that up to a scalar, it is the counting measure on Γ. This is why the last integral above is the same as the sum. Moreover, if $x, y \in U$, U compact, then

$$|f_\Gamma(x) - f_\Gamma(y)| = |\int_\Gamma f(x\gamma) - f(y\gamma)d\mu_\Gamma| \leq \mu_\Gamma(\Gamma \cap U^{-1}K) \sup_\gamma |f(x\gamma - y\gamma)|.$$

where $K = supp(f)$. Since f is continuous on a compact set, therefore uniformly continuous. This shows that f_Γ is continuous. It is easy to see that f_Γ is left(right) Γ-invariant, so it defines a continuous function $\bar{f}$ on the quotient group G/Γ, such that $\bar{f}(x\Gamma) = f_\Gamma(x)$. Let $q : G \to G/\Gamma$ be the quotient map, then since f is supported on K, $\bar{f}$ is supported on $q(K)$. So $\bar{f} \in C_c(G/\Gamma)$. Since G is a locally compact abelian group, G/Γ is also locally compact, therefore there exist a unique Haar measure(up to scalar) d_0^*x on G/Γ. Let $\lambda : C_c(G) \to \mathbb{C}$ be a functional defined by

$$\lambda(f) = \int_{G/\Gamma} \bar{f} d_0^* x$$

This linear funtional is positive, i.e. if $f \geq 0$, then $\lambda(f) \geq 0$. By Riesz representation theory, there is a regular Borel measure μ_G on G such that

$$\lambda(f) = \int_G f d\mu_G$$

It is easy to check that this μ_G is left(right) invariant, so it is a Haar measure, therefore it is d^*x multiplying by a scalar. Replace d_0^*x by a scalar multiple of it in the beginning if necessary, without loss of generality, we have

$$\lambda(f) = \int_G f d^* x.$$

Therefore we obtain

$$\int_G f d^* x = \int_{G/\Gamma} \bar{f} d_0^* x = \int_{G/\Gamma} \sum_{\gamma\in\Gamma} f(x\gamma) d_0^* x.$$

□

Theorem 8. *Let F be a bounded automorphic factorizable function on $\mathbb{I}_K$, $f \in C_c^\infty(\mathbb{A}_K)$ be an Adelic Bruhat-Schwartz function. Then $L(s, f, F)$ has a meromorphic continuation to $\{s \in \mathbb{C} | Re(s) > 0\}$, with only simple pole at $s = 1$.*

Proof. First we know for $Re(s) > 1$, the integral defining $L(s, f, F)$ converges absolutely, since F

is bounded. Moreover, by lemma 7,

$$L(s,f,F)=\int\limits_{\mathbb{I}_K} f(x)F(x)\|x\|^s d^*x=\int\limits_{\mathbb{I}_K/K^*} F(x)(\sum_{\xi\in K^*} f(x\xi))\|x\|^s d_0^*x,$$

where d_0^*x is the unique Haar measure on $\mathbb{I}_K/K^*$ such that the formula works. Since $\mathbb{I}_K/K^*\simeq \mathbb{I}_K^1/K^*\times\mathbb{R}_+^*$ as locally compact groups. Let dx^1 be the Haar measure on $\mathbb{I}_K/K^*$, $d^*t=\frac{dt}{t}$ be the Haar measure on $\mathbb{R}_+^*$. Through the isomorphism Φ in the above proposition, and by uniqueness theorem of Haar measure on locally compact groups, we may identify $d_0^*x=dx^1\cdot d^*t$. Then

$$L(s,f,F)=\int\limits_{\mathbb{I}_K/K^*} F(x)(\sum_{\xi\in K^*} f(x\xi))\|x\|^s d_0^*x$$

$$=\int_0^\infty t^s\int\limits_{\mathbb{I}_K^1/K^*} F(x^1\tilde{t})\sum_{\xi\in K^*} f(x^1\tilde{t}\xi)dx^1\frac{dt}{t}=(1)+(2),$$

where

$$(1)=\int_0^1 t^s\int\limits_{\mathbb{I}_K^1/K^*} F(x^1\tilde{t})\sum_{\xi\in K^*} f(x^1\tilde{t}\xi)dx^1\frac{dt}{t}$$

,

$$(2)=\int_1^\infty t^s\int\limits_{\mathbb{I}_K^1/K^*} F(x^1\tilde{t})\sum_{\xi\in K^*} f(x^1\tilde{t}\xi)dx^1\frac{dt}{t},$$

here $\mathbb{I}_K^1=\{x\in\mathbb{I}_K|\|x\|=1\}$, we write $x=x^1\cdot\tilde{t}$ via the isomorphism in the above proposition.

$$(2)=\int_1^\infty t^s\int\limits_{\mathbb{I}_K^1/K^*} F(x^1\tilde{t})\sum_{\xi\in K^*} f(x^1\tilde{t}\xi)dx^1\frac{dt}{t}=\int\limits_{\{x\in\mathbb{I}_K|\|x\|\geq 1\}} f(x)F(x)\|x\|^s d^*x.$$

For $\sigma_1\geq\sigma_2$, we have

$$\int\limits_{\{x\in\mathbb{I}_K|\|x\|\geq 1\}} |f(x)|\cdot|F(x)|\|x\|_1^\sigma d^*x\geq\int\limits_{\{x\in\mathbb{I}_K|\|x\|\geq 1\}} |f(x)|\cdot|F(x)|\|x\|_2^\sigma d^*x.$$

Since we already know

$$\int\limits_{\{x\in\mathbb{I}_K|\|x\|\geq 1\}} f(x)F(x)\|x\|^s d^*x$$

converges for $Re(s)>1$, this implies that (2) converges for $\forall s\in\mathbb{C}$.

$$(1) = \int_0^1 t^s \int\limits_{\mathbb{I}_K/K^*} F(x^1\tilde{t}) \sum_{\xi\in K^*} f(x^1\tilde{t}\xi)dx^1 \frac{dt}{t},$$

make the substitution $x \mapsto x^{-1}, t \mapsto t^{-1}, x^1 \mapsto (x^1)^{-1}$, we have

$$(1) = \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K/K^*} F((x^1)^{-1}\tilde{t}^{-1}) \sum_{\xi\in K^*} f((x^1)^{-1}\tilde{t}^{-1}\xi)dx^1 \frac{dt}{t}$$

$$= -f(0) \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1 \frac{dt}{t}$$

$$+ \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K/K^*} F((x^1)^{-1}\tilde{t}^{-1}) \sum_{\xi\in K} f((x^{-1}\xi)dx^1 \frac{dt}{t} \ldots\ldots (*)$$

To continue, we need

Theorem A. *Let $f \in C_c^\infty(\mathbb{A}_K)$ be an Adelic Bruhat-Schwartz function, dx be the Haar measure on $\mathbb{A}_K$, then there exists constants C_K, D_K, N_K, depending only on the number field K, such that for any given $x \in \mathbb{I}_K$, we have*

$$\sum_{\xi\in K} f(x\xi) = C_K\|x\|^{-1} \cdot \int\limits_{\mathbb{A}_K} f(y)dy + g(\|x\|),$$

where $|g(\|x\|)| \le D_K\|x\|^N$, for $\forall N \ge N_K$.

Proof. See later. □

By theorem A,we have

$$(*) = -f(0) \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1 \frac{dt}{t}$$

$$+ \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})(C_K \cdot t \int\limits_{\mathbb{A}_K} f(y)dy + g(t^{-1}))dx^1 \frac{dt}{t}$$

$$= -f(0) \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1 \frac{dt}{t}$$

$$+ \int_1^\infty t^{-s+1} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1 (C_K \int\limits_{\mathbb{A}_K} f(y)dy) \frac{dt}{t}$$

$$+\int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})g(t^{-1})dx^1\frac{dt}{t}$$

denote

$$(A) = -f(0)\int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1\frac{dt}{t},$$

$$(B) = \int_1^\infty t^{-s+1} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1(C_K \int\limits_{\mathbb{A}_K} f(y)dy)\frac{dt}{t},$$

$$(C) = \int_1^\infty t^{-s} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})g(t^{-1})dx^1\frac{dt}{t}$$

.

For (A), since F is bounded, and $\mathbb{I}_K^1/K^*$ is compact, there exists a constant $C > 0$, such that

$$|(A)| \leq C \cdot \int_1^\infty t^{-\sigma}\frac{dt}{t} = C \cdot \frac{t^{-\sigma}}{\sigma}|_1^\infty < \infty,$$

if $\sigma > 0$, here $\sigma = Re(s)$. Therefore, (A) converges for $Re(s) > 0$.

For (C), again since F is bounded, and $\mathbb{I}_K^1/K^*$ is compact, and by theorem A, there exists a constant C'_N such that

$$|(C)| \leq C'_N \int_1^\infty t^{-\sigma} \cdot t^{-N}\frac{dt}{t} = C'_N \int_1^\infty t^{-(\sigma+N+1)}dt = C'_N \frac{1}{-\sigma-N}t^{-\sigma-N}|_1^\infty < \infty$$

if $\sigma + N > 0$, i.e if $N > -\sigma$. Fix σ, we can choose N large enough such that $N > max\{-\sigma, N_K\}$. Then the desired estimate holds. Therefore (C) is converges for all $s \in \mathbb{C}$.

Now we just need to work on (B). As F is factorizable, we can write $F(x^1\tilde{t}) = F_0(x^1)F_+(t)$, where F_0 is a function on $\mathbb{I}_K^1/K^*$, F is a function on $\mathbb{R}_+^*$. Since F is bounded, both F_0 and F_+ are bounded.

Define

$$G(t) = \frac{F_+(t) - F_+(0)}{t}$$

Assume F_+ is right continuous and right differentiable at 0. Let $G(0) = F'_+(0), F_+(t) = tG(t) + F_+(0)$.

$$(B) = \int_1^\infty t^{-s+1} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1(C_K \int\limits_{\mathbb{A}_K} f(y)dy)\frac{dt}{t},$$

since $C_K \int\limits_{\mathbb{A}_K} f(y)dy$ is a constant, let's look at

$$\int_1^\infty t^{-s+1} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1 \frac{dt}{t}.$$

We have

$$\int_1^\infty t^{-s+1} \int\limits_{\mathbb{I}_K^1/K^*} F((x^1)^{-1}\tilde{t}^{-1})dx^1 \frac{dt}{t} = \int_1^\infty t^{-s+1} (\int\limits_{\mathbb{I}_K^1/K^*} F_0((x^1)^{-1})dx^1) F_+(t^{-1}) \frac{dt}{t}$$

$$= c \cdot \int_0^1 t^{s-1} F_+(t) \frac{dt}{t} = c \cdot (\int_0^1 t^{s-1} F_+(0) \frac{dt}{t} + \int_0^1 t^s G(t) \frac{dt}{t}),$$

where

$$c = \int\limits_{\mathbb{I}_K^1/K^*} F_0((x^1)^{-1})dx^1$$

is a constant. We claim that G is bounded near 0: Since by the assumption on F, $F_+(t)$ is right continuous at 0, so $F'_+(0)$ exists, $F_+(t)$ is right differentiable at 0, therefore $G(t)$ is right continuous at 0 and $G(0)$ exists. This implies that there exists $\epsilon > 0$, such that $G(t)$ is bounded for $\forall t \in [0, \epsilon)$. For $t \in [\epsilon, 1]$, note that $F_+(t)$ is bounded, so $G(t)$ is also bounded on $[\epsilon, 1]$, therefore $G(t)$ is bounded on $[0, 1]$.

This implies that

$$| \int_0^1 t^s G(t \frac{dt}{t})| \leq C' \cdot \int_0^1 t^{\sigma-1} dt = C' \frac{t^\sigma}{\sigma} |_0^1 < \infty,$$

if $\sigma > 0$. Therefore

$$(B) = c \cdot C_K \int\limits_{\mathbb{A}_K} f(y)dy \cdot (F_+(0) \frac{t^{s-1}}{s-1} |_0^1 + \int_0^1 t^s G(t) \frac{dt}{t})$$

converges for $Re(s) = \sigma > 0$, with only simple pole at $s = 1$, with residue

$$F_+(0) C_K \cdot \int\limits_{\mathbb{I}_K^1/K^*} F_0(x^1)dx^1 \int\limits_{\mathbb{A}_K} f(y)dy.$$

This proves the theorem. □

Recall

$$L(s, f, \chi) = \int\limits_{\mathbb{I}_K} f(x)\chi(x)\|x\|^s d^*x$$

defines a holomorphic function for $Re(s) > 1$. A continuous character χ on $\mathbb{I}_K/K^*$ is called a *grossëncharacter*. Applying theorem 8 to the case $F = \chi$, we obtain the **Analytic Continuation of L-function defined by a grossëncharacter**:

Theorem 9. *$L(s, f, \chi)$ defines a holomorphic function for $Re(s) > 1$, for $f \in C_c^\infty((A)_K)$, an Adelic Bruhat-Schwartz function, and $\chi : \mathbb{I}_K/K^* \to \mathbb{C}^1$, a continuous character. $L(s, f, \chi)$ can be extended to a meromorphic function on $Re(s) > 0$, with only simple pole at $s = 1$, with residue*

$$C_K \int_{\mathbb{A}_K} f(x)dx \int_{\mathbb{I}_K^1/K^*} \chi_0(x^1)dx^1.$$

Here C_K is a constant depending only on the number field K, $\chi = \chi_0 \cdot \chi_\infty$, χ_0 is a continuous character on $\mathbb{I}_K^1/K^*$ induced by χ.

Proof. It follows from theorem 8 immediately. We leave it to the reader to check that a *grossëncharacter* χ satisfies the assumptions on F in theorem 8. □

Now we prove theorem A.

We first reduce theorem A to a real-vector space case(theorem A', see later), then we prove theorem A' to complete the proof of theorem A.

Proof. $\mathbb{I}_K = \mathbb{I}_K^1 \cdot \mathbb{R}_+^*$, we can write $x = x^1 \cdot \tilde{t}$, where $\tilde{t} = (1, \cdots, 1, t^{\frac{1}{n}}, \cdots, t^{\frac{1}{n}}), t = \|x\|$. We need to show

$$\sum_{\xi \in K} f(x\tilde{t}\xi) = C_K t^{-1} \int_{\mathbb{A}_K} f(y)d\mu(y) + g(t)$$

(Here to be clear, we write the Haar measure on $\mathbb{A}_K$ as $d\mu(y)$).

Let $L_{x^1} f(y) = f(x^1 y), \forall y \in \mathbb{A}_K$, then we need to show

$$\sum_{\xi \in K} L_{x^1} f(\tilde{t}\xi) = C_K t^{-1} \int_{\mathbb{A}_K} f(y)d\mu(y) + g(t)$$

$$= C_K t^{-1} \int_{\mathbb{A}_K} f(x^1 y)d\mu(y) + g(t) = C_K t^{-1} \int_{\mathbb{A}_K} L_{x^1} f(y)d\mu(y) + g(t).$$

The second equality follows from that

$$\int_{\mathbb{A}_K} f(x^1 y)d\mu(y) = \int_{\mathbb{A}_K} f(u)d\mu(x^{1^{-1}}u) = \int_{\mathbb{A}_K} f(u)d\mu(u),$$

since the Haar measure $d\mu(x^{1^{-1}}u) = \|x^{1^{-1}}\|d\mu(u) = d\mu(u)$. Thus, replace f by $L_{x^1} f$ if necessary, we may assume f is a function on $\mathbb{R}_+^* \subset \mathbb{A}_K$.

Moreover, since $f \in C_c^\infty(\mathbb{A}_K)$, f is a finite linear combination of functions of the form $f_0 \otimes f_\infty$, where $f_0 = \otimes'_{v<\infty} f_v, f_v \in C_c(K_v)$, locally constant and of compact support, $f_v = 1_{O_v}$ for almost all v. The sum on the left hand side is a finite sum since K is discrete in $\mathbb{A}_K$, and f is of compact support. the right hand side is an integral, which is also linear in f. It follows that without loss of generality, it suffices to show the desired equality for functions of the form $f = \prod_{v\in S} 1_{x_v+\alpha_v} \prod_{v\notin S} 1_{O_v}$.

Using this f, the left hand side of the desired equality becomes

$$\sum_{\xi\in K} f(\tilde{t}\xi) = \sum_{\xi\in \prod_{v\in S}(x_v+\alpha_v) \prod_{v\notin S} O_v} f_\infty(\tilde{t}\xi_\infty),$$

here we write $\xi = (\xi, \cdots, \xi) = (\xi_0, \xi_\infty)$.

By strong approximation theorem, take the special place $v_0 = \infty$, we can find $\xi' \in K$, such that $|\xi'|_v \leq 1, \forall v \notin S; \xi' \equiv x_v (mod\ \alpha_v), \forall v \in S$.

Then

$$\sum_{\xi\in K} f(\tilde{t}\xi) = \sum_{\xi\in \prod_{v\in S}(x_v+\alpha_v) \prod_{v\notin S} O_v} f_\infty(\tilde{t}\xi_\infty) = \sum_{\xi-\xi'\in(\prod_{v\in S}\alpha_v \prod_{v\notin S} O_v)\cap K} f_\infty(\tilde{t}\xi_\infty) = \sum_{\xi-\xi'\in\alpha} f_\infty(\tilde{t}\xi_\infty).$$

Here $\alpha = (\prod_{v\in S}\alpha_v \prod_{v\notin S} O_v) \cap K$, a fractional ideal of K. Since each α_v is generated by some $\pi_v^{m_v}$ (since it is principal), multiply by $c = \prod_{v\in S} \pi_v^{m_v}$ for those $v \in S$, such that $m_v < 0$. Then $c\alpha \subset O_K$. Since O_K is a free $\mathbb{Z}$ module of rank n, so is α.

Let $V = K \otimes \mathbb{R} \simeq \oplus_{v|\infty} K_v$. V is a free $\mathbb{R}$ module of rank n. Therefore $V \simeq \mathbb{R}^n$ as $\mathbb{R}$ modules. So α is a lattice in V, and $V/\alpha \simeq \oplus_{i=1}^n (\mathbb{R}/\mathbb{Z}) \simeq (S^1)^n$ is compact.

The right hand side of the desired equation becomes

$$C_K t^{-1} \int_{\mathbb{A}_K} f(y)d\mu(y) + g(t) = C_K t^{-1} \prod_{v\in S} \mu_v(x_v + \alpha_v) \cdot \prod_{v\notin S} \mu_v(O_v) \int_{\mathbb{A}_\infty} f_\infty(y)d\mu_\infty(y) + g(t)$$

$$= C_K t^{-1} \prod_{v\in S} \mu_v(\alpha_v) \cdot \prod_{v\notin S} \mu_v(O_v) \int_{\mathbb{A}_\infty} f_\infty(y)d\mu_\infty(y) + g(t)$$

$$= C_K t^{-1} \prod_{v\in S} \frac{\mu_v(O_v)}{N_v(\alpha_v)} \prod_{v\notin S} \mu_v(O_v) \int_{\mathbb{A}_\infty} f_\infty(y)d\mu_\infty(y) + g(t)$$

$$= C_K t^{-1} \frac{1}{N_{K/\mathbb{Q}}(\alpha)} \int_{\mathbb{A}_\infty} f_\infty(y)d\mu_\infty(y) + g(t)$$

$$= C_K t^{-1} \frac{1}{Vol(V/\alpha)} \int\limits_{\mathbb{A}_\infty} f_\infty(y) d\mu_\infty(y) + g(t)$$

$$= C_K t^{-1} \frac{1}{Vol(V/\alpha)} \int\limits_{V} f_\infty(y) d\mu_\infty(y) + g(t)$$

here $N_v(\cdot)$ is the local norm at v, $N_{K/\mathbb{Q}}(\cdot)$ is the global norm from K to $\mathbb{Q}$. Also note that $Vol(V/\alpha) = 2^{-r_2}\mathcal{D}_{K/\mathbb{Q}}^{1/2} N_{K/\mathbb{Q}}(\alpha)$, r_2 is the number of imbeddings from K to $\mathbb{C}$, $\mathcal{D}_{K/\mathbb{Q}}$ is the discriminant. $\mathbb{A}_\infty = \prod\limits_{v|\infty} K_v \simeq K \otimes_{\mathbb{Q}} \mathbb{R} \simeq V$.

Therefore it suffices to show that

$$\sum_{\xi - \xi' \in \alpha} f_\infty(\tilde{t}\xi_\infty) = C_K t^{-1} \frac{1}{Vol(V/\alpha)} \int\limits_{V} f_\infty(y) d\mu_\infty(y) + g(t)$$

Let $\lambda = \xi - \xi'$, we obtain

$$\sum_{\lambda \in \alpha} f_\infty(\tilde{t}\xi' + \tilde{t}\lambda) = C_K t^{-1} \frac{1}{Vol(V/\alpha)} \int\limits_{V} f_\infty(y) d\mu_\infty(y) + g(t)$$

Let $T_{\tilde{t}\xi'} f_\infty(y) = f_\infty(\tilde{t}\xi' + y), \forall y \in V$, the desired equation becomes

$$\sum_{\lambda \in \alpha} T_{\tilde{t}\xi'} f_\infty(\tilde{t}\lambda) = C_K t^{-1} \frac{1}{Vol(V/\alpha)} \int\limits_{\mathbb{A}_K} f_\infty(y) d\mu_\infty(y) + g(t)$$

$$= C_K t^{-1} \frac{1}{Vol(V/\alpha)} \int\limits_{\mathbb{A}_K} T_{\tilde{t}\xi'} f_\infty(y) d\mu_\infty(y) + g(t),$$

by the left invariance of Haar measure. Replace $T_{\tilde{t}\xi'} f_\infty$ by f_∞ if necessary. Write f instead of f_∞, f is then a function on V, a real vector space. Since now f is a function of t, we may write t instead of $\tilde{t}$. Then we have reduced the original equation to the case in a real vector space. It suffices to show the following result to complete the proof of theorem A. □

Theorem A'. *Let V be an n-dimensional $\mathbb{R}$ vector space, L a lattice in V, with V/L compact. Given $f \in C_c^\infty(V)$, then we have*

$$\sum_{\lambda \in L} f(t\lambda) = C_K t^{-n} \frac{1}{Vol(V/L)} \int\limits_{V} f(x) dx + g(t),$$

$|g(t)| \leq C_K t^N$, for $\forall t > 0, \forall N \geq N_K$, where C_K, D_K, N_K are constants depending only on V.

Proof. In order to prove theorem A', we need some preparations:

First, let's introduce some background of Fourier analysis on a real vector space.

Let V, L be as in theorem A'. Let B be a symmetric non-degenerate bilinear form on V. Let $L^* = \{\eta \in V | B(\xi, \eta) \in \mathbb{Z}, \forall \xi \in L\}$ be the dual lattice of L.

For $F \in C_c^\infty(V/L)$, define the **Fourier transform** of F by

$$\hat{F}(\eta) = \frac{1}{Vol(V/L)} \int\limits_{V/L} F(v) e^{-2\pi i B(v,\eta)} dv$$

Note that the integral on the right hand side only depends on the equivalent class of v in V/L. For if $v' = v + \lambda, \lambda \in L$, $e^{-2\pi i B(v+\lambda,\eta)} = e^{-2\pi i B(v,\eta)} \cdot e^{-2\pi i B(v,\eta)} = e^{-2\pi i B(v,\eta)}$, since $\lambda \in L, \eta \in L^*$ implies $e^{-2\pi i B(\lambda,\eta)} = 1$. So the integral is well-defined.

Next, we have

Lemma 10. *Given a polynomial $P \in \mathbb{R}[x_1, \cdots, x_n]$, there exists a linear differential operator $\mathcal{D}$ with constant coefficients, such that*

$$\widehat{\mathcal{D}F}(\xi) = P(\xi) \cdot \hat{F}(\xi),$$

for $\forall F \in C^\infty(V/L), \forall \xi \in V$

Proof. Let $\{e_1, \cdots, e_n\}$ be a $\mathbb{Z}$-basis for L, $\{e_1^*, \cdots, e_n^*\}$ be the dual basis of $\{e_1, \cdots, e_n\}$ for the dual lattice L^*. Then for $x \in V$, we can write $x = x_1 e_1 + \cdots + x_n e_n$, for $\xi \in L^*$, write $\xi = \xi_1 e_1^* + \cdots + \xi_n e_n^*$. Moreover, $B(e_1, e_j^*) = \delta_{ij}$ here

$$\delta_{ij} = \begin{cases} 1, \ if & i = j \\ 0, \ if & i \neq j \end{cases} \tag{1}$$

is the Kronecker function.

For $\xi \in L^*$, using integral by parts, we have

$$\widehat{\frac{\partial F}{\partial x_1}}(\xi) = \frac{1}{Vol(V/L)} \cdot \int_0^1 \cdots \int_0^1 \frac{\partial F}{\partial x_1}(x_1, \cdots, x_n) e^{-2\pi\sqrt{-1}\sum \xi_i x_i} dx_1 \cdots dx_n$$

$$= \frac{-2\pi\sqrt{-1}\xi_1}{Vol(V/L)} \int_0^1 \cdots \int_0^1 F(x_1, \cdots, x_n) e^{-2\pi\sqrt{-1}\sum \xi_i x_i} dx_1 \cdots dx_n = \frac{-2\pi\sqrt{-1}\xi_1}{Vol(V/L)} \hat{F}(\xi).$$

Inductively, we have $r = (r_1, \cdots, r_n)$, $|r| = \sum\limits_{i=1}^n r_i$,

$$\widehat{\frac{\partial^r F}{\partial x_1^{r_1} \cdots \partial x_n^{r_n}}} = (\frac{-2\pi\sqrt{-1}}{Vol(V/L)})^{|r|} \cdot \xi_1^{r_1} \cdots \xi_n^{r_n} \hat{F}(\xi)$$

Since polynomials are linear combinations of monomials, the lemma follows in general. □

Corollary 11. *Given P, V, and $F \in C^\infty(V/L)$ as in the above lemma, there exists a constant $c > 0$, such that*

$$|P(\xi)\hat{F}(\xi)| < c,$$

for $\forall \xi \in V$.

Proof. By the above lemma, $|P(\xi)\hat{F}(\xi)| = |\widehat{\mathcal{D}F}(\xi)|$ for some differential operator $\mathcal{D}$ with constant coefficients. Since $F \in C^\infty(V/L)$, $\mathcal{D}F \in C^\infty(V/L)$, V/L is compact, so $|\widehat{\mathcal{D}F}(\xi)| \leq c$ for some constant c. □

Proposition 12. (Fourier Inversion Formula).

$$F(v) = \sum_{\eta \in L^*} \hat{F}(\eta) e^{-2\pi i B(v,\eta)}$$

.

The sum converges absolutely and uniformly on compact sets.

Proof. $\hat{F}(\eta) < \frac{c}{|P(\eta)|}$, by the above corollary. Take $P(\xi) = (\xi_1^2 + \cdots + \xi_n^2)^k$.

$$|\sum_{\eta \in L^*} \hat{F}(\eta) e^{-2\pi i B(v,\eta)}| < \sum_{0 \neq \xi \in L^*} \frac{c}{(\xi_1^2 + \cdots + \xi_n^2)^k}.$$

It is easy to see when k is large, we get that the sum converges absolutely and uniformly on compact sets, by Weirestrass M-test.

Let $G(v) = \sum\limits_{\eta \in L^*} \hat{F}(\eta) e^{w\pi i B(v,\eta)}$, then

$$\hat{G}(\eta) = \sum_{\xi \in L^*} \frac{1}{Vol(V/L)} \int\limits_{V/L} \hat{F}(\eta) e^{2\pi i (B(\xi,v) - B(\eta,v))} dv$$

$$= \sum_{\xi \in L^*} \frac{1}{Vol(V/L)} \int\limits_{V/L} \hat{F}(\eta) e^{2\pi i B(\xi - \eta, v)} dv = \hat{F}(\eta),$$

this is because $v \mapsto e^{2\pi i B(\xi - \eta, v)}$ is a character of $V \simeq \mathbb{R}^n$. Let G be a locally compact topological group, if $\chi \neq 1$ is a continuous character of G, take g_0 such that $\chi(g_0) \neq 1$, then

$$I = \int\limits_G \chi(g) dg = \int\limits_G \chi(g g_0) dg = \chi(g_0) \int\limits_G \chi(g) dg = \chi(g_0) \cdot I,$$

therefore $I = 0$. Indeed,

$$I = \int_G \chi(g)dg = \begin{cases} \mu(G), & if \quad \chi = 1 \\ 0, & if \qquad \chi \neq 1 \end{cases} \tag{2}$$

So we have $(\widehat{G - F})(\eta) = 0, \forall \eta \in L^*$

A **Fourier Polynomial** is a finite linear combination of exponential functions, by Stone-Weirestrass theorem, the *-algebra generated by Fourier polynomials is dense in the space of $\mathbb{C}$-valued continuous functions(We will discuss this explicitly in the next chapter, the reader could admit this result here).

Let H be a Fourier polynomial, since $(\widehat{G - F}) = 0$, we have $\int_{V/L} (G - F)H(v)dv = 0, \forall H$. Take a sequence of fourier polynomials H_n with limit $G \bar{-} F$, we obtain

$$\int_{V/L} (G - F)(v)(\overline{G - F})(v)dv = 0,$$

i.e. $\int_{V/L} |G - F|^2 dv = 0$, so $G = F$ a.e. □

By the Fourier inversion formula, we have $F(0) = \sum_{\eta \in L^*} \hat{F}(\eta)$. If $f \in C_c^\infty(V)$, let $F(v) = \sum_{\xi \in L} f(v + \xi)$. Then since f is of compact support and L is discrete in V, the sum on the right hand side is finite, this implies $F(v) \in C^\infty(V/L)$. And then $\sum_{\xi \in L} f(\xi) = F(0) = \sum_{\eta \in L^*} \hat{F}(\eta)$.

Let $H(v) = f(v)e^{-2\pi i B(v,\eta)}$, then

$$Vol(V/L)\hat{F}(\eta) = \int_{V/L} \sum_{\xi \in L} f(v + \xi)e^{-2\pi i B(v+\xi,\eta)}dv$$

$$= \int_{V/L} \sum_{\xi \in L} H(v + \xi)dv = \int_V H(v)dv = \int_V f(v)e^{-2\pi i B(v,\eta)}dv$$

Define

$$(\mathcal{F}f)(\eta) = \int_V f(v)e^{-2\pi i B(v,\eta)}dv,$$

we obtain the

Proposition 13.(Poisson Summation Formula). *Let $f \in C_c^\infty(V)$, then*

$$\sum_{\xi \in L} f(\xi) = \frac{1}{Vol(V/L)} \sum_{\eta \in L^*} (\mathcal{F}f)(\eta)$$

We use this to prove theorem A': Denote $f_t(x) = f(tx), t \in \mathbb{R}_+^*$. Fix t, then we have

$$\sum_{\xi \in L} f_t(\xi) = \frac{1}{Vol(V/L)} \sum_{\eta \in L^*} (\mathcal{F}f_t)(\eta)$$

$$= \frac{1}{Vol(V/L)} t^{-n} \sum_{\eta \in L^*} (\mathcal{F}f)(t^{-1}\eta)$$

$$= \frac{t^{-n}}{Vol(V/L)} (\int_V f(v)dv + \sum_{0 \neq \eta \in L^*} (\mathcal{F}f)(t^{-1}\eta))$$

Then recall

$$\sum_{\xi \in L} f_t(\xi) = \frac{t^{-n}}{Vol(V/L)} \sum_{\eta \in L^*} (\mathcal{F}f)(t^{-1}\eta)$$

$$= \frac{t^{-n}}{Vol(V/L)} \int_V f(v)dv + \sum_{0 \neq \eta \in L^*} (\mathcal{F}f)(t^{-1}\eta)$$

Let $P(\eta) = (\eta_1^2 + \cdots \eta_n^2)^k$, $k \in \mathbb{N}$, $\eta_i \in \mathbb{Z}$, the coordinates of η with respect to a $\mathbb{Z}$-basis of L^*. Let

$$g(t) = \frac{t^{-n}}{Vol(V/L)} \sum_{0 \neq \eta \in L^*} (\mathcal{F}f)(t^{-1}\eta),$$

then

$$|g(t)| \leq \frac{ct^{-n}}{Vol(V/L)} \sum_{0 \neq \eta \in L^*} \frac{1}{|P(t^{-1}\eta)|} = \frac{c't^{2k-n}}{Vol(V/L)} \sum_{0 \neq \eta \in L^*} \frac{1}{|P(\eta)|},$$

for some constant c'. Denote $\frac{c'}{Vol(V/L)} \sum_{0 \neq \eta \in L^*} \frac{1}{|P(\eta)|}$ as D_K, set $N = 2k - n$,it's clear that they both depend only on V, we have $|g(t)| \leq D_K \cdot t^N$. This completes the proof of theorem A'.

□

2.3 Non-vanishing property of L-function at 1, Dirichlet's theorem

Recall for $f \in C_c^\infty(\mathbb{A}_K)$ an Adelic Bruhat-Schwartz function, we defined the L-function

$$L(s, f, \chi) = \int_{\mathbb{I}_K} f(x)\chi)(x)\|x\|^s d^*x = \prod_{v|\infty, v \in S_1} L(s, f_v, \chi_v) \prod_{v \notin S_1} (1 - \chi_v(\pi_v)q_v^{-s})^{-1}$$

$$= \prod_{v \in S} L(s, f_v, \chi_v) L_K(s, \chi),$$

here $S = S_1 \cup \{v|\infty\}, S_1 = \{v < \infty | f_v = 1_{O_v}, \ \ \chi_v|_{O_v^*} = 1, \ \forall v \notin S_1\}, L_K(s,\chi) = \prod_{v \notin S_1} (1-\chi_v(\pi_v) q_v^{-s})^{-1}$. Note that $\prod_{v \in S} L(s, f_v, \chi_v)$ is an entire function, since if $v \in S_1$, without loss of generality, we may assume $f_v = 1_{a+\mathfrak{p}_v^{m_v}}$, then

$$L(s, f_v, \chi_v) = \int_{K_v^*} f_v(x)\chi_v(x)|x|_v^s d^*x_v = \int_{a+\mathfrak{p}_v^{m_v}} \chi_v(x)|x|_v^s d^*x_v$$

$$= q_v^{-sm_v} \int_{a+\mathfrak{p}_v^{m_v}} \chi_v(x) d^*x_v = c_v \cdot q_v^{-sm_v},$$

where $c_v = \int_{a+\mathfrak{p}_v^{m_v}} \chi_v(x) d^*x_v$, therefore each $L(s, f_v, \chi_v), v \in S_1$ is holomorphic.

For $v|\infty$, f_v is of compact support, say $supp(f_v) = C_v$, then

$$|L(s, f_v, \chi_v)| \leq \int_{C_v} |x|^\sigma \frac{dx}{x} < \infty, \ \forall \sigma \in \mathbb{R},$$

since $|x|^\sigma$ is a continuous function of x and $C_v \subset \mathbb{R}^*$ or $\mathbb{C}^*$ is compact. Therefore each $L(s, f_v, \chi_v), v|\infty$ is holomorphic.

By theorem 3' in the last section, $L(s, f, \chi)$, where $\chi : \mathbb{I}_K/K^* \mapsto \mathbb{C}^1$ a continuous character, defines a holomorphic function for $Re(s) > 1$, and has a meromorphic continuation to the right half plane, with only simple pole at $s = 1$. Moreprecisely,

$$L(s, f, \chi) = F(s, f, \chi) + E(s, f, \chi) + \frac{C_K \int_{\mathbb{A}_K} f(x)dx \int_{\mathbb{I}_K^1/K^*} \chi_0(x^1)dx^1}{s-1},$$

here $\chi = \chi_0 \cdot \chi_\infty$, χ_0 is a continuous character of $\mathbb{I}_K^1/K^*$ induced by χ, χ_∞ is a continuous character of $\mathbb{R}_+^*$ induced by χ. $F(s, f, \chi)$ is entire, $E(s, f, \chi)$ is holomorphic on $\{s \in \mathbb{C} | Re(s) > 0\}$

Assume $\chi|_{\mathbb{R}_+^*} = 1$, we have

Proposition 14. *(1), if $\chi \neq 1$, $\lim_{s\to 1}(s-1)L_K(s,\chi) = 0$; (2), if $\chi = 1$, $\lim_{s\to 1}(s-1)L_K(s,\chi) = C_{K,\chi} \cdot Vol(\mathbb{I}_K^1/K^*) \int_{\mathbb{A}_K} f(x)dx$, where $C_{K,\chi}$ is a constant depending on K and χ.*

Proof. Since $\prod_{v \in S} L(s, f_v, \chi_v)$ is an entire function,

$$\lim_{s\to 1} \prod_{v \in S} L(s, f_v, \chi_v) = \prod_{v \in S} L(1, f_v, \chi_v),$$

call it C_0. Then

$$\lim_{s\to 1}(s-1)L(s, f, \chi) = C_0 \cdot \lim_{s\to 1}(s-1)L_K(s, \chi)$$

$$= \begin{cases} C_0 \cdot C_K \int\limits_{\mathbb{A}_K} f(x)dx \cdot Vol(\mathbb{I}_K^1/K^*), & if \chi_0 = 1 \ (\Leftrightarrow \chi = 1); \\ 0, & if \chi_0 \neq 1 \ (\Leftrightarrow \chi \neq 1). \end{cases} \tag{3}$$

□

Theorem 15(Hadamard) Non vanishing property of $L_K(s,\chi)$ at s=1. *Let χ be a grossëncharacter of the number field K, trivial on $\mathbb{R}_+^*$. Suppose $\chi|_{\mathbb{I}_K^1} \neq 1$. Then $L_K(1,\chi) \neq 0$.*

Proof. **Case 1.** Suppose $\chi^2 \neq 1$.

Then for $\sigma > 1$,

$$L(\sigma,\chi) = exp(\sum_{v \notin S} \sum_{m \geq 1} \frac{\chi_v(\pi_v)^m}{m q_v^{m\sigma}}),$$

let $f(s) = L_K(s,1)^3 \cdot L_K(s,\chi)^4 \cdot L_K(s,\chi^2)$. Since $\chi_v(\pi_v) \in \mathbb{C}^{\mathbb{1}}$, $\chi_v(\pi_v) = e^{i\theta_v}$, then

$$|f(\sigma)|^2 = exp(\sum_{v \notin S} \sum_{m \geq 1} \frac{2(3 + 4\cos(m\theta_v) + \cos(2m\theta_v))}{m q_v^{m\sigma}})$$

$$= exp(\sum_{v \notin S} \sum_{m \geq 1} \frac{2(\cos\theta_v + 1)^2}{m q_v^{m\sigma}}) \geq 1,$$

since $(\cos\theta_v + 1)^2 \geq 0$. Suppose $L_K(1,\chi) = 0$, $\because \chi^2 \neq 1$, by the above proposition,

$$\lim_{s \to 1}(s-1)L_K(s,\chi^2) = 0$$

(then 1 is not a pole of $L_K(s,\chi^2)$, $\therefore L_K(1,\chi^2) \neq \infty$ On the other hand, however, $L_K(s,\chi)^4$ has a zero of order 4 at $s=1$, $L_K(s,1)^3$ has a pole of order 3 at $s=1$. $\Rightarrow \lim_{\sigma \to 1} |f(\sigma)| = 0$. But $|f(\sigma)| \geq 1$, a contradiction.

Case 2. Suppose $\chi^2 = 1$. First we make some notations. Let $\mathfrak{a}$ be an integral ideal of the number field K. S is a finite set of places of K, and $(\mathfrak{a}, S) = 1$ means: if $\mathfrak{p}|\mathfrak{a}$, then $\mathfrak{p} \notin S$. Suppose χ is unramified outside S.

Now Let $S = S_1 \cup \{v|\infty\}$ as before. If $\mathfrak{a} = \prod_v \mathfrak{p}_v^{e_v}$, $\mathfrak{p}_v \notin S$, $\Rightarrow \chi(\mathfrak{a}) = \prod_v \chi_v(\epsilon_v \pi_v^{e_v}) = \prod_v \chi_v(\pi_v)\chi_v(\pi_v^{e_v}) = \prod_v \chi_v(\pi_v)^{e_v}$, $N(\mathfrak{a}) = \prod_v N(\mathfrak{p}_v^{e_v}) = \prod_v q_v^{e_v}$. Here N is the norm map. Moreover, if $\mathfrak{p} \in S$, $\mathfrak{p}|\mathfrak{a}$, let $\chi(\mathfrak{a}) = 0$. Then

$$L_K(s,\chi) = \prod_{v \notin S}(1 - \chi_v(\pi_v)q_v^{-s})^{-1} = \sum_{\mathfrak{a} \ integral} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

Now

$$L_K(s,1)\cdot L_K(s,\chi)=\sum_{\mathfrak{a}\ integral} N(\mathfrak{a})^{-s}\sum_{\mathfrak{b}\ integral}\chi(\mathfrak{b})N(\mathfrak{b})^{-s}$$

$$=\sum_{\mathfrak{a},\mathfrak{b}\ integral}\chi(\mathfrak{b})N(\mathfrak{a}\mathfrak{b})^{-s}=\sum_{\mathfrak{c}\ integral}(\sum_{\mathfrak{b}|\mathfrak{c}}\chi(\mathfrak{b})N(\mathfrak{c}))^{-s}$$

Note that

$$\sum_{\mathfrak{b}|\mathfrak{c}}\chi(\mathfrak{b})=\prod_{\mathfrak{p}|\mathfrak{c}}(1+\chi(\mathfrak{p})+\cdots+\chi(\mathfrak{p})^{e_{\mathfrak{p}}}),$$

here $\mathfrak{c}=\prod\mathfrak{p}^{e_{\mathfrak{p}}}$. Since $\chi^2=1$, $\Rightarrow\chi(\mathfrak{p})=\pm1$.

If $\chi(\mathfrak{p})=-1$,

$$1+\chi(\mathfrak{p})+\cdots+\chi(\mathfrak{p})^{e_{\mathfrak{p}}}=\frac{1-\chi(\mathfrak{p})^{e_{\mathfrak{p}}+1}}{1-\chi(\mathfrak{p})}=\begin{cases}1, & if\ e_{\mathfrak{p}}\ is\ even;\\ 0, & if\ e_{\mathfrak{p}}\ is\ odd.\end{cases}\tag{4}$$

If $\chi(\mathfrak{p})=1$, we see that $1+\chi(\mathfrak{p})+\cdots+\chi(\mathfrak{p})^{e_{\mathfrak{p}}}\geq1$. So if $\mathfrak{c}$ is even, i.e. if $\mathfrak{c}=\mathfrak{c}'^2$, for some $\mathfrak{c}'$ integral ideal of K, then all $\sum\limits_{\mathfrak{b}|\mathfrak{c}}\chi(\mathfrak{b})\geq1$,

$$\Rightarrow L_K(s,1)\cdot L_K(s,\chi)=\sum_{\mathfrak{c}\ integral}(\sum_{\mathfrak{b}|\mathfrak{c}}\chi(\mathfrak{b}))N(\mathfrak{c})^{-s}=\sum_{\mathfrak{c}\ even}a_c\cdot N(\mathfrak{c})^{-s}+g(s),$$

with $a_c\geq1, g(s)=\sum\limits_{\mathfrak{c}\ not\ even}(\sum\limits_{\mathfrak{b}|\mathfrak{c}}\chi(\mathfrak{b}))N(\mathfrak{c})^{-s}$. Also note that $g(\sigma)\geq0$ if $\sigma\geq1$.

To proceed, we need

Lemma 16(Landau). *Suppose $f(s)=\sum\limits_{n\geq1}a_nn^{-s}$ converges when $Re(s)>0$, with $a_n\geq0$. Assume that $f(s)$ extends to a holomorphic function at σ_0. Then there exists $\sigma_1>0$, such that $f(s)=\sum\limits_{n\geq1}a_nn^{-s}$ converges for $Re(s)>\sigma_0-\sigma_1$.*

Proof. replace s by $s-\sigma_0$ if necessary, we may assume $\sigma_0=0$. For $\delta>0, 0<\sigma<\delta$,

$$f(\sigma)=\sum_{n\geq1}a_nn^{-\sigma}=\sum_{n\geq1}a_ne^{-\delta\log n}=\sum_{n\geq1}a_ne^{-(\sigma-\delta)\log n}\cdot e^{-\delta\log n}$$

$$=\sum_{n\geq1}a_ne^{-\delta\log n}\cdot\sum_{v\geq0}\frac{(\delta-\sigma)^v}{v!}(\log n)^v,$$

Note that $\delta-\sigma>0,\ a_n\geq0,\ e^{-(\sigma-\delta)\log n}>0$, thus all terms in the sum are non-negative and $f(\sigma)<\infty$ by assumption. By Fubini's theorem,

$$f(\sigma)=\sum_{v\geq 0}\frac{(-1)^v}{v!}(\sum_{n\geq 1}a_n(\log n)^v e^{-\delta\log n})(\sigma-\delta)^v$$

It is the Taylor expansion of $f(\sigma)$ at δ, which converges for $0<\sigma<\delta$. Therefore the radius of convergence is at least δ, i.e. the series converges for $0<|\sigma-\delta|<\delta$, i.e. it converges for $0<\sigma<2\delta$. And it extends to a holomorphic function at $s=\sigma_0=0$(being holomorphic at 0 means being holomorphic in a neighborhood of 0), which means the series converges for $-\epsilon<\sigma<2\delta+\epsilon$ by the general theory of Taylor series. □

Now since we know $L_K(s,1)L_K(s,\chi)$ converges for $Re(s)>1$, and $L_K(s,1)$ extends to a meromorphic function on $Re(s)>0$, with only simple pole at $s=1$, we can write

$$L_K(s,1)=\frac{c}{s-1}+F(s),$$

c is a constant and F is a holomorphic function on $Re(s)>0$. And since $\chi\neq 1$,we also have $L_K(s,\chi)$ extends to a holomorphic function on $Re(s)>0$.

Suppose $L_K(1,\chi)=0$, then $L_K(s,\chi)$ has a zero at $s=1$ with order at least 1. Therefore $L_K(s,1)L_K(s,\chi)$ extends to a holomorphic function on $Re(s)>0$, thus on $Re(s)>1/3$.

Apply Landau's lemma to $\sigma_0=1$, we see that $L_K(s,1)L_K(s,\chi)$ converges absolutely up to $Re(s)>1/3$.

On the other hand, $L_K(s,1)L_K(s,\chi)=\sum\limits_{\mathfrak{c}\ even}a_c\cdot N(\mathfrak{c})^{-s}+g(s)$. Note that

$$\sum_{\mathfrak{c}\ even}a_c\cdot N(\mathfrak{c})^{-\sigma}\geq\sum_{\mathfrak{c}'\ integral}N(\mathfrak{c}')^{-2\sigma},$$

and $\sum\limits_{\mathfrak{c}'\ integral}N(\mathfrak{c}')^{-2\sigma}$ has a pole at $\sigma=1/2$, since $L_K(s,1)$ has a pole at $s=1$. This implies that $L_K(s,1)L_K(s,\chi)$ has a pole at $s=1/2$, a contradiction. We conclude that $L_K(1,\chi)\neq 0$. □

Corollary 17. *Let $\chi=\otimes'_v\chi_v$ be a grossëncharacter of a given number field K. $S\supset S_1\cup\{v|\infty\}$ be a finite set of places such that χ_v is unramified outside S. Then*

$$(1).\ \lim_{\sigma\to 1^+}\frac{\sum\limits_{v\notin S}q_v^{-\sigma}}{\ln\frac{1}{\sigma-1}}=1,$$

$$(2).If\ \chi\neq 1\ on\ \mathbb{I}_K^1,\ then\ \lim_{\sigma\to 1^+}\sum_{v\notin S}\chi_v(\pi_v)q_v^{-\sigma}\ exists.$$

Proof. Recall that for $Re(s) > 1$, similar to the previous argument, we have

$$L_K^S(s,\chi) = exp(\sum_{v\notin S} \chi_v(\pi_v) q_v^{-s}) exp(g_0(s,\chi)),$$

where $g_0(s,\chi)$ is holomorphic on $Re(s) > 1/2$. $\Rightarrow L_K^S(\sigma,1) > 0$ if $\sigma > 0$(Take $\chi = 1$), $\Rightarrow \lim_{\sigma\to 1^+}(\sigma-1)L_K^S(\sigma,1) = \kappa > 0$ (since $L(s,f,1) = \prod_{v\in S} L(s,f_v,1_v)\cdot L_K^S(s,1)$ has simple pole at $s=1$, and $\prod_{v\in S} L(s,f_v,1_v)$ is holomorphic for all $s\in\mathbb{C}$ by previous theorem, $\Rightarrow L_K^S(s,1)$ has simple pole at $s=1$), then

$$\lim_{\sigma\to 1^+} \ln(\sigma-1) + \lim_{\sigma\to 1^+} \ln(L_K^S(\sigma,1)) = \lim_{\sigma\to 1^+} \ln\kappa$$

$$\Rightarrow \frac{\ln(L_K^S(\sigma,1))}{\ln(\frac{1}{\sigma-1})} \to 1 + \frac{\ln\kappa}{\ln(\frac{1}{\sigma-1})} \to 1,\ as\ \sigma\to 1^+.$$

$$\Rightarrow \frac{\sum\limits_{v\notin S} q_v^{-\sigma}}{\ln(\frac{1}{\sigma-1})} + \frac{g_0(\sigma,1)}{\ln(\frac{1}{\sigma-1})} \to 1,\ as\ \sigma\to 1^+.$$

Since $g_0(s,\chi)$ is holomorphic for $Re(s) > 1/2$, $\lim\limits_{\sigma\to 1^+} g_0(\sigma,1)$ exists. Therefore

$$\lim_{\sigma\to 1^+} \frac{\sum\limits_{v\notin S} q_v^{-\sigma}}{\ln(\frac{1}{\sigma-1})} = 1$$

This proves (1).

For (2), note that $\ln(L_K^S(s,\chi)) = \sum\limits_{v\notin S} \chi_v(\pi_v) q_v^{-s} + g_0(s,\chi)$, $\lim\limits_{\sigma\to 1^+} g_0(\sigma,1)$ exists, it suffices to show that $\lim\limits_{\sigma\to 1^+} L_K^S(\sigma,\chi)$ exist. But by previous theorem, saying that $L_K(s,\chi)$ defined by a non-trivial *grossëncharacter* χ does not vanish at $s=1$, and note that the same proof also works for $L_K^S(1,\chi)$. We have $L_K^S(1,\chi) \neq 0$ for $\chi \neq 1$, $\Rightarrow \lim\limits_{\sigma\to 1^+} \ln L_K^S(\sigma,\chi)$ exists. This proves (2). □

For the rest part of this section, we use the non-vanishing property of $L_K(s,\chi)$ at $s=1$ to show the famous Dirchlet theorem, which states that there are infinitely many prime numbers of the form $an+b$, $n\in\mathbb{N}$, where a and b are coprime.

Suppose v is an unramified place of the number field K(i.e. the ramification index $e_v = e(K_v/\mathbb{Q}_p) = 1$), here $v|p$. If we also have the corresponding inertial degree $f_v = f(K_v/\mathbb{Q}_p) = 1$, we call such a place is of **absolute degree 1**. Note that for an absolutely degree 1 place v, we have $K_v = \mathbb{Q}_p$ since $[K_v:\mathbb{Q}_p] = e_v\cdot f_v = 1$.

Theorem 18. *Let χ be a grossëncharacter on $\mathbb{I}_K$, assume $\chi|_{\mathbb{R}_+^*} = 1$, $S \supset S_1 \cup \{v|\infty\}$ be a finite*

set of places such that χ_v is unramified outside S we have

$$\lim_{\sigma\to 1^+}\frac{\sum\limits_{v\notin S, abdeg(v)=1}\chi_v(\pi_v)q_v^{-\sigma}}{\ln\frac{1}{\sigma-1}}=\begin{cases}1, & if\ \chi=1;\\ 0, & if\ \chi\neq 1.\end{cases}\tag{5}$$

Proof. Recall that by the previous corollary, $\lim\limits_{\sigma\to 1^+}\frac{\sum\limits_{v\notin S}q_v^{-\sigma}}{\ln\frac{1}{\sigma-1}}=1$; And if $\chi\neq 1$, then $\lim\limits_{\sigma\to 1^+}\sum\limits_{v\notin S}\chi_v(\pi_v)q_v^{-\sigma}$ exists. So it suffices to show that for $v\notin S$ and of absolute degree >1,

$$|\sum_{v\notin S,\ abdeg(v)>1}\chi_v(\pi_v)q_v^{-s}|<\infty,\quad as\ Re(s)=\sigma\to 1^+$$

So without loss of generality, we may assume $\chi=1$, then

$$\sum_{v\notin S,\ abdeg(v)>1}q_v^{-\sigma}\leq[K:\mathbb{Q}]\cdot\sum_p\sum_{m\geq 2}p^{-m\sigma}$$

$$=[K:\mathbb{Q}]\cdot\sum_p\frac{p^{-2\sigma}}{1-p^{-\sigma}}\leq[K:\mathbb{Q}]\cdot\sum_p p^{-2\sigma}\cdot\frac{1}{1-2^{-\sigma}}<\infty$$

□

Given a place v of K, to simplify the notation, let $\pi_v=(1,\cdots,1,\pi_v,1,\cdots,1)\in\mathbb{I}_K$, $\tilde{t}=(1,\cdots,1,t^{\frac{1}{n}},\cdots,t^{\frac{1}{n}})\in\mathbb{R}_+^*$, where $t=|\pi_v|_v$. Then $\|\pi_v\|=|\pi_v|_v=t$, $\frac{\pi_v}{|\pi_v|_v}=\pi_v\tilde{t}^{-1}\in\mathbb{I}_K^1$. Assume $\chi|_{\mathbb{R}_+^*}=1$, $\Rightarrow\chi(\pi_v)=\chi(\frac{\pi_v}{|\pi_v|_v})$.

A **Fourier Polynomial** is a function on $\mathbb{I}_K^1$ of the form $f=a_1\chi_1+\cdots+a_r\chi_r$, where

$$\chi_i:\mathbb{I}_K^1/K^*\to\mathbb{C}^1,\ i=1,2,\cdots,r$$

are continuous characters on $\mathbb{I}_K^1/K^*$. Specifically, let $\chi_1=1$.

Define

$$D(f)=\lim_{\sigma\to 1^+}\frac{\sum\limits_{v\notin S,\ abdeg(v)=1}f(\pi_v)q_v^{-\sigma}}{ln\frac{1}{\sigma-1}},$$

the limit exists by previous theorem, and it's easy to see that $D(f)=a_1$. Moreover, we have $\int\limits_{\mathbb{I}_K^1/K^*}f(x)d^*x=a_1$, by orthogonality. Therefore we have

$$\int_{\mathbb{I}_K^1/K^*}f(x)d^*x=D(f)=\lim_{\sigma\to 1^+}\frac{\sum\limits_{v\notin S,\ abdeg(v)=1}f(\pi_v)q_v^{-\sigma}}{ln\frac{1}{\sigma-1}}$$

Lemma 19. *The limit*

$$\lim_{\sigma\to 1^+}\frac{\sum\limits_{v\notin S,\ abdeg(v)=1} f(\pi_v)q_v^{-\sigma}}{ln\frac{1}{\sigma-1}}$$

exists for any continuous function f on $\mathbb{I}_K^1/K^*$, and it equals $\int\limits_{\mathbb{I}_K^1/K^*} f(x)d^*x$.

Proof. The proof is essentially the

Theorem 20(Stone-Weirestrass) (1)**.** Let X be a compact Hausdorff space and let S be a subset of $C(X,\mathbb{C})$, the space of complex-valued continuous functions on X, which separate points. Then the complex unital *-algebra generated by S is dense in $C(X,\mathbb{C})$.(Here separate points means if $x\neq y,\ x,y\in X$, then there exists some $f\in S$, such that $f(x)\neq f(y)$. And in our case $f^*=\bar{f}$, the complex conjugation.)

Now let $G=\mathbb{I}_K^1/K^*$, then as we know, G is compact. Let

$$S=\left\{\chi:\mathbb{I}_K^1/K^*\to\mathbb{C}|\chi \textit{ is a continuous homomorphism}\right\}$$

We see that $1\in S$ and the *-algebra generated by S is $\mathcal{F}$, the space of Fourier polynomials. Note that if $\chi_1,\ \chi_2\in S$, we have $\chi_1\cdot\chi_2\in S$, and $(\chi_1\cdot\chi_2)^*=\overline{\chi_1\cdot\chi_2}=\bar{\chi_2}\cdot\bar{\chi_1}=\chi_2^*\cdot\chi_1^*$. Therefore, if f_1 and f_2 are Fourier polynomials, $f_1\cdot f_2$ is also a Fourier polynomial.

To see S separates points on G, let $x,y\in G,\ x\neq y$. Then $z=xy^{-1}\neq 1$, and $z\in G$ since G is a group. Suppose $\forall\chi\in S,\chi(z)=\chi(xy^{-1})=1$, by **Pontryajin duality**, $G\simeq\hat{\hat{G}}$, it is an isomorphism of locally compact groups. Suppose the isomorphism is given by the map $z\mapsto\phi_z$, and then $\phi_z(\chi)=\chi(z)$. Now if $\chi(z)=1$ for all $\chi\in S$, $\phi_z(\chi)=\chi(z)=1$, for all $\chi\in\hat{G}$. $\Rightarrow\phi_z=1$, but $z\neq 1$, contradicting the Pontryajin duality. Therefore there exists a $\chi\in S$, such that $\chi(z)\neq 1$, i.e. $\chi(xy)=\chi(x)\chi(y)^{-1}\neq 1$, i.e. there exists a $\chi\in S$, such that $\chi(x)\neq\chi(y)$. S separates points. Thus $\mathcal{F}$ is dense in $C(X,\mathbb{C})$, by Stone-Weirestrass theorem. This means that for $\forall\epsilon>0$, and $\forall f\in C(X,\mathbb{C})$, there exists some $g\in\mathcal{F}$, such that $\|g-f\|_\infty<\epsilon$, then $|f(x)-g(x)|<\epsilon$, for $\forall x\in\mathbb{I}_K^1/K^*$.

Let T be a finite set of places, everything unramified, let $h=f-g$, we have

$$\sum_{v\in T,abdeg(v)=1} f(\pi_v)q_v^{-\sigma}=\sum_{v\in T,abdeg(v)=1} g(\pi_v)q_v^{-\sigma}+\sum_{v\in T,abdeg(v)=1} h(\pi_v)q_v^{-\sigma},$$

Let

$$D(f,\sigma)=\frac{\sum\limits_{v\in T,abdeg(v)=1} f(\pi_v)q_v^{-\sigma}}{\ln\frac{1}{\sigma-1}},$$

$$R(T,\sigma) = \sum_{v\in T, abdeg(v)=1} h(\pi_v) q_v^{-\sigma},$$

then $|R(T,\sigma)| < \epsilon \cdot \sum_{v\in T, abdeg(v)=1} q_v^{-\sigma}$, and we have

$$D(f,\sigma) = D(g,\sigma) + \frac{R(T,\sigma)}{\ln \frac{1}{\sigma-1}},$$

we know

$$|\frac{R(T,\sigma)}{\ln \frac{1}{\sigma-1}}| < \epsilon \cdot \frac{\sum_{v\in T, abdeg(v)=1} q_v^{-\sigma}}{\ln \frac{1}{\sigma-1}} \leq 2\epsilon.$$

Let $D(f) = \lim_{\sigma\to 1^+} D(f,\sigma)$, then if we choose $\sigma \to 1^+$ be close enough, say $\sigma - 1 < \delta$, we have

$$|D(f,\sigma) - D(g)| \leq |D(f,\sigma) - D(g,\sigma)| + |D(g,\sigma) - D(g)| < 2\epsilon + \epsilon = 3\epsilon,$$

Also note that

$$|\int_{\mathbb{I}_K^1/K^*} f(x)d^*x - \int_{\mathbb{I}_K^1/K^*} g(x)d^*x| < \epsilon \cdot \int_{\mathbb{I}_K^1/K^*} d^*x = \epsilon.$$

So we have

$$|D(f,\sigma) - \int_{\mathbb{I}_K^1/K^*} f(x)d^*x| < 4\epsilon,\ if\ \sigma - 1 < \delta$$

□

Corollary 21. *Let $S \supset \{v|\infty\}$ be a finite set of places of a number field K, then the image of $\left\{\frac{\pi_v}{|\pi_v|_v} | v \notin S\right\}$ is dense in $\mathbb{I}_K^1/K^*$.*

Proof. Let C be the closure of the image as stated. Suppose $C \neq \mathbb{I}_K^1/K^*$, then the complement of C in $\mathbb{I}_K^1/K^*$, call it V, is open. Since $\mathbb{I}_K^1/K^*$ is compact and Hausdorff, therefore normal. So we can find a compact subset $K \subset V$, and $d^*x(K) > 0$ since d^*x is a Haar measure.

By Urysohn's lemma, there exists $f \in C(\mathbb{I}_K^1/K^*)$, such that $f|_K = 1$,and $suppf \subset V$. Then

$$\int_{\mathbb{I}_K^1/K^*} f(x)d^*x = d^*x(K) > 0.$$

On the other hand, since Fourier polynomials are dense in $C(K)$, we can find a sequence of Fourier polynomials g_n on K such that $g_n \to f$. Now note that $supp(g_n) \subset K \subset V = \mathbb{I}_K^1/K^* - \left\{\frac{\pi_v}{|\pi_v|_v | v\notin S}\right\}$,

so

$$\int\limits_{\mathbb{I}_K^1/K^*} g_n(x)d^*x = \lim_{\sigma\to 1^+} \frac{\sum\limits_{v\notin S, abdeg(v)=1} g_n(\pi_v)q_v^{-\sigma}}{\ln\frac{1}{\sigma-1}} = 0,$$

since $g_n\pi_v = 0$ for $v \notin S, abdeg(v) = 1$. But this implies that

$$\int\limits_{\mathbb{I}_K^1/K^*} f(x)d^*x = \lim_{\sigma\to 1^+} \int\limits_{\mathbb{I}_K^1/K^*} g_n(x)d^*x = 0,$$

a contradiction. □

Corollary 22. *If $\phi : \mathbb{I}_K^1/K^* \twoheadrightarrow G$ is a surjective continuous homomorphism of topological groups, where G is a finite group with discrete topology. Then there are infinitely many v for which $\frac{\pi_v}{|\pi_v|_v}$ goes to any fixed element.(i.e. the fibre of ϕ over any element in G is infinite)*

Proof. suppose $\phi^{-1}(\{x\})$ is finite. Since $\phi^{-1}(\{x\})$ is open and $\left\{\frac{\pi_v}{|\pi_v|_v} | v \notin S\right\}$ is dense in $\mathbb{I}_K^1/K^*$. Then there is an open set in $\mathbb{I}_K^1/K^*$ which contains only finitely many $\frac{\pi_v}{|\pi_v|_v}$ in it. A contradiction, since $\mathbb{I}_K^1/K^*$ is a metric space. (Simply take balls of radius $\frac{1}{n}$ contained in the open set, by density we can find infinitely many such $\frac{\pi_v}{|\pi_v|_v}$.) □

Lemma 23.

$$\mathbb{I}_{\mathbb{Q}} = \mathbb{Q}^* \cdot \prod_p \mathbb{Z}_p^* \cdot \mathbb{R}_+^*$$

Proof. Let $x = (x_p)_p \in \mathbb{I}_{\mathbb{Q}}$, let $n = \prod\limits_{p<\infty} p^{ord_p x_p}$, then $\tilde{n} = (n, \cdots, n) \in \mathbb{Q}^*$ and thus $(\tilde{n})^{-1}x \in U \cdot \mathbb{R}^*$, where $U = \prod\limits_{p<\infty} \mathbb{Z}_p^*$. Let the last coordinate be the place of infinity, note that $(1, \cdots, 1, -1) = (-1, \cdots, -1)\cdot(-1, \cdots, -1, 1), (-1, \cdots, -1) \in \mathbb{Q}^*, (-1, \cdots, -1, 1) \in U$, so multiply by $(1, \cdots, 1, -1)$ if necessary, we obtain $(\tilde{n})^{-1}x \in U \cdot \mathbb{R}_+^*$, i.e. $x \in \mathbb{Q}^* \cdot \prod\limits_p \mathbb{Z}_p^* \cdot \mathbb{R}_+^*$. The lemma follows. □

Next, we prove the famous

Theorem 24(Dirichlet). *Suppose a and m are integers, $(a, m) = 1$, then there are infinitely many prime numbers p such that $p \equiv a(\mod m)$*

Proof. We have $\mathbb{I}_{\mathbb{Q}}^1 = \mathbb{Q}^* \cdot U$, then it is easy to see

$$\mathbb{I}_{\mathbb{Q}}^1/\mathbb{Q}^* = (\mathbb{Q}^* \cdot U)/\mathbb{Q}^* \simeq U/(\mathbb{Q}^* \cap U) \simeq U,$$

as topological groups, let

$$U_m = \prod_{p\nmid m} \mathbb{Z}_p^* \cdot \prod_{p|m} (1 + p^{ord_p(m)})$$

the map

$$\mathbb{I}^1_{\mathbb{Q}}/\mathbb{Q}^* \simeq U \to U/U_m \simeq \prod_{p|m} \mathbb{Z}_p^*/(1+p^{ord_p(m)}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

(the last isomorphism follows from Chinese Remainder Theorem) is continuous, since U_m is open in U, and surjective. So by the previous corollary, the fiber of any element in $(\mathbb{Z}/m\mathbb{Z})^*$ is infinite.

Let $p_{\mathbb{Q}}^{-1} = (1, \cdots, 1, p^{-1}, 1, \cdots, 1) = (p, \cdots, p, 1, p, \cdots, p, 1) \cdot (p^{-1}, \cdots, p^{-1}) \cdot (1, \cdots, 1, p) \in \mathbb{I}_{\mathbb{Q}}$. Note that

$$(p, \cdots, p, 1, p, \cdots, p, 1) \in U,\ (p^{-1}, \cdots, p^{-1}) \in \mathbb{Q}^*,\ (1, \cdots, 1, p) \in \mathbb{R}_+^*.$$

So the image of $p_{\mathbb{Q}}^{-1}$ in $\mathbb{I}^1_{\mathbb{Q}}/\mathbb{Q}^* \simeq U$ is $(p, \cdots, p, 1, p, \cdots, p, 1)$. Since the isomorphism $\mathbb{Z}_p^*/(1+p^r\mathbb{Z}_p) \to (\mathbb{Z}/p^r\mathbb{Z})^*$ is given by $x \cdot (1 + p^r\mathbb{Z}_p) \mapsto x \mod p^r\mathbb{Z}$, we can see that for $q \neq p$, the image of $(p, \cdots, p, 1, p, \cdots, p)$ in $(\mathbb{Z}/q^{ord_q(m)}\mathbb{Z})^*$ is the conjugacy class $p \mod q^{ord_q(m)}\mathbb{Z}$; for $q = p$, the image of $(p, \cdots, p, 1, p, \cdots, p)$ in $(\mathbb{Z}/p^{ord_p(m)}\mathbb{Z})^*$ is the conjugacy class $0 \mod p^{ord_p(m)}\mathbb{Z}$. So we can see that the image of $(p, \cdots, p, 1, p, \cdots, p)$ in $(\mathbb{Z}/m\mathbb{Z})^*$ is the conjugacy class $p \mod m$, by Chinese Remainder Theorem. Therefore by the argument in the first paragraph of the proof, if we have $(a, m) = 1$, there are infinitely many prime numbers p such that the image of $(p, \cdots, p, 1, p, \cdots, p)$ goes to $a \mod m$. i.e. there are infinitely many primes p such that $p \equiv a(\mod m)$, if $(a, m) = 1$. □

2.4 The first inequality.

Theorem 25(the first inequlity). *Let L/K be a Galois extension of number fields, then*

$$h = [\mathbb{I}_K^1 : N_{L/K}(\mathbb{I}_K^1)K^*] \leq [L : K] = n$$

Proof. Let

$$S_L = \{\omega \text{ place of } L | \omega < \infty,\ \omega | p,\ L_\omega = \mathbb{Q}_p\},$$

$$S'_L = \{\pi_\omega | \omega \in S_L,\ \pi_\omega = 1 + \cdots + 1 = p_\omega \in \mathbb{Q}_p\}.$$

If $\omega \in S_L,\ \omega | v | p$, it is easy to see that $[L_\omega : \mathbb{Q}_p] = 1$, this is equivalent to say that $[L_\omega : K_v] = [K_v : \mathbb{Q}_p] = 1$. Note that $S'_L \subset \mathbb{I}_L$.

Lemma 26. *The norm map $N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ maps S'_L into S'_K.*

Proof. If $\pi_\omega \in S'_L$, $\pi_\omega = p_\omega = (1, \cdots, 1, p_\omega, 1, \cdots, 1) \in \mathbb{I}_L$.

$$N_{L/K}(\pi_\omega) = N_{L/K}(1, \cdots, 1, p_\omega, 1, \cdots, 1) = (1, \cdots, 1, N_{L_\omega/K_v}(p_\omega), 1, \cdots, 1)$$

$$= (1, \cdots, 1, p_v^{f_\omega}, 1, \cdots, 1) == (1, \cdots, 1, p_v, 1, \cdots, 1) \in S'_K,$$

since $e_\omega \cdot f_\omega = [L_\omega : K_v] = 1$, and then we have $e_\omega = f_\omega = 1$. Here $e_\omega = e(L_\omega/K_v)$ is the ramification index at ω, $f_\omega = f(L_\omega/K_v)$ is the inertial degree at ω. □

Lemma 27. *The norm map $N_{L/K} : S'_L \to S'_K$ is n to 1, $n = [L : K]$, i.e. every $p_v = (1, \cdots, 1, p_v, 1, \cdots, 1) \in S'_K$ has exactly n preimages in S'_L.*

Proof. Let $p_v = (1, \cdots, 1, p_v, 1, \cdots, 1) \in S'_K$ be fixed. Since L/K is Galois, if $\omega \in S'_L$, $\omega|v|p$, suppose $\omega_1|v|p$ for another place ω_1 of L, then

$$1 = [L_\omega : K_v] = [L_{\omega_1} : K_v] = e_{\omega_1} \cdot f_{\omega_1},$$

it follows that $\omega_1 \in S'_L$. Let $\omega_1, \cdots, \omega_r$ be all conjugate places of $\omega|v|p$, then

$$[L_{\omega_1} : K_v] = [L_{\omega_2} : K_v] = \cdots = [L_{\omega_{r_v}} : K_v] = 1,$$

This shows $e_{\omega_i} = f_{\omega_i} = 1$, for all $i = 1, 2, \cdots, r_v$. Since we know $e_v f_v r_v = n = [L : K]$, and now $e_v = f_v = 1$, so $r_v = n$. Then it is easy to see that $N_{L/K} : S'_L \to S'_K$ maps each π_{ω_i}, $(i = 1, 2, \cdots, r_v = n)$ to p_v by the above argument. Therefore $N_{L/K} : S'_L \to S'_K$ is n to 1. □

Moreover, we know $N_{L/K}(\mathbb{I}^1_L)K^*/K^*$ is an open subgroup of $\mathbb{I}^1_K \cdot K^*/K^* = \mathbb{I}^1_K/K^*$ of finite index, therefore $N_{L/K}(\mathbb{I}^1_L)K^*/K^*$ is also closed in $\mathbb{I}^1_K/K^*$, since $\mathbb{I}^1_K/K^*$ is a topological group(In a topological group G, any open subgroup H is also closed since $H = G - \cup_{gH \neq H} gH$, and each gH is open since $\phi(g) : G \to G$ defined by $\phi(g)(x) = gx$ is a homeomorphism and H is open, thus each coset gH is open, so H is closed.). Then if we let $f = 1_{N_{L/K}(\mathbb{I}^1_L)K^*/K^*}$, we can see that f is a continuous function on the compact group $\mathbb{I}^1_K/K^*$.

Now we have

$$\frac{1}{h} = \frac{1}{[\mathbb{I}^1_K/K^* : N_{L/K}(\mathbb{I}^1_L)K^*/K^*]} = \int\limits_{\mathbb{I}^1_K/K^*} f(x) d^*x,$$

this is because the Haar measure $d\mu = d^*x$ on the compact group $\mathbb{I}^1_K/K^*$ is normalised so that $\mu(\mathbb{I}^1_K/K^*) = 1$, and the fact:

Lemma 28. *Let G be a locally compact topological group, $d\mu$ is a (left) Haar measure on G. H is a subgroup of G, let $f = 1_H$ be the characteristic function of H, then*

$$\int\limits_G f d\mu = \frac{\mu(G)}{[G : H]}.$$

Proof. Note that

$$\int\limits_G f d\mu = \int\limits_G 1_H d\mu = \mu(H),$$

on the other hand,

$$\mu(G) = \int_G 1 d\mu = \int_{\sqcup gH} 1 d\mu = \sum \mu(gH) = \sum \mu(H) = [G:H]\mu(H),$$

here $\mu(gH) = \mu(H),\ \forall g \in G$, by the left-invariance of Haar measure, therefore

$$\int_g f d\mu = \mu(H) = \frac{\mu(G)}{[G:H]}.$$

□

Now we have

$$\frac{1}{h} = \int_{\mathbb{I}_K^1/K^*} f(x) d^*x = \lim_{\sigma \to 1^+} D(f, \sigma)$$

$$= \lim_{\sigma \to 1^+} \frac{\sum_{v \notin S, abdeg(v)=1} f(p_v) q_v^{-\sigma}}{\ln \frac{1}{\sigma - 1}},$$

where $p_v = (1, \cdots, 1.p_v, 1, \cdots, 1)$, thus $|p_v|_v = \|p_v\|$.

Lemma 29.

$$\alpha \in N_{L/K}(\mathbb{I}_L)K^* \Leftrightarrow \frac{\alpha}{\|\alpha\|} \in N_{L/K}(\mathbb{I}_L^1)K^*$$

Proof. $\alpha \in N_{L/K}(\mathbb{I}_L)K^* \Rightarrow \alpha = N_{L/K}(x)\beta$, for some $x \in \mathbb{I}_L, \beta \in K^*$. Since $\mathbb{I}_L \simeq \mathbb{I}_L^1 \cdot \mathbb{R}_+^*$, we can write $x = x^1 \cdot \tilde{\tau}$, $x^1 \in \mathbb{I}_L^1$, $\tilde{\tau} = (1, \cdots, 1, \tau^{\frac{1}{n}}, \cdots, \tau^{\frac{1}{n}})$, $\tau = \|x\|$. Then

$$\alpha = N_{L/K}(x^1 \cdot \tilde{\tau}) \cdot \beta = N_{L/K}(x^1) N_{L/K}(\tilde{\tau}) \cdot \beta = \alpha^1 \cdot \tilde{t} \cdot \beta,$$

where $\alpha^1 = N_{L/K}(x^1) \in \mathbb{I}_K^1$, $\beta \in K^*$, $\tilde{t} = (1, \cdots, 1, t^{\frac{1}{n}}, \cdots, t^{\frac{1}{n}}) = N_{L/K}(\tilde{\tau}) \in \mathbb{R}_+^*$. Then

$$\|\alpha\| = \|\alpha^1 \cdot \tilde{t} \cdot \beta\| = \|\alpha^1\| \cdot \|\tilde{t}\| \cdot \|\beta\| = \|\tilde{t}\| = t = \|N_{L/K}(\tilde{\tau})\| = N_{L/K}(\|x\|).$$

since $\|\frac{\tilde{\tau}}{\|x\|}\| = \frac{\tau}{\|x\|} = 1, \Rightarrow \frac{\tilde{\tau}}{\|x\|} \in \mathbb{I}_K^1$,

$$\Rightarrow \frac{\alpha}{\|\alpha\|} = N_{L/K}(x^1 \cdot \frac{\tilde{\tau}}{\|x\|}) \cdot \beta \in N_{L/K}(\mathbb{I}_L^1) \cdot K^*,$$

Conversely, if $\frac{\alpha}{\|\alpha\|} = N_{L/K}(x^1) \cdot \beta$, for some $x^1 \in \mathbb{I}_L^1$, $\beta \in K^*$, $\Rightarrow \alpha = N_{L/K}(x^1)\|\alpha\| \cdot \beta$, let $t = \|\alpha\|$, then $\alpha = N_{L/K}(x^1 \cdot \tilde{t}) \cdot \beta$, now $x^1 \cdot \tilde{t} \in \mathbb{I}_L^1 \cdot \mathbb{R}_+^* = \mathbb{I}_L$, $\Rightarrow \alpha \in N_{L/K}(\mathbb{I}_K) \cdot K^*$. □

By the lemma, it is easy to see that

$$\frac{p_v}{|P_v|_v} = \frac{p_v}{\|p_v\|} \in N_{L/K}(\mathbb{I}_L)K^*/K^* \Leftrightarrow p_v \in N_{L/K}(\mathbb{I}_L)K^*/K^*.$$

Now we can see $f(p_v) = f(\frac{p_v}{|p_v|_v}) = \frac{p_v}{\|p_v\|} = 1$ if $\frac{p_v}{\|p_v\|} \in N_{L/K}(\mathbb{I}_L)K^*/K^* \Leftrightarrow p_v \in N_{L/K}(\mathbb{I}_L)K^*/K^*$. Also note we require $v \notin S$ and $abdeg(v) = 1$, this is equivalent to say that $v \in S'_K$, so

$$\frac{1}{h} = \int\limits_{\mathbb{I}_K^1/K^*} f(x)d^*x = \lim_{\sigma\to 1^+} D(f,\sigma) = \lim_{\sigma\to 1^+} \frac{\sum\limits_{v\notin S, abdeg(v)=1} f(p_v)q_v^{-\sigma}}{\ln\frac{1}{n-1}}$$

$$= \lim_{\sigma\to 1^+} \frac{\sum\limits_{v\in S'_K} q_v^{-\sigma}}{\ln\frac{1}{n-1}} \geq \lim_{\sigma\to 1^+} \frac{1}{n}\cdot\frac{\sum\limits_{\omega\in S'_L} q_\omega^{-\sigma}}{\ln\frac{1}{n-1}} = \frac{1}{n}\lim_{\sigma\to 1^+} \frac{\sum\limits_{abdeg(\omega)=1} q_\omega^{-\sigma}}{\ln\frac{1}{n-1}} = \frac{1}{n},$$

here first note that $q_v = q_\omega^{f_\omega} = q_\omega$, and recall that $N_{L/K} : S'_L \to S'_K$ is n to 1. Moreover, $\omega \in S'_L \Leftrightarrow \omega \in S_L,\ \pi_\omega = 1 + \cdots + 1 = p_\omega \Leftrightarrow \omega < \infty,\ \omega|p, L_\omega = \mathbb{Q}_p,\ \pi_\omega = p_\omega = p^{e(L_\omega/\mathbb{Q}_p)} = p \Leftrightarrow e_\omega = f_\omega = 1 \Leftrightarrow abdeg(\omega) = 1$. And by previous theorem we have

$$\lim_{\sigma\to 1^+} \frac{\sum\limits_{abdeg(\omega)=1} q_\omega^{-\sigma}}{\ln\frac{1}{n-1}} = 1$$

i.e. $\frac{1}{h} \geq \frac{1}{n}$, so $h \leq n$. Now we completed the proof of the first inequality in class field theory. $\square$

3 Cohomology, and the Second Inequality

3.1 Herbrand Quotients

Suppose that A is an abelian group, B is a subgroup of A, and f is a homomorphism of A into some other abelian group. Let $A_f = \operatorname{Ker} f$ and $A^f = \operatorname{Im} f$. By restricting f we obtain a homomorphism of B, for which we use similar notation: $B_f = \operatorname{Ker}(f_{|B})$ and $B^f = \operatorname{Im} f_{|B}$.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & A_f/B_f & \to & A/B & \to & A^f/B^f & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & A_f & \to & A & \to & A^f & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & B_f & \to & B & \to & B^f & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The diagram above has all of its columns as well as the bottom two rows exact. It is easy to see that the obvious maps in the upper row are well defined, and a diagram chase shows that this row is exact. Hence we have the identity

$$[A : B] = [A_f : B_f][A^f : B^f]$$

in the sense that if two of the indices above are finite, then so is the third and equality holds.

Now, suppose that f and g are *endomorphisms* of A such that $f \circ g = g \circ f = 0$. Then $A^g \subseteq A_f$ and $A^f \subseteq A^g$, and we can define the **Herbrand quotient**

$$Q_{f,g}(A) = Q(A) = \frac{[A_f : A^g]}{[A_g : A^f]}$$

provided the numerator and denominator are finite. Note that if $f(B), g(B) \subseteq B$, then there are unique induced homomorphisms

$$\bar{f}, \bar{g} : A/B \to A/B$$

satisfying $\bar{f}(x + B) = f(x) + B$ and $\bar{g}(x + B) = g(x) + B$. So again we will have $\bar{f} \circ \bar{g} = \bar{f} \circ \bar{g} = 0$, and we can define another Herbrand quotient

$$Q_{\bar{f},\bar{g}}(A/B) = Q(A/B) = \frac{[(A/B)_{\bar{f}} : (A/B)^{\bar{g}}]}{[(A/B)_{\bar{g}} : (A/B)^{\bar{f}}]}$$

when the numerator and denominator are finite.

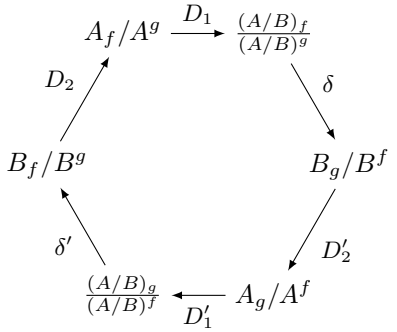
Lemma 1. *If A is finite, then $Q(A) = 1$.*

Proof. We have $A/A_g \cong A^g$ and $A/A_f \cong A^f$, so

$$|A^g| \cdot |A_g| = |A| = |A^f| \cdot |A_f|$$

□

We will investigate the properties of the following hexagonal diagram:



The definitions of the homomorphisms D_2, D_1 are morally obvious, while those of δ, δ' are not. We explain all the definitions in detail:

- For the composition $B_f \hookrightarrow A_f \twoheadrightarrow A_f/A^g$, the fact that $B^g \subseteq A^g$ implies that the map $D_2 : B_f/B^g \to A_f/A^g$ given by $D_2(x + B^g) = x + A^g$ is well defined. D_2' is defined similarly.

- The image of the composition $A_f \hookrightarrow A \twoheadrightarrow A/B$ is clearly contained in $(A/B)_{\bar{f}}$, so we have a well defined homomorphism $\pi : A_f \to (A/B)_{\bar{f}}$ given by $\pi(x) = x + B$. Clearly the image of A^g under π is contained in $(A/B)^{\bar{g}}$, so the mapping $D_1 : A_f/A^g \to \frac{(A/B)_{\bar{f}}}{(A/B)^{\bar{g}}}$ given by $D_1(x + A^g) = (x + B) + (A/B)^{\bar{g}}$ is well defined. D_1' is defined similarly.

- To define δ, we first define a homomorphism $\rho : (A/B)_{\bar{f}} \to B_g/B^f$ given by $x+B \mapsto f(x)+B^f$. It is not clear that the formula we have given makes any sense at all. We will explain. The group $(A/B)_{\bar{f}}$ consists of all those cosets $x + B$ for which the representative x satisfies $f(x) \in B$. Since $\operatorname{Im} f \subseteq \operatorname{Ker} g$, we have that if $x+B$ is an element of $(A/B)_{\bar{f}}$, then $f(x) \in B_g$. Thus ρ maps $(A/B)_{\bar{f}}$ into the desired codomain. To show the map is well defined, suppose $x + B, y + B$ are elements of $(A/B)_{\bar{f}}$ with $x + B = y + B$. Then $x - y \in B$, so $f(x - y) \in B^f$, hence $\rho(x + B) = \rho(y + B)$.

  With ρ well defined, we observe that $(A/B)^{\bar{g}}$ is contained in the kernel of ρ: any element of $(A/B)^{\bar{g}}$ can be written as $g(x) + B$ for some $x \in A$, and we know that $f(g(x)) = 0$, so

$\rho(g(x) + B) = 0 + B^f$. This gives us a well defined homomorphism

$$\delta : \frac{(A/B)_{\bar{f}}}{(A/B)^{\bar{g}}} \to \frac{B_g}{B^f}$$

$$(x + B) + (A/B)^{\bar{g}} \mapsto f(x) + B^f$$

Proposition 2. *The diagram above is exact.*

Proof. I . $\operatorname{Ker} D_1 = \operatorname{Im} D_2$

A typical element of $\operatorname{Im} D_2$ is $x + A^g$ for some $x \in B_f$. Then $D_1(x + A^g) = (x + B) + (A/B)^{\bar{g}}$, which is zero because $x \in B$. Conversely suppose that $x + A^g$ (for $x \in A_f$) is in the kernel of D_1. Then $x + B$ lies in $(A/B)^{\bar{g}}$, so there is some $y \in A$ for which $x + B = g(y) + B$. There is then an element $b \in B$, necessarily in $\operatorname{Ker} f$, for which $x - g(y) = b$. Then $x + A^g = x - g(y) + A^g = b + A^g$, with $b + A^g \in \operatorname{Im} D_2$. The equality $\operatorname{Ker} D_1' = \operatorname{Im} D_2'$ is similar.

II . $\operatorname{Ker} \delta = \operatorname{Im} D_1$

A typical element of $\operatorname{Im} D_1$ is $(x + B) + (A/B)^{\bar{g}}$ with $x \in A_f$. If we apply δ, we get $f(x) + B^f$, which is zero because $f(x) = 0$. Conversely suppose $z = (x + B) + (A/B)^{\bar{g}}$ be in the kernel of δ, where $x + B \in (A/B)_{\bar{f}}$. Then $f(x) + B^f = 0 + B^f$, so there exists $b \in B$ such that $f(x) = f(b)$. Then $x + B = x - b + B$, so $(x + B) + (A/B)^{\bar{g}} = (x - b + B) + (A/B)^{\bar{g}}$, with $x - b \in A_f$. Thus $z \in \operatorname{Im} D_1$. The equality $\operatorname{Ker} \delta' = \operatorname{Im} D_1'$ is similar.

III . $\operatorname{Ker} D_2' = \operatorname{Im} \delta$

Let $(x + B) + (A/B)^{\bar{g}}$ be an element of $\frac{(A/B)_{\bar{f}}}{(A/B)^{\bar{g}}}$. If we apply δ, we get $f(x) + B^f$, and applying D_2' to this gets us $f(x) + A^f$, which is obviously zero. Conversely suppose $x + B^f$, for $x \in B_g$, lies in the kernel of D_2'. Then $x \in A^f$, so there is some $y \in A$ with $x = f(y)$. Since $x \in B$, the coset $y + B$ lies in $(A/B)_{\bar{f}}$, with

$$\delta((y + B) + (A/B)^{\bar{g}}) = f(y) + B^f = x + B^f$$

This shows that $x + B^f$ lies in the image of D_2. The equality $\operatorname{Ker} D_2 = \operatorname{Im} \delta'$ is similar.

□

Let C be the quotient A/B. From the previous proposition, we see that if two of the three Herbrand quotients $Q(A), Q(B), Q(C)$ are defined, then so is the third. For example, suppose $Q(A)$ and $Q(B)$ are defined. Already four of the six objects in the diagram are finite groups. The image of D_1 is finite, and if we take the group $\frac{(A/B)_{\bar{f}}}{(A/B)^{\bar{g}}}$ modulo this image, the resulting quotient is by exactness isomorphic to a subgroup of B_g/B^f, also finite. Hence $\frac{(A/B)_{\bar{f}}}{(A/B)^{\bar{g}}}$ is finite, and similarly one can argue that $\frac{(A/B)_{\bar{g}}}{(A/B)^{\bar{f}}}$ is finite.

Proposition 3. *We have the identity*

$$Q(A) = Q(B)Q(A/B)$$

whenever these Herbrand quotients are defined.

Proof. The cardinality of any object in the diagram is equal to the cardinality of the image of the map preceding it, multiplied by the cardinality of the image of the map following it. For example, A_f/A^g modulo the kernel of D_1 is isomorphic to the image of D_1, so

$$|A_f/A^g| = |\operatorname{Ker} D_1| \cdot |\operatorname{Im} D_1| = |\operatorname{Im} D_2| \cdot |\operatorname{Im} D_1|$$

Therefore,

$$Q(B)Q(A/C) = \frac{|B_f/B^g|}{|B_g/B^f|} \cdot \frac{|\frac{(A/B)_{\bar{f}}}{(A/B)^{\bar{g}}}|}{|\frac{(A/B)_{\bar{g}}}{(A/B)^{\bar{f}}}|} = \frac{|\operatorname{Im}\delta'| \cdot |\operatorname{Im} D_2|}{|\operatorname{Im}\delta| \cdot |\operatorname{Im} D_2'|} \cdot \frac{|\operatorname{Im} D_1| \cdot |\operatorname{Im}\delta|}{|\operatorname{Im} D_1'| \cdot |\operatorname{Im}\delta'|}$$

$$= \frac{|\operatorname{Im} D_2| \cdot |\operatorname{Im} D_1|}{|\operatorname{Im} D_2'| \cdot |\operatorname{Im} D_1'|} = \frac{|A_f/A^g|}{|A_g/A^f|} = Q(A)$$

□

3.2 The first two cohomology groups

Let G be a finite multiplicative group with identity $1_G = 1$, and R a ring. We recall the definition of the group ring $R[G]$. As an abelian group, $R[G]$ is the product $\prod_{g\in G} R$, where an element is written as a formal sum $\sum_{g\in G} gr_g$ for $r_g \in R$. This becomes a ring when we define multiplication by

$$(\sum_{g\in G} gr_g)(\sum_{h\in G} hs_h) = \sum_{g,h} ghr_g s_h$$

Suppose A is an additive abelian group. If A is a module over the ring $\mathbb{Z}[G]$, then we call A a G-module rather than a $\mathbb{Z}[G]$ module. A G-module structure on A can equivalently be described as a group action of G on A for which $g(x+y) = gx + gy$ for any $g \in G$ and $x, y \in A$.

Suppose A is a G-module. We define the trace homomorphism $\operatorname{Tr}_G : A \to A$ by

$$a \mapsto \sum_{g\in G} ga$$

and we also let A^G be the submodule of A consisting of all $a \in A$ which are fixed by every $g \in G$. Check that $\operatorname{Tr}_G(ga) = g \operatorname{Tr}_G(a) = \operatorname{Tr}_G(a)$ for any $g \in G, a \in A$. It is easy to see that $\operatorname{Tr}_G A \subseteq A^G$,

so we may define the *cohomology group*

$$H_0(G, A) = \frac{A^G}{\mathrm{Tr}_G A}$$

Also, let I_G be the additive subgroup of $\mathbb{Z}[G]$ generated by $1 - g : g \in G$. This is actually an ideal, since for $g, h \in G$ we have

$$h(1 - g) = h - hg = (h - 1) + (1 - hg)$$

Therefore $I_G A = \{ga : g \in I_G, a \in A\}$ is a submodule of A, and it furthermore contained in $\mathrm{Ker}\,\mathrm{Tr}_G$, since

$$\mathrm{Tr}_G((1 - g)a) = \mathrm{Tr}_G(a - ga) = \mathrm{Tr}_G(a) - \mathrm{Tr}_G(ga) = 0$$

So we may define the next cohomology group

$$H_1(G, A) = \frac{\mathrm{Ker}\,\mathrm{Tr}_G}{I_G A}$$

Although we have taken quotients of submodules, we really only care about $H_0(G, A)$ and $H_1(G, A)$ as abelian groups (and, more specifically, we will be interested in their cardinalities). There are higher cohomology groups $H_2(G, A), H_3(G, A)$ etc. but they are more complicated to define and work with, and we shall only require the first two. See the appendix for a more categorical treatment of the groups H_0 and H_1.

Suppose A is a direct sum $\sum_{i=1}^{s} A_i$. We say that G acts **semilocally** on A if G permutes the A_i transitively. In that case, define the decomposition group $G_j = \{\tau \in G : \tau A_j = A_j\}$. If $\phi A_j = A_k$, then the decomposition group of A_k is $\phi G_j \phi^{-1}$, so we can stick with just one decomposition group, say G_1. Write G as a disjoint union of left cosets

$$G = \bigcup_{i=1} \sigma_i G_1$$

and arrange the indices so that $\sigma_k A_1 = A_k$. Therefore, every element $a \in A$ can be uniquely expressed as $\sigma_1(a_1') + \cdots + \sigma_s(a_s')$ for $a_i' \in A_1$.

Lemma 4. *The projection $\pi : A \to A_1$ induces an isomorphism*

$$H^0(G, A) \cong H^0(G_1, A_1)$$

Proof. We first claim that

$$A^G = \{\sigma_1(a_1) + \cdots + \sigma_s(a_1) : a_1 \in A_1^{G_1}\}$$

First suppose $\alpha \in A^G$. Write α as $a_1 + \cdots + a_s$, where $a_k \in A_k$. If $\phi \in G_1$, then $\phi(a_1) \in A_1$, and $\phi(a_k)$ is not in A_1 unless it is zero, for otherwise $a_k \in \phi^{-1}A_1 = A_1$, whose intersection with A_k is trivial. Thus $\phi(a_1) + \cdots + \phi(a_s) = \phi(\alpha) = \alpha$, and by unique representation we get $\phi(a_1) = a_1$. Since ϕ was arbitrary, we have $a_1 \in A_1^{G_1}$.

Now also $\alpha = \sigma_1(a_1') + \cdots + \sigma_s(a_s')$, where $a_k' = \sigma_k^{-1}(a_k)$ (we know $a_1 = \sigma_1(a_1') = a_1'$). For a fixed k, apply σ_k^{-1} to α to get $a_k' + \sum_{j \neq k} \sigma_k^{-1}\sigma_j(a_j') = \sigma_k^{-1}\alpha = \alpha$, with none of the $\sigma_k^{-1}\sigma_j(a_j') \in A_1$ unless $a_j' = 0$ (otherwise $\sigma_k^{-1}\sigma_j G_1 = G_1$, so $j = k$). Hence by unique representation we obtain $a_1 = a_k'$, so $a = \sigma_1(a_1) + \cdots + \sigma_s(a_1)$, with $a_1 \in A_1^{G_1}$ as required.

Conversely suppose $\alpha \in A$ takes the form $\sigma_1(a_1) + \cdots + \sigma_s(a_1)$, with $a_1 \in A_1^{G_1}$. Then $\sigma_k(a_1) \in \sigma_k(A_1^{G_1}) = A_k^{G_k}$. Now if $\phi \in G$, then ϕ permutes the A_k, sending A_k to, say, $A_{\phi(k)}$. It follows that for each k, we have

$$\phi\sigma_k A_1 = \phi A_k = A_{\phi(k)} = \sigma_{\phi(k)} A_1$$

so $\sigma_{\phi(k)}^{-1}\phi\sigma_k \in G_1$. Hence $\sigma_{\phi(k)}^{-1}\phi\sigma_k(a_1) = a_1$, which implies $\phi\sigma_k(a_1) = \sigma_{\phi(k)}(a_1)$. But then

$$\phi(\alpha) = \phi\sigma_1(a_1) + \cdots + \phi\sigma_s(a_1) = \sigma_{\phi(1)}(a_1) + \cdots + \sigma_{\phi(s)}(a_1) = \alpha$$

Now that we have proven the first claim, we see that restriction to A^G of the projection map $A \to A_1$, given by (for $a_1 \in A_1^{G_1}$)

$$\sigma_1(a_1) + \cdots + \sigma_s(a_1) \mapsto \sigma_1 a_1 = a_1$$

is an isomorphism. So we only have to show that under this mapping, $\mathrm{Tr}_G(A)$ is mapped onto $\mathrm{Tr}_{G_1}(A_1)$. This is done if we can show that

$$\mathrm{Tr}_G(A) = \{\sum_{i=1}^{s} \mathrm{Tr}_{G_1}(a_1) : a_1 \in A_1\}$$

Remember that $\sigma_i, i = 1, ..., s$ is a set of left coset representatives for G_1 in G. For the inclusion, '$\supseteq$', we have

$$\sum_{i=1}^{s} \sigma_i \,\mathrm{Tr}_{G_1}(a_1) = \sum_{i=1}^{s} \sigma_i \sum_{\tau \in G_1} \tau(a_1) = \sum_{\phi \in G} \phi a_1 = \mathrm{Tr}_G(a_1) \in \mathrm{Tr}_G(A)$$

Conversely let us take the trace of an element $\sum_{j=1}^{s} \sigma_j(a_j)$ for $a_j \in A_1$. Define $b = \sum_{j=1}^{s} \mathrm{Tr}_{G_1}(a_j) \in A_1$.

Using the same argument as in the first inclusion, we have

$$\mathrm{Tr}_G(\sum_{j=1}^{s}\sigma_j(a_j)) = \sum_{j=1}^{s}\mathrm{Tr}_G\,\sigma_j(a_j) = \sum_{j=1}^{s}\sum_{i=1}^{s}\sigma_i\,\mathrm{Tr}_{G_1}(a_j)$$

$$= \sum_{i=1}^{s}\sigma_i\sum_{j=1}^{s}\mathrm{Tr}_{G_1}(a_j) = \sum_{i=1}^{s}\sigma_i(b)$$

□

Lemma 5. *There is an isomorphism*

$$H_1(G,A) \cong H_1(G_1,A_1)$$

Proof. At the end of the last proof, we showed that for any $\alpha \in A$, written as $\sigma_1(a_1') + \cdots + \sigma_s(a_s')$ for uniquely determined $a_i' \in A_1$,

$$\mathrm{Tr}_G(\alpha) = \sum_{i=1}^{s}\sigma_i\,\mathrm{Tr}_{G_1}(a_1' + \cdots + a_s')$$

Thus $\mathrm{Tr}_G(\alpha) = 0$ if and only if $\mathrm{Tr}_{G_1}(a_1' + \cdots + a_s') = 0$. Thus

$$\alpha \mapsto a_1' + \cdots + a_s'$$

maps $\mathrm{Ker}\,\mathrm{Tr}_G$ onto $\mathrm{Ker}\,\mathrm{Tr}_{G_1}$ (surjectivity is obvious). This mapping, λ, induces the desired isomorphism, provided we can show that $I_G A$ is mapped onto $I_{G_1}(A_1)$.

First, to show $\lambda I_G A \subseteq I_{G_1}A_1$, it suffices to show that if $\tau \in G$ and $\alpha \in A$, then $\lambda(\tau(\alpha) - \alpha) \in I_{G_1}A_1$. So fix τ and α. Since $\sigma_i, i = 1, ...s$ are a set of left coset representatives for G_1 in G, there is for each j a unique index $\pi(j)$ and a unique element $\tau_{\pi(j)} \in G_1$ such that $\tau\sigma = \sigma_{\pi(j)}\tau_{\pi(j)}$. In fact, we can take π as a permutation of $1, ..., s$. Thus

$$\tau(\alpha) = \sum_{i=1}^{s}\tau\sigma_i(a_i') = \sum_{i=1}^{s}\sigma_{\pi(i)}\tau_{\pi(i)}(a_i')$$

so $\lambda(\tau(\alpha)) = \sum_{i=1}^{s}\tau_{\pi(i)}a_i'$. But then

$$\lambda(\tau(\alpha) - \alpha) = \sum_{i=1}^{s}\tau_{\pi(i)}(a_i') - a_i' \in I_{G_1}A_1$$

For the converse, suppose that $\lambda(\alpha) = a_1' + \cdots + a_s'$ is equal to some $b \in I_{G_1}A_1$. Now $I_{G_1}A_1 \subseteq I_G A$,

so $b \in I_G A$, and

$$\alpha = b + \alpha - b = b + \sum_{i=1}^{s} \sigma_i(a_i') - a_i \in I_G A$$

□

3.3 Applying the above machinery

For most of the rest of this chapter, G will be a finite cyclic group, in fact the Galois group of a cyclic extension of local or global fields. We will continue to take A as an abelian group with a G-module structure, but will write A multiplicatively. Hopefully the fact that we have written A additively up to this point will not cause any confusion. For example, the trace map

$$Tr_G = g : A \to A, x \mapsto \sum_{i=0}^{N-1} \sigma^i(x)$$

will actually be the norm. If we set $f : A \to A$ by $f(x) = \sigma(x) - x$, then $I_G A$ is exactly the image of f. This is not difficult to see from the identity

$$1 - \sigma^i = (1 - \sigma)(1 + \sigma + \cdots + \sigma^{i-1})$$

Furthermore A^G is exactly the kernel of f, so in the notation of the first section we have

$$H_0(G, A) = A_f / A^g$$

$$H_1(G, A) = A_g / A^f$$

$$Q(A) = \frac{|H_0(G, A)|}{|H_1(G, A)|}$$

We may deal with Herbrand quotients involving different groups, so we will write $Q(G, A)$ instead of just $Q(A)$. If $\Phi : A \to A'$ is an isomorphism of abelian groups, then there is an obvious induced G-module structure on A' for which the cohomlogy groups $H_i(G, A), H_i(G, A')$ are isomorphic and $Q(G, A) = Q(G, A')$. Another way of saying this is that an isomorphism of G-modules induces an isomorphism of cohomology groups and equality of Herbrand quotients.

Lemma 6. *If G acts trivially on $\mathbb{Z}$, then $Q(G, \mathbb{Z}) = N$, the order of G.*

Proof. Just check that $A_f = \mathbb{Z}, A^g = N\mathbb{Z}$, and $A_g = A^f = 0$.

□

Examples:

- Let L/K be a cyclic extension of global fields. The Galois group $G = \mathrm{Gal}(L/K)$ acts on L and gives L^* the structure of a G-module. Let σ generate G. Now $H_1(G, L^*)$ is equal to the group of $\frac{x}{\sigma(x)} : x \in K^*$ modulo the group of $x \in L^*$ with norm 1. Hilbert's theorem 90 just asserts that $H_1(G, L^*)$ is the trivial group.
- If L and K are global fields, then G acts on the ideles $\mathbb{I}_L$, and therefore the idele class group $C_L = \mathbb{I}_L/L^*$, in a natural way. There is a natural injection $C_K \to C_L$ for which one obtains

  $$|H_1(G, C_L)| = [C_K : N_{L/K}(C_L)] = [\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)]$$

  Work out the details as an exercise.
- If L and K are p-adic fields, then $\mathcal{O}_L$ has a G-module structure, and

  $$H_0(G, \mathcal{O}_L) = [\mathcal{O}_K : N_{L/K}(\mathcal{O}_L)]$$

3.4 The local norm index

Let $k \subseteq K$ be finite extensions of $\mathbb{Q}_p$, with $n = [K : k]$. Suppose K/k is cyclic with Galois group G. We have the cohomology groups $H_0(G, K^*) = k^*/N_{K/k}(K^*)$ and $H_1(G, K^*)$, the group of norm 1 elements modded out by the set of $\sigma(x)/x$, which is trivial by Hilbert's Theorem 90. Thus

$$Q(G, K^*) = \frac{|H_0(G, K^*)|}{|H_1(G, K^*)|} = [k^* : N_{K/k}(K^*)]$$

The maps $x \mapsto \sigma(x)/x$ and $N_{K/k}$ send U_K to itself, so we can discuss the Herbrand quotients $Q(U_K)$ and $Q(K^*/U_K)$.

Proposition 7. $Q(U_K) = 1$

Proof. The logarithm and the exponential functions may both be defined for p-adic fields by their power series. These series do not always converge, but exp will map sufficiently small open additive subgroups homeomorphically and isomorphically onto small open multiplicative subgroups, the inverse mapping being the logarithm. See the appendix for more details.

Any finite Galois extension of fields F/E has a *normal basis*, i.e. a basis $w_\gamma : \gamma \in \mathrm{Gal}(F/E)$ for which $\phi w_\gamma = w_{\phi\gamma}$. Let $w_1, ..., w_N$ be such a basis for K/k. Multiply these elements by sufficiently high powers of p so that the elements of subgroup

$$M = \mathcal{O}_k w_1 + \cdots + \mathcal{O}_k w_N$$

are all very small, p-adically speaking. The group G acts semilocally on M with trivial decomposition group, so $Q(G, M) = 1$. If M is chosen very small, exp gives an isomorphism and homeomor-

phism from M into the unit group U_K. Since $\exp\phi(x) = \phi\exp x$ by continuity, the induced action of G on $\exp M$ is the same as that obtained by restricting the regular action on K^*. Thus

$$Q(U_K) = Q(\exp M)\cdot Q(U_K/\exp M)$$

where $Q(\exp M) = Q(M) = 1$. Also since M is open, so is $\exp M$, so by compactness $\exp M$ is of finite index in U_K. Therefore $Q(U_K/\exp M) = 1$.

□

Theorem 8.

$$[k^* : N_{K/k}(K^*)] = [K : k]$$

and

$$[U_k : N_{K/k}(U_K)] = e(K/k)$$

Proof. The first result follows directly from the previous proposition. Already we mentioned that $Q(K^*) = [k^* : N_{K/k}(K^*)]$. Also, K^*/U_K is isomorphic to $\mathbb{Z}$, with G inducing the trivial action on the quotient. Therefore

$$[K : k] = |G| = Q(K^*/U_K) = \frac{Q(K^*)}{Q(U_K)} = [k^* : N_{K/k}(K^*)]$$

For the second assertion, we again use the fact that $Q(U_K) = 1$. Let $e = e(K/k)$. We have

$$[U_k : N_{K/k}(U_K)] = |H_0(G, U_K)| = |H_1(G, U_K)|$$

By Hilbert's Theorem 90 and the fact that automorphisms preserve absolute values, it is not difficult to see that $|H_1(G, U_K)| = [K^{*g} : U_K^g]$, these latter two objects respectively denoting the images of K^* and U_K under the map $g = 1 - \sigma$. Actually, $U_K^g = (k^*U_K)^g$, so by the identity $[A : B] = [A^f : B^f][A_f : B_f]$ we have

$$|H_1(G, U_K)| = \frac{[K^* : k^*U_K]}{[K_g^* : (k^*U_K)_g]}$$

The denominator of this fraction is 1: both K_g^* and $(k^*U_K)_g$ are equal to k^*. If $\mathscr{P}, \mathfrak{p}$ denote the respective primes of K, k, then $\mathrm{ord}_{\mathfrak{p}}(x) = e\,\mathrm{ord}_{\mathscr{P}}(x)$ for any $x \in k^*$, so it is not difficult to see that the kernel of the composition

$$K^* \xrightarrow{\mathrm{ord}_{\mathscr{P}}} \mathbb{Z} \to \mathbb{Z}/e\mathbb{Z}$$

is exactly k^*U_K.

□

Corollary 9. *If K/k is abelian, then*

$$[k^* : N_{K/k}(K^*)] \leq [K : k]$$

and

$$[U_k : N_{K/k}(U_K)] \leq e(K/k)$$

Proof. Actually, equality still holds even when K/k is abelian and not cyclic. But it will disrupt the elegance of our progression to prove this before we have developed local class field theory. In the meantime, we can quickly prove this lesser result as follows:

There exists a tower of intermediate fields

$$k \subseteq E \subseteq E' \subseteq \cdots \subseteq K$$

where the extensions $E/k, E'/E$ etc. are cyclic. By induction, $[E^* : N_{K/E}(K^*)] \leq [K : E]$. By the identity $[A : B] = [A^f : B^f][A_f : B_f]$ introduced in the beginning of this section, we have

$$[N_{E/k}(E^*) : N_{E/k} \circ N_{K/E}(K^*)] \leq [E^* : N_{K/E}(K^*)]$$

Now we use the theorem:

$$[k^* : N_{K/k}(K^*)] = [k^* : N_{E/k}(E^*)][N_{E/k}(E^*) : N_{E/k} \circ N_{K/E}(K^*)]$$

$$\leq [k^* : N_{E/k}(E^*)][E^* : N_{K/E}(K^*)] \leq [k^* : N_{E/k}(E^*)][K : E]$$

$$= [E : k][K : E] = [K : k]$$

The argument for the unit group is identical.

□

While we are on the subject of local indices, let us prove another result which will be needed later in the proof of the existence of class fields. Take $k, \mathfrak{p}$ etc. as we have above, and let $\mathcal{O}, U$ be respectively the integers and units of this field. Let π be a uniformizer for k. Multiplication by π^i gives an isomorphism of $\mathcal{O}$-modules $\mathcal{O}/\mathfrak{p} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$. The multiplicative analogue of the powers $\mathfrak{p}_i$ are the groups $1 + \pi^i\mathcal{O}$. Let $U_i = 1 + \pi^i\mathcal{O}$ for $i \geq 1$. Reduction modulo π induces an abelian group epimorphism $U \to (O/\mathfrak{p})^*$ whose kernel is U_1. For $i \geq 1$, the map $x \mapsto 1 + x$ gives an isomorphism $\mathfrak{p}^i/\mathfrak{p}^{i+1} \to U_i/U_{i+1}$.

Therefore the cardinality of U_i/U_{i+1} is $p^{f(\mathfrak{p}/p)}$. Notice that

$$||\pi||_{\mathfrak{p}} = |N_{k/\mathbb{Q}_p}(\pi)|_p = |p^{f(\mathfrak{p}/p)}|_p = \frac{1}{\mathcal{N}(\mathfrak{p})}$$

Fix an $n \in \mathbb{N}$, and let $U^n = \{x^n : x \in U\}$. The corollary to Hensel's lemma mentioned in the introduction shows that for sufficiently large i, $U_i \subseteq U^n$. Thus $[U : U^n]$ is always finite. We will now determine this index.

Theorem 10. *Let W be the group of nth roots of unity in K.*

$$[U : U^n] = \frac{|W|}{||n||_{\mathfrak{p}}}$$

$$[k^* : k^{*n}] = \frac{n}{||n||_{\mathfrak{p}}}|W|$$

Proof. Let $s = \operatorname{ord}_{\mathfrak{p}} n$, and take r to be large enough so that:

- $r \geq s + 1$.
- U_r is contained in U^n.
- 1 is the only nth root of unity in U_r.

The first condition ensures that $|n\pi^{r+1}|_p \geq |\pi|_p^{2r}$. Then if $(1 + x\pi^r)$ is any element of U_r, we have

$$(1 + x\pi^r)^n = 1 + nx\pi^r + \cdots \in U_{r+s}$$

This shows that $U^n \subseteq U_{r+s}$. On the other hand U_r, and hence U_{r+s}, is contained in U^n. Thus $U_{r+s} = U_r^n$. Let $f : U \to K$ be the homomorphism $x \mapsto x^n$. Then

$$[U : U_r] = [\operatorname{Im} f : \operatorname{Im} f_{|U_r}][\operatorname{Ker} f : \operatorname{Ker} f_{|U_r}] = [U^n : U_r^n][W : 1] = [U^n : U_{r+s}] \cdot |W|$$

and

$$[U : U^n] = \frac{[U : U_r]}{[U^n : U_r]} = \frac{[U^n : U_{r+s}]}{[U^n : U_r]}|W| = [U_r : U_{r+s}]|W|$$

Since $[U_i : U_{i+1}] = p^{f(\mathfrak{p}/p)}$, we have

$$[U_r : U_{r+s}] = [U_r : U_{r+1}]^s = p^{f(\mathfrak{p}/p)s} = \frac{1}{||\pi||_{\mathfrak{p}}^s} = \frac{1}{||n||_{\mathfrak{p}}}$$

This proves the first assertion. For the second assertion, we need only use the fact that $k^* \cong \mathbb{Z} \times U$ as abelian groups. Then

$$k^*/k^{*n} \cong \frac{\mathbb{Z} \times U}{n\mathbb{Z} \times U^n} \cong \mathbb{Z}/n\mathbb{Z} \times U/U^n$$

□

3.5 The cyclic global norm index equality

In this section L/K is a cyclic extension of number fields, $N = [L : K]$, $G = \mathrm{Gal}(L/K)$. Let S be a finite set of places of K containing all the archimedean ones, and let S_1 be the set of places of L which lie over the places of K. Then $w \in S_1$ implies $\sigma w \in S_1$ for any $\sigma \in G$. Choose $s := |S_1|$ symbols $x_w : w \in S_1$ and let V be the $\mathbb{R}$-vector space having x_w as a basis. If we define

$$\sigma x_w = x_{\sigma w}$$

then we obtain a G-module structure on V. For an element $v = \sum_{w \in S_1} c_w x_w$ (for $c_w \in \mathbb{R}$) in V, the sup norm

$$||v||_\infty = \sup_{w \in S_1} |c_w|$$

induces the product topology on V. It is obvious that $||\sigma v||_\infty = ||v||_\infty$ for $v \in V, \sigma \in G$.

Let M be a full lattice of V. As topological groups,

$$V/M \cong \frac{\bigoplus_w \mathbb{R}}{\bigoplus_w \mathbb{Z}} \cong \bigoplus_w \mathbb{R}/\mathbb{Z}$$

so V/M is compact in the quotient topology. Giving the same topology on V/M is the induced norm

$$||v + M|| = \inf_{m \in M} ||v - m||_\infty$$

Since V/M is a compact metric space, it must be bounded, so there exists $\delta > 0$ such that $||v+M|| < \delta$ for all $v \in V$. But by the definition of the quotient norm, δ has the property for every $v \in V$, there is an $m \in M$ such that $||v - m||_\infty < \delta$.

Proposition 11. *Let M be a full lattice of V which is G-invariant ($\sigma M \subseteq M$ for $\sigma \in G$). There exists a sublattice M' of M such that $[M : M']$ is finite, M' is G-invariant, and there exists a basis $y_w : w \in K_S$ for M' such that*

$$\sigma y_w = y_{\sigma w}$$

Proof. Remember that for a sublattice $M' \subseteq M$, the index $[M : M']$ is finite if and only if M' is of full rank. To say that M is G-invariant means that M inherits the structure of a G-module from V. Let s, N, δ be as above, and for each $v \in S$, fix a place w_v of S_1 lying over v. For w also lying over v, let m_w be the number of $\sigma \in G$ such that $\sigma w_v = w$. Let m be the mimimum of these m_w, and choose $t > \frac{sbN}{m}$.

For each v, we can find a $z_{w_v} \in M$ such that $||t x_{w_v} - z_{w_v}||_\infty < b$. For $w \in S_1$, if we set

$$y_w = \sum_{\sigma w_v = w} \sigma z_{w_v}$$

then for any $\tau \in G$, we have

$$\tau y_w = \sum_{\sigma w_v = w} \tau\sigma z_{w_v} = \sum_{\rho w_v = \tau w} \rho z_{w_v} = y_{\tau w}$$

This shows that $y_w \in M$ has the desired G-module properties. We will be done once we show that the y_w are linearly independent.

Suppose that $\sum_w c_w y_w = 0$ for $c_w \in \mathbb{R}$, not all zero. Then we can arrange that all $|c_w| \leq 1$, with at least one c_w being equal to 1. Let $B_{w_v} = z_{w_v} - t x_{w_v}$, so $||B_{w_v}||_\infty < b$. Then

$$y_w = \sum_{\sigma w_v = w} \sigma(t x_{w_v} + B_{w_v}) = \sum_{\sigma w_v = w} t x_w + \sum_{\sigma w_v = w} \sigma B_{w_v} = t m_w \cdot x_w + B_w$$

where $B_w = \sum_{\sigma w_v = w} \sigma B_{w_v}$, and

$$||B_w||_\infty \leq \sum_{\sigma w_v = w} ||\sigma B_{w_v}||_\infty = \sum_{\sigma w_v = w} ||B_{w_v}||_\infty \leq Nb$$

Now

$$0 = \sum_w c_w y_w = \sum_w c_w (t m_w x_w + B_w) = \sum_w (c_w t m_w) \cdot x_w + B$$

where $B = \sum_w c_w B_w$, so $||B||_\infty \leq s \operatorname{Max}_w |c_w| \cdot \operatorname{Max}_w ||B_w||_\infty \leq sb|G|$. We should have $||B||_\infty = ||\sum_w (c_w t m_w) \cdot x_w||_\infty$. But, letting w_0 be a place such that $c_{w_0} = 1$, we have

$$||\sum_w (c_w t m_w) \cdot x_w||_\infty = \operatorname{Max}_w |c_w t m_w| \geq |c_{w_0} t m_{w_0}| \geq tm > sNb \geq ||B||_\infty$$

a contradiction.

□

Suppose G acts on an abelian group $A = A_1 \oplus \cdots \oplus A_s$, such that $\sigma A_i = A_i$ for all σ and $1 \leq i \leq s$. We have

$$Q(G, A) = Q(G, A_1) Q(G, A/A_1) = Q(G, A_1) Q(G, A_2 \oplus \cdots \oplus A_s)$$

so by induction, we have

$$Q(G, A) = Q(G, A_1) \cdots Q(G, A_s)$$

On the other hand, if G acts semilocally on the A_i, and G_1 is the decomposition group of A_1, then we proved

$$Q(G, A) = Q(G_1, A_1)$$

Let X be the full lattice of V with basis $x_w : w \in S_1$. For each $v \in S$, choose a place w_v lying over it. We can write X as a direct sum

$$X = \bigoplus_{v \in S} \bigoplus_{w|v} \mathbb{Z} x_w$$

and so

$$Q(G, X) = \prod_{v \in S} Q(G, \bigoplus_{w|v} \mathbb{Z} x_w) = \prod_{v \in S} Q(G_v, \mathbb{Z} x_{w_v})$$

where G_v is the decomposition group of w_v (actually, of any $w \mid v$). Since G_v acts trivially on the cyclic group $\mathbb{Z} x_{w_v}$, we have $Q(G_v, \mathbb{Z} w_v) = |G_v|$.

Corollary 12. *Let M be a full lattice in V which is G-invariant. Then*

$$Q(G, M) = \prod_{v \in S} |G_v|$$

Proof. Find a sublattice M' of M satisfying the proposition. Clearly M' is G-isomorphic to X, and the quotient M/M' is finite, so we have

$$Q(G, M) = Q(G, M') = Q(G, X) = \prod_{v \in S} |G_v|$$

□

We can now calculate the Herbrand quotient of the S_1-units L_{S_1}. Remember that S_1-units are those $x \in L^*$ which are units outside of S_1.

Proposition 13. $Q(G, L_{S_1}) = \frac{1}{N} \prod_{v \in S} |G_v|$

Proof. The image of L_{S_1} under the log mapping $\log : L_{S_1} \to V$

$$\xi \mapsto \sum_w \log ||\xi||_w x_w$$

is a subgroup of V contained in the $s-1$ dimensional subspace

$$H = \{\sum_w c_w x_w \in V : \sum_w c_w = 0\}$$

and the Dirichlet unit theorem tells us that this image is a lattice of rank $s-1$, and that the kernel is the group J of roots of unity in L. Thus $Q(G, J) = 1$. Notice that $|\xi|_{\sigma^{-1} w} = |\sigma \xi|_w$ for any

$\xi \in L_{S_1}$. This implies

$$\log(\sigma\xi) = \sum_w |\sigma\xi|_w x_w = \sum_w |\xi|_{\sigma^{-1}w} x_w$$

$$= \sum_w |\xi|_w x_{\sigma w} = \sigma \log(\xi)$$

so log is a G-module homomorphism, and hence induces a G-module isomorphism $L_{S_1}/J \cong \log L_{S_1}$. Thus

$$Q(G, L_{S_1}) = Q(G, L_{S_1}/J) = Q(G, \log L_{S_1})$$

Now $x_0 := \sum_w x_w$ is linearly independent of $\log L_{S_1}$, since it does not lie in H. Thus $M = \log L_{S_1} + \mathbb{Z}x_0$ is the direct sum of $\log L_{S_1}$ and $\mathbb{Z}x_0$, and is also G-invariant. Its two direct summands are also G-invariant, so

$$Q(G, M) = Q(G, \log L_{S_1}) Q(G, \mathbb{Z}x_0) = Q(G, L_{S_1}) \cdot N$$

We calculated $Q(G, M)$ in the corollary.

□

We're about to prove the global norm index equality for cyclic extensions. We have

$$Q(C_L) = \frac{[C_K : N_{L/K}(C_L)]}{|H_1(G, C_L)|}$$

The significance of the group $H_1(G, C_L)$ will not be made apparent in these notes, but we will show as a byproduct of the global cyclic norm equality that it is trivial.

As a final preliminary, suppose A is a G-module which is direct product of abelian groups $A_1 \times A_2 \times A_3 \times \cdots$, with $\sigma A_i = A_i$ for all i. Suppose that $H_0(G, A_i)$ is trivial for all i. One can then prove that $H_0(G, A)$ also trivial. Just use the definition of H_0. Similarly if each $H_1(G, A_i)$ is the trivial group, then so is $H_1(G, A)$.

Theorem 14. *(Global cyclic norm index equality) For L/K cyclic,*

$$[\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)] = [L : K]$$

and

$$|H_1(G, C_L)| = 1$$

Proof. Let S_1 be a finite set of places of L which contain all the archimedean ones, all those which are ramified in L/K, and enough places so that $\mathbb{I}_L = L^* \mathbb{I}_L^{S_1}$. Also, complete S_1 in the sense that if $w \in S_1$ lies over a place v of K, so does σw for $\sigma \in G$. Then let S be the set of places of K over

which the places of S_1 lie. We can write $\mathbb{I}_L^{S_1}$ as a direct product

$$B \times A$$

where

$$B = \prod_{v \in S} \prod_{w|v} L_w^*, A = \prod_{w \nmid v} \prod_{w|v} \mathcal{O}_w^*$$

so $Q(G, \mathbb{I}_L^{S_1}) = Q(G, A)Q(G, B)$. Now A is the direct product of $A_v = \prod_{w|v} \mathcal{O}_w^*$. The decomposition group G_v is the Galois group of L_{w_v}/K_v. Since G acts on the components of A_v semilocally, we have

$$H_0(G, A_v) = H_0(G_v, \mathcal{O}_{w_v}^*) = 1$$

and

$$H_1(G, A_v) = H_1(G_1, \mathcal{O}_{w_v}^*) = 1$$

by the local norm index computations. By the remark just before this theorem, this implies that $Q(G, A) = 1$. On the other hand, we can compute

$$Q(G, B) = \prod_v Q(G, \prod_{w|v} L_w^*) = \prod_v Q(G_v, L_{w_v}) = \prod_v |G_v|$$

again a local computation from section 3. Now we use the computation of $Q(G, L_{S_1})$ to get

$$[L : K] = \frac{Q(G, \mathbb{I}_L^{S_1})}{Q(G, L_{S_1})} = Q(G, \mathbb{I}_L^{S_1}/L_{S_1}) = Q(G, K^* \mathbb{I}_L^{S_1}/K^*)$$

$$= Q(G, \mathbb{I}_L/K^*) = Q(C_L)$$

We used the fact that the inclusion $\mathbb{I}_L^{S_1} \subseteq K^* \mathbb{I}_L^{S_1}$ induces an isomorphism of G-modules $\mathbb{I}_L^{S_1}/L_{S_1} \cong K^* \mathbb{I}_L^{S_1}/K^*$. Thus

$$[L : K] = \frac{[C_K : N_{L/K}(C_L)]}{|H_1(G, C_L)|}$$

Since $[C_K : N_{L/K}(C_L)] \leq [L : K]$ by the global norm index inequality, we must have equality, and this implies $H_1(G, C_L)$ is trivial.

□

Corollary 15. *Let L/K be cyclic of degree > 1. Then infinitely many primes of K do not split completely in L.*

Proof. Let $\alpha \in \mathbb{I}_K$. If the set T of places of K which do not split completely is finite, then by the weak approximation theorem we can find an $x \in K^*$ for which $x\alpha_v - 1$ is very small for $v \in T$, say

small enough so that $x\alpha_v$ is a local norm in K_v. For all $v \notin T$, $x\alpha_v$ is already a local norm, because $K_w = K_v$ for $w \mid v$. Thus $x\alpha \in N_{L/K}(\mathbb{I}_L)$. This shows that $\mathbb{I}_K = K^* N_{L/K}(\mathbb{I}_L)$, so

$$[L : K] = [\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)] = 1$$

□

4 The Law of Artin Reciprocity

The original approach to global class field theory involved looking at *generalized ideal class groups*, which we will define below. Later, Chavalley introduced the ideles to simplify the global results, and to tie local and global class field theory together. Analogous to ideal class groups are *idele class groups*, which we will also define.

The idelic and idealic approaches to class field theory are equivalent. But there are advantages to each approach. Ideals are really the more natural way to approach the classical problem of describing, via congruence conditions, how prime ideals decompose in a given abelian extension. But for the classification of abelian extensions, the treatment of infinite Galois extensions, and the development of local class field theory, the idelic approach gives cleaner results.

Let L/K be abelian, and $\mathfrak{p}$ a prime of K which is unramified in L. We know that there exists a unique $\sigma \in \mathrm{Gal}(L/K)$ with the property that

$$\sigma x \equiv x^{\mathcal{N}\mathfrak{p}} \pmod{\mathscr{P}}$$

for any $x \in \mathcal{O}_L$ and any prime $\mathscr{P}$ of L lying over $\mathfrak{p}$. This element σ is called the Frobenius element at $\mathfrak{p}$, and will be denoted by $(\mathfrak{p}, L/K)$. The map $(-, L/K)$, defined on unramified primes of K, extends by multiplicativity to a homomorphism on the group of fractional ideals of K which are relatively prime to the discriminant:

$$(\mathfrak{a}, L/K) = \prod_{\mathfrak{p}} (\mathfrak{p}, L/K)^{\mathrm{ord}_{\mathfrak{p}}\, \mathfrak{a}}$$

We call this homomorphism the **Artin map** on *ideals*.

Proposition 1. *(Properties of the Artin map)*

(i) If σ is an embedding of L into $\overline{\mathbb{Q}}$ (not necessarily the identity on K), then

$$(\sigma\mathfrak{a}, \sigma L/\sigma K) = \sigma(\mathfrak{a}, L/K)\sigma^{-1}$$

(ii) If L' is an abelian extension of K containing L, then the restriction of $(\mathfrak{a}, L'/K)$ to L is $(\mathfrak{a}, L/K)$. This is known as the ***consistency property****.*

(iii) If E is a finite extension of K, then LE/E is abelian. If $\mathfrak{b}$ is a fractional ideal of E which is relatively prime to the discriminant of L/K, then the restriction of $(\mathfrak{b}, LE/E)$ to L is $(N_{E/K}(\mathfrak{b}), L/K)$.

(iv) If E is an intermediate field of L/K, and $\mathfrak{b}$ is a fractional ideal of E which is relatively

prime to the discriminant of L/K, then

$$(\mathfrak{b}, L/E) = (N_{E/K}(\mathfrak{b}), L/K)$$

Proof. Since the Artin map is a homomorphism, it is sufficient to check everything when $\mathfrak{a}$ is a prime ideal. An embedding such as σ preserves the relevant algebraic structures, for example $\sigma\mathcal{O}_K$ is the ring of integers of σK, and $\sigma\mathcal{O}_L$ is the integral closure of $\sigma\mathcal{O}_K$ in σL. So (i) is just a definition chase.

For (ii), let $\mathscr{P}' \mid \mathscr{P} \mid \mathfrak{p}$ be primes of L', L, K respectively, and $\tau = (\mathfrak{p}, L'/K) \in \mathrm{Gal}(L'/K)$. If $x \in \mathcal{O}_L \subseteq \mathcal{O}_{L'}$, then τ has the effect

$$\tau x \equiv x^{\mathcal{N}\mathfrak{p}} \pmod{\mathscr{P}'}$$

So $\tau x - x^{\mathcal{N}\mathfrak{p}} \in \mathscr{P}' \cap \mathcal{O}_L = \mathscr{P}$. This means that the restriction of τ to L does what is required. By uniqueness, $\tau_{|L} = (\mathfrak{p}, L/K)$.

Now let $\mathfrak{P}$ be a prime of E, relatively prime to the discriminant of L/K, so if $\mathfrak{P}$ lies over the prime $\mathfrak{p}$ in K, then $\mathfrak{p}$ is unramified in L. Let $f = f(\mathfrak{P}/\mathfrak{p})$, $\mathcal{P}$ a prime of LE lying over $\mathfrak{P}$, and $\mathscr{P} = \mathcal{P} \cap \mathcal{O}_L$. Finally, let $\tau = (\mathfrak{P}, LE/E)$. Now

$$\phi := (N_{E/K}(\mathfrak{P}), L/K) = (\mathfrak{p}^f, L/K) = (\mathfrak{p}, L/K)^f$$

has the effect

$$\phi(x) \equiv x^{\mathcal{N}(\mathfrak{p})f} \pmod{\mathscr{P}}$$

for any $x \in \mathcal{O}_L$. But also for $x \in \mathcal{O}_L \subseteq \mathcal{O}_{LE}$, we have

$$\tau x - x^{\mathcal{N}(\mathfrak{P})} \in \mathcal{P} \cap \mathcal{O}_L = \mathscr{P}$$

with $\mathcal{N}(\mathfrak{P}) = \mathcal{N}(\mathfrak{p})f$. Thus $\tau_{|L}$ has the same effect as ϕ on L. Combining the uniqueness of τ with the fact that any element of $\mathrm{Gal}(LE/E)$ is completely determined by its effect on L gives us (iii).

(iv) is just a special case of (iii).

□

As a consequence of the global norm index equality, we can prove the surjectivity of this map.

Theorem 2. *Let S be a finite set of prime ideals of K containing all those which ramify in L, and $I(S)$ the group of fractional ideals of K relatively prime to S. Then the restriction of the Artin map to $I(S)$:*

$$(-, L/K) : I(S) \to \mathrm{Gal}(L/K)$$

is surjective.

Proof. Suppose the Artin map is not surjective. Let E be the fixed field of the image of $(-, L/K)$. Then E/K is abelian of degree > 1, so we can find an intermediate field $E_1 \subseteq E$ such that E_1/K is cyclic of degree > 1. If $\mathfrak{p}$ is a prime of K, not in S, then $(\mathfrak{p}, E_1/K)$ is the restriction of $(\mathfrak{p}, L/K)$ to E_1. But $(\mathfrak{p}, L/K) \in \mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/E_1)$, so $(\mathfrak{p}, E_1/K) = 1$.

This shows that for $\mathfrak{p} \notin S$, the inertia degree of $\mathfrak{p}$ in E_1 is 1. Thus almost all primes of K split completely in E_1. But this contradicts 3, Theorem 19. □

One of the main goals in this chapter is to prove the existence of a similar homomorphism, also called the Artin map, defined on the ideles. A natural way of doing so is to introduce the language of cycles.

4.1 Cycles

First, we introduce the language of cycles. By a **cycle** $\mathfrak{m}$ of K we mean a sequence of nonnegative integers $\mathfrak{m}(v)$, one for each place of K, such that:

1. $\mathfrak{m}(v) = 0$ for almost all v.
2. $\mathfrak{m}(v) = 0$ or 1 when v is real.
3. $\mathfrak{m}(v) = 0$ when v is complex.

Another cycle $\mathfrak{c}$ is said to *divide* $\mathfrak{m}$ if $\mathfrak{c}(v) \leq \mathfrak{m}(v)$ for all v. A place v divides $\mathfrak{m}$ if $\mathfrak{m}(v) \geq 1$. A fractional ideal $\mathfrak{a}$ is said to be relatively prime to $\mathfrak{m}$ if $\mathrm{ord}_v(\mathfrak{a}) = 0$ whenever $\mathfrak{m}(v) \geq 1$. The meaning of other statements involving divisibility, for example two cycles being relatively prime, is obvious. Given $\mathfrak{m}$, we define

$$H_{\mathfrak{m}} = \prod_{\substack{v|\mathfrak{m} \\ v<\infty}} 1 + \mathfrak{p}_v^{\mathfrak{m}(v)} \prod_{v\nmid\mathfrak{m}}{}' K_v^* \prod_{\substack{v|\mathfrak{m} \\ v|\infty}} K_v^\circ$$

which is a subgroup of the ideles. Here K_v° refers to the connected component of 1 in K_v^*. So $K_v^\circ = K_v^*$ if v is complex, and $(0, \infty)$ if v is real. We also set

$$W_{\mathfrak{m}} = \prod_{\substack{v|\mathfrak{m} \\ v<\infty}} 1 + \mathfrak{p}_v^{\mathfrak{m}(v)} \prod_{v\nmid\mathfrak{m}} U_v \prod_{\substack{v|\mathfrak{m} \\ v|\infty}} K_v^\circ$$

where U_v is either $\mathcal{O}_v^*$ or K_v^*, depending on whether v is finite or infinite. Given $x \in K^*$ we write

$$x \equiv 1 \mod {}^*\mathfrak{m}$$

to mean that $x \in H_{\mathfrak{m}}$.

Lemma 3. *Let $\mathfrak{m}$ be a cycle of K. Then*

$$\mathbb{I}_K = K^* H_{\mathfrak{m}}$$

Proof. Given $\alpha \in \mathbb{I}_K$, we must find an $x \in K^*$ such that $\alpha x \in H_{\mathfrak{m}}$. We can use the approximation theorem to produce an x which simultaneously takes into account all the places dividing $\mathfrak{m}$. Note there is no contradiction in designating an $x \in K \cap \mathbb{R}$ to be simultaneously positive and negative at different real places. For example, if $K = \mathbb{Q}(\sqrt{2})$, then $\sqrt{2}$ is positive at one of the real places, and negative at the other.

For v real, we can choose x to have the same sign as α_v, so that $\alpha_v x \in (0, \infty)$ in K_v. For example, if we want x to be positive at the place v, then we can arrange that $|\frac{1}{2} - x|_v < \frac{1}{2}$.

For v finite, we want $\alpha_v x - 1$ to be very small, specifically $|\alpha_v x - 1|_v \leq |\pi_v^{\mathfrak{m}(v)}|_v$. Choose x so that

$$|\alpha_v^{-1} - x|_v \leq |\pi_v^{\mathfrak{m}(v) - \operatorname{ord}_v \alpha_v}|_v$$

Multiply both sides by $|\alpha_v| = |\pi_v^{\operatorname{ord}_v(\alpha_v)}|_v$ to get the result.

□

We will eventually use Lemma 3 to define the Artin map for ideles. We will first define the Artin map ϕ on $H_{\mathfrak{m}}$. Then given an $\alpha \in \mathbb{I}_K$, there is an $x \in K^*$ such that $\alpha x \in H_{\mathfrak{m}}$ by the lemma, so we can define the Artin map on α to be $\phi(\alpha x)$. Showing that this is well defined is the hard part, and we are a long way from that point.

4.2 The transfer principle

Let L/K be abelian, $\mathfrak{m}$ a cycle of K. We will say that $\mathfrak{m}$ is **admissible** (for L/K) if:

- $\mathfrak{m}$ is divisible by all ramified places.
- For v finite, $1 + \mathfrak{p}_v^{\mathfrak{m}(v)}$ is contained in the group of local norms $N_{w/v}(L_w^*)$ for some (equivalently any) place w lying over v.
- If v is real and there is a complex place lying over it, then $\mathfrak{m}(v) = 1$.

The second condition says that $K_v^\circ = (0, \infty)$ coincides with the norm group $N_{w/v}(L_w^*)$, since $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) = (0, \infty)$. Some authors refer to a infinite place as ramified if it is real and it has a complex place lying over it. We will adopt the name **generalized ramified place** which, although cumbersome, will help us avoid ambiguity as well as even more cumbersome statements.

It is clear that there is a unique *smallest admissible cycle* $\mathfrak{f}$ which divides all other admissible cycles, and it can be described as follows: $\mathfrak{f}$ is only divisible by ramified places and real places which have a complex place lying over them. For v ramified, $\mathfrak{f}(v)$ is the smallest number such that $1 + \mathfrak{p}_v^{\mathfrak{f}(v)}$

is contained in the group of local norms. We call this smallest admissible cycle the **conductor** of L/K.

We are almost done making definitions. Let $\mathfrak{m}$ be a cycle, not necessarily admissible.

- $\mathrm{Id}(\mathfrak{m})$ is the group of fractional ideals which are relatively prime to $\mathfrak{m}$.
- $P_{\mathfrak{m}}$ is the group of principal fractional ideals (x), where $x \equiv 1 \pmod{{}^*\mathfrak{m}}$.
- $\mathfrak{N}(\mathfrak{m})$ is the group of norms $N_{L/K}(\mathfrak{b})$, where $\mathfrak{b}$ is a fractional ideal of L and relatively prime to $\mathfrak{m}$ (that is, relatively prime to any places of L which lie over places dividing $\mathfrak{m}$).

The next results depend heavily on the approximation theorem. We remark that if v is a place of K, and x is a norm from L, then x is a local norm from L_w, for all w lying over v. This is because if $x = N_{L/K}(y)$ for $y \in L$, then $x = \prod_{w|v} N_{w/v}(y)$. For a fixed place w_0, each $N_{w/v}(y)$ is a norm from L_w, hence it is a norm from L_{w_0}, since L/K is Galois. Thus x is a local norm from L_{w_0} as a product of such norms.

Lemma 4. *Let $x \in K^*$, and S a finite set of places of K with the property that x is a local norm from L_w for all $v \in S$, $w \mid v$. There exists a $\gamma \in L^*$ such that $xN_{L/K}(\gamma^{-1})$ is close to 1 at each $v \in S$. If $|x|_v = 1$ for a particular $v \in S$ which is finite, then γ can be chosen to be a unit at all $w \mid v$.*

Proof. Fix a $v \in S$. Since each local norm $L_w \to K_v$ is continuous, so is the map $\prod_{w|v} L_w \to K_v$ given by

$$(y_w) \mapsto \prod_{w|v} N_{w/v}(y_w)$$

as a product of continuous functions. Let $w_0, w_1, ...$ be the places of L lying over v. Write x as $N_{w_0/v}(\gamma_0)$ for some $\gamma_0 \in \mathcal{L}^*_{w_0}$. By the approximation theorem, there exists a $\gamma \in L^*$ which is close to γ_0 at w_0, and close to 1 at the other places $w_1, w_2, ...$ Since $(\gamma_0, 1, 1, ...)$ and $(\gamma, \gamma, ...)$ are close to each other in $\prod_w L_w$, we have that

$$|N_{w_0/v}(\gamma_0) - \prod_{w|v} N_{w/v}(\gamma)|_v = |x - N_{L/K}(\gamma)|_v$$

is also very small. Given $\epsilon > 0$, we can choose $\gamma \in L$ so that $|x - N_{L/K}(\gamma)|_v < \epsilon |x|_v$, and then multiply both sides by $|x|_v^{-1}$ to get that $|1 - x^{-1}N_{L/K}(\gamma)|_v < \epsilon$. Since $x^{-1}N_{L/K}(\gamma)$ is very close to 1 at v, so is $xN_{L/K}(\gamma^{-1})$, which is what we wanted. The claim follows when we use the approximation theorem simultaneously for all $v \in S$.

If v is finite, and $|x|_v = 1$, then $x \in \mathcal{O}_v^*$, so the element γ_0 such that $N_{w_0/v}(\gamma_0) = x$ must be a unit in $\mathcal{O}_{w_0}$. Since $\mathcal{O}_w^*$ is open, any element of L_w^* which is very close to a unit will automatically be a unit.

□

Proposition 5. *Let* $\mathfrak{m}$ *be admissible. The inclusion* $\mathrm{Id}(\mathfrak{m}) \subseteq \mathrm{Id}(\mathfrak{f})$ *induces an isomorphism*

$$\mathrm{Id}(\mathfrak{m})/P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}) \cong \mathrm{Id}(\mathfrak{f})/P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})$$

Also, $P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f}) \cap \mathrm{Id}(\mathfrak{m}) = P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$.

Proof. Injectivity and well definedness of the desired map is equivalent to the assertion that $P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f}) \cap \mathrm{Id}(\mathfrak{m}) = P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$. The inclusion '$\supseteq$' is clear, so suppose $J \in P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f}) \cap \mathrm{Id}(\mathfrak{m})$ is equal to $(x)N_{L/K}(\mathfrak{b})$ where $x \equiv 1 \pmod{{}^*f}$ and $\mathfrak{b}$ is a fractional ideal of L which is relatively prime to $\mathfrak{f}$.

For each place v dividing $\mathfrak{f}$, and each $w \mid v$, x is a local norm from $\mathcal{O}_w^*$ (or L_w^* for v infinite). By Lemma 4, we can produce a $\gamma \in L^*$ such that $xN_{L/K}(\gamma^{-1})$ is very close to 1 at each $v \mid \mathfrak{f}$. For $v \mid \mathfrak{f}$ finite and $w \mid v$, we can choose γ to be a unit at w.

Using the approximation theorem, we can also do a little more than what we just did. We applied the lemma to the places $v \mid \mathfrak{f}$ (or more specifically, the places lying over those which divided $\mathfrak{f}$). At the same time, we can take all the *finite* places v which divide $\mathfrak{m}$, but not $\mathfrak{f}$, and add the stipulation that $\mathrm{ord}_w \gamma = -\mathrm{ord}_w \mathfrak{b}$, for all w lying over such v. This ensures that $N_{L/K}(\gamma\mathfrak{b})$ is a unit at each finite $v \mid \mathfrak{m}, v \nmid \mathfrak{f}$. But γ and $\mathfrak{b}$ were already units at all w lying over finite $v \mid \mathfrak{f}$, so in fact $N_{L/K}(\gamma\mathfrak{b})$ is a unit at all finite places $v \mid \mathfrak{m}$. We can write

$$J = (x)N_{L/K}(\gamma^{-1}) \cdot N_{L/K}(\gamma\mathfrak{b})$$

Since $N_{L/K}(\gamma\mathfrak{b})$ and J are both units at $v \mid \mathfrak{m}, v < \infty$, so is $xN_{L/K}(\gamma^{-1})$. We are almost done, but we do not know that $xN_{L/K}(\gamma^{-1})$ is $\equiv 1 \pmod{{}^*\mathfrak{m}}$.

Let $\beta = xN_{L/K}(\gamma^{-1})$. At each $v \mid \mathfrak{f}$, we have that β, having been forced so close to 1, is a local norm. But for v finite, $v \mid \mathfrak{m}, v \nmid \mathfrak{f}$, we also have that β is a local norm. This is because v is necessarily unramified, $\beta \in \mathcal{O}_v^*$, and the local norm $\mathcal{O}_w^* \to \mathcal{O}_v^*$ is surjective. And for v infinite, $v \mid \mathfrak{m}, v \nmid \mathfrak{f}$, v is necessarily a real place which has only real places lying over it, so β is trivially a local norm here. Thus β is a norm for all $v \mid \mathfrak{m}$, finite or infinite.

Since β is a local norm for all places v dividing $\mathfrak{m}$, we can apply the same argument as we did at the beginning of the proof. Specifically, we can find a $\delta \in L^*$ such that $\beta N_{L/K}(\delta^{-1})$ is very close to 1 at all $v \mid \mathfrak{m}$. This gets us $\beta N_{L/K}(\delta^{-1}) \equiv 1 \pmod{{}^*\mathfrak{m}}$. In picking δ, we can assume that δ will be a unit at all finite places $w \mid v \mid \mathfrak{m}$. Thus $N_{L/K}(\gamma\mathfrak{b})$, and hence $N_{L/K}(\delta\gamma\mathfrak{b})$, is in $\mathfrak{N}(\mathfrak{m})$. Thus

$$J = xN_{L/K}(\gamma^{-1})N_{L/K}(\delta^{-1})N_{L/K}(\delta\gamma\mathfrak{b}) = [\beta N_{L/K}(\delta^{-1})] \cdot [N_{L/K}(\delta\gamma\mathfrak{b})]$$

is in $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$, as required.

Finally, let us prove surjectivity. This is much easier than the injectivity we just did. Given

$\mathfrak{a} \in \mathrm{Id}(\mathfrak{f})$, it is enough to find an $x \in K^*$ such that $x \equiv 1 \pmod{{}^*\mathfrak{f}}$ and $x\mathfrak{a}$ is relatively prime to $\mathfrak{m}$. Just use the approximation theorem: for $v \mid \mathfrak{f}$, pick x to be very close 1, and for $v \mid \mathfrak{m}, v \nmid \mathfrak{f}, v < \infty$, pick x so that $\mathrm{ord}_v\, x = -\mathrm{ord}_v\, \mathfrak{a}$.

□

For $\mathfrak{m}$ an admissible cycle, let $\mathbb{I}_L(1, \mathfrak{m})$ be the set of ideles in L which have component 1 at all $w \mid v \mid \mathfrak{m}$. Recall the definitions of $H_\mathfrak{m}, W_\mathfrak{m}$ given earlier. It is straightforward to check that

$$W_\mathfrak{m} N_{L/K}(\mathbb{I}_L(1, \mathfrak{m})) = H_\mathfrak{m} \cap N_{L/K}(\mathbb{I}_L)$$

Just use the fact that the local norm is surjective for $v \nmid \mathfrak{m}$.

Theorem 6. *Let $\mathfrak{m}$ be admissible. There is an isomorphism, to be described in the proof:*

$$\mathbb{I}_K / K^* N_{L/K}(\mathbb{I}_L) \cong \mathrm{Id}(\mathfrak{m}) / P_\mathfrak{m} \mathfrak{N}(\mathfrak{m})$$

Proof. Let $\psi : H_\mathfrak{m} \to \mathrm{Id}(\mathfrak{m})$ be the homomorphism $\alpha \mapsto \prod_{v \nmid \mathfrak{m}, v < \infty} \mathfrak{p}_v^{ord_v \alpha}$ which is obviously surjective. Let $\overline{\psi}$ be the composition

$$H_\mathfrak{m} \xrightarrow{\phi} \mathrm{Id}(\mathfrak{m}) \to \mathrm{Id}(\mathfrak{m}) / P_\mathfrak{m} \mathfrak{N}(\mathfrak{m})$$

And, let $\overline{\phi}$ be the composition

$$H_\mathfrak{m} \subseteq \mathbb{I}_K \to \mathbb{I}_K / K^* N_{L/K}(\mathbb{I}_L)$$

This is surjective by Lemma 3. We claim that $\mathrm{Ker}\, \overline{\psi} = \mathrm{Ker}\, \overline{\phi}$. This will suffice for the proof, since then

$$\mathrm{Id}(\mathfrak{m}) / P_\mathfrak{m} \mathfrak{N}(\mathfrak{m}) \cong H_\mathfrak{m} / \mathrm{Ker}\, \overline{\psi} = H_\mathfrak{m} / \mathrm{Ker}\, \overline{\phi} \cong \mathbb{I}_K / K^* N_{L/K}(\mathbb{I}_L)$$

First, we claim that

$$\mathrm{Ker}\, \overline{\psi} = (H_\mathfrak{m} \cap K^*) W_\mathfrak{m} N_{L/K}(\mathbb{I}_L(1, \mathfrak{m}))$$

The inclusion '$\supseteq$' is straightforward: just check that $(K^* \cap H_\mathfrak{m}), W_\mathfrak{m}$, and $N_{L/K}(\mathbb{I}_L(1, \mathfrak{m}))$ are each contained in the kernel. Conversely, suppose that $\alpha \in H_\mathfrak{m}$ lies in the kernel of $\overline{\psi}$. Then $\psi(\alpha) = (x) N_{L/K}(\mathfrak{b})$ for some $x \equiv 1 \pmod{}* \mathfrak{m}$ and fractional ideal $\mathfrak{b}$ of L which relatively prime to $\mathfrak{m}$. Let β be an idele of L such that $\mathrm{ord}_w\, \beta = \mathrm{ord}_w\, \mathfrak{b}$ whenever $w < \infty$ and $\mathrm{ord}_w\, \mathfrak{b} \neq 0$, and otherwise set $\beta_w = 1$. Then $\psi N_{L/K}(\beta) = N_{L/K}(\mathfrak{b})$. Also $(x) = \psi x$, where $x \in K^* \cap H_\mathfrak{m}$. This implies $\alpha x^{-1} N_{L/K}(\beta^{-1})$ is in the kernel of ψ. But it is easy to see that the kernel of ψ is $W_\mathfrak{m}$. This proves what we wanted, since $x \in H_\mathfrak{m} \cap K^*$ and $N_{L/K}(\beta) \in N_{L/K}(\mathbb{I}_L(1, \mathfrak{m}))$.

Now, by the remark just above this theorem and by what we just proved, $\mathrm{Ker}\, \overline{\psi} = (H_\mathfrak{m} \cap K^*)(H_\mathfrak{m} \cap N_{L/K}(\mathbb{I}_L)$. And it is easy to see that $\mathrm{Ker}\, \overline{\phi} = H_\mathfrak{m} \cap K^* N_{L/K}(\mathbb{I}_L)$. So, the only thing left

to prove is that

$$(H_{\mathfrak{m}} \cap K^*)(H_{\mathfrak{m}} \cap N_{L/K}(\mathbb{I}_L)) = H_{\mathfrak{m}} \cap K^* N_{L/K}(\mathbb{I}_L)$$

The inclusion '$\subseteq$' is straightforward. Conversely, suppose $\alpha \in H_{\mathfrak{m}}$ is equal to a product $xN_{L/K}(\beta)$ for $x \in K^*$ and $\beta \in \mathbb{I}_L$. By the approximation theorem, it is possible to find a $\gamma \in L^*$ such that $N_{L/K}(\beta)N_{L/K}(\gamma^{-1}) = N_{L/K}(\gamma^{-1}\beta)$ is close to 1 for all $v \mid \mathfrak{m}$. (Lemma 4). If chosen close enough to 1, we will have $N_{L/K}(\gamma^{-1}\beta) \in H_{\mathfrak{m}} \cap N_{L/K}(\mathbb{I}_L)$. Since $\alpha \in H_{\mathfrak{m}}$ and

$$\alpha = xN_{L/K}(\gamma)N_{L/K}(\gamma^{-1}\beta)$$

it follows that $xN_{L/K}(\gamma) \in H_{\mathfrak{m}} \cap K^*$. This completes the proof.

□

Corollary 7. *If $\mathfrak{m}$ is admissible for L/K, then*

$$[\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)] = [\mathrm{Id}(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})]$$

4.3 The kernel of the Artin map

Let L/K be abelian, and $\mathfrak{m}$ a cycle of K which is divisible by the ramified places. We defined the Artin map for ideals

$$\Phi : \mathrm{Id}(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

in the beginning of the chapter. This mapping is surjective (Theorem 2). Suppose that $P_{\mathfrak{m}}$ were contained in the kernel of Φ. Then, we can enlarge $\mathfrak{m}$ (and thus shrink $P_{\mathfrak{m}}, \mathrm{Id}(\mathfrak{m})$) so that $\mathfrak{m}$ is admissible, and $P_{\mathfrak{m}}$ is still contained in the kernel of the new Artin map. So without loss of generality, we can assume $\mathfrak{m}$ is admissible. Clearly $\mathfrak{N}(\mathfrak{m})$ is always contained in the kernel of Φ, so we have $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m}) \subseteq \operatorname{Ker}\Phi$. But combining Corollary 7 with the first global norm index inequality,

$$[\mathrm{Id}(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})] = [\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)] \leq |\operatorname{Gal}(L/K) = [\mathrm{Id}(\mathfrak{m}) : \operatorname{Ker}\Phi]$$

we must have equality everywhere. We state this as a proposition.

Proposition 8. *If L/K is abelian, $\mathfrak{m}$ is admissible for L/K, and $P_{\mathfrak{m}}$ is contained in the kernel of the Artin map on* $\mathrm{Id}(\mathfrak{m})$*, then the kernel is exactly $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$, and*

$$[L : K] = [\mathrm{Id}(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})] = [\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)]$$

If $\mathfrak{m}'$ is another admissible cycle, and $\mathfrak{m}$ divides $\mathfrak{m}'$, then $P_{\mathfrak{m}'}$ is contained in the kernel of the Artin map on $\mathrm{Id}(\mathfrak{m}')$*, hence $P_{\mathfrak{m}'}\mathfrak{N}(\mathfrak{m}')$ is the kernel of the Artin map on* $\mathrm{Id}(\mathfrak{m}')$*.*

The goal of the next chapter is to show that the hypothesis of Proposition 8 holds for all abelian extensions and all admissible cycles. For a fixed abelian extension L/K, in order to prove that the kernel of the Artin map on $\mathrm{Id}(\mathfrak{m})$ is $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ for *all* admissible cycles $\mathfrak{m}$, it suffices by Proposition 5 to do so with an admissible cycle $\mathfrak{c}$ which is only divisible by generalized ramified places.

The first step is showing this holds for cyclotomic extensions.

Proposition 9. *Let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta)$ for ζ a primitive mth root of unity. There is an admissible cycle $\mathfrak{m}$ of $\mathbb{Q}$, divisible only by ramified places (that is, those places which divide m) and the unique infinite place of $\mathbb{Q}$, such that $P_{\mathfrak{m}}$ is contained in the kernel of the Artin map on* $\mathrm{Id}(\mathfrak{m})$.

Proof. Let $x \in \mathbb{Q}^*$, and $x = \frac{a}{b}$ for $a, b \in \mathbb{Z}$. We know that if q is a prime which does not divide m, then $(q, \mathbb{Q}(\zeta)/\mathbb{Q})$ is the map $\zeta \mapsto \zeta^q$. It follows by multiplicativity that $(x, \mathbb{Q}(\zeta)/\mathbb{Q})$ is the map $\zeta \mapsto \zeta^{ab^{-1}}$, where by b^{-1} we mean an integer which is an inverse of b modulo m.

Define a cycle $\mathfrak{c}$ to be the formal product of the integer m (that is, $\mathfrak{c}(v) = \mathrm{ord}_v(m)$) and the unique infinite place, and suppose $x \equiv 1 \pmod{{}^*\mathfrak{c}}$. We want to show that $(x, \mathbb{Q}(\zeta)/\mathbb{Q}) = 1$, or in other words $ab^{-1} \equiv 1 \pmod{m}$. Afterwards, we can enlarge $\mathfrak{c}$ to be admissible (although it doesn't matter for this chapter, actually $\mathfrak{c}$ is already admissible for $\mathbb{Q}(\zeta)/\mathbb{Q}$. This is 7, Corollary 4).

Write m as $p_1^{e_1} \cdots p_s^{e_s}$ for primes p_i. For each i, we have by hypothesis that $x - 1 \in p_i^{e_i}\mathbb{Z}_{p_i}$. Then $\frac{x-1}{p_i^{e_i}} \in \mathbb{Z}_{p_i} \cap \mathbb{Q} = \mathbb{Z}_{(p_i)}$ (the localization of $\mathbb{Z}$ at p_i), so $x \equiv 1 \pmod{p_i^{e_i}\mathbb{Z}_{(p_i)}}$. We have isomorphisms

$$(\mathbb{Z}/m\mathbb{Z})^* \to \prod_{i=1}^{s} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^* \to \prod_{i=1}^{s} (\mathbb{Z}_{(p_i)}/p_i^{e_i}\mathbb{Z}_{(p_i)})^*$$

which send $ab^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*$ to x at each coordinate on the right. Thus ab^{-1} is the identity.

□

An exercise: where did we use the fact that x was positive?

Corollary 10. *Let K be a number field, $K \subseteq L \subseteq K(\zeta)$, where ζ is a primitive mth root of unity. There is an admissible cycle $\mathfrak{l}$ for L/K, divisible at the finite places only by v dividing m, such that $P_{\mathfrak{l}}$ is contained in the kernel of the Artin map for L/K, this Artin map being defined on* $\mathrm{Id}(\mathfrak{l})$.

Proof. We first prove the case $L = K(\zeta)$. Let $\mathfrak{m}$ be the admissible cycle for $\mathbb{Q}(\zeta)/\mathbb{Q}$ in the last proposition. It is only divisible by places dividing m and by the unique infinite place of $\mathbb{Q}$. Since the local norms are continuous, it is possible to find a cycle $\mathfrak{l}$ of K such that if $x \equiv 1 \pmod{{}^*\mathfrak{l}}$, then $N_{K/\mathbb{Q}}(x) \equiv 1 \pmod{{}^*\mathfrak{m}}$. This does what is required.

The case $L \subsetneq K(\zeta)$ follows easily from what we have just proved.

□

Although all the ramified primes of K must divide m, a prime divisor of m need not be ramified. So we have yet to find an admissible cycle for $K(\zeta)/K$ which is only divisible by generalized ramified

places. However, the cycle we have found so far is small enough for us to be able to deduce what we want about cyclic extensions, which is the next section.

4.4 Admissibility of cyclic extensions

Lemma 11. *Let $a, r, q > 1$ be integers with q prime. There exists a prime number p such that a has multiplicative order q^r in $(\mathbb{Z}/p\mathbb{Z})^*$.*

For r large, we know of course that q^r divides $p-1$, so also p must be large. So from the lemma we see that, given $1 < r_0 \in \mathbb{N}$ we can find arbitrarily large primes p such that the order of a is divisible by q^{r_0}.

If G is an abelian group, we say that $a, b \in G$ are **independent** if the cyclic groups they generate have trivial intersection.

Lemma 12. *Let $a, n > 1$ be integers, with*

$$n = q_1^{r_1} \cdots q_s^{r_s}$$

for distinct primes q_i. There exist b, m, with m squarefree and divisible by $2s$ distinct primes, such that:

(i) The multiplicative orders of a and b (modulo m) are divisible by n.

(ii) a and b are independent modulo m.

Moreover, all the prime numbers comprising m can be chosen arbitrarily large.

Let $\mathfrak{p}$ be a prime of K, and ζ an mth root of unity. Then $K(\zeta)$ is an abelian extension of K, and for any K-automorphism of $K(\zeta)$, restriction to $\mathbb{Q}(\zeta)$ induces an isomorphism:

$$\mathrm{Gal}(K(\zeta)/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/K \cap \mathbb{Q}(\zeta))$$

If we assume that $\mathfrak{p}$ does not divide m, then $\mathfrak{p}$ will be unramified in $K(\zeta)$. We have

$$(\mathfrak{p}, K(\zeta)/K))_{|\mathbb{Q}(\zeta)} = (N_{K/\mathbb{Q}}(\mathfrak{p}), \mathbb{Q}(\zeta)/\mathbb{Q}) = (p, \mathbb{Q}(\zeta)/\mathbb{Q})^{f(\mathfrak{p}/p)}$$

where $\mathfrak{p}$ lies over p. Since $(p, \mathbb{Q}(\zeta)/\mathbb{Q})$ applied to ζ is equal to ζ^p, we conclude that

$$(\mathfrak{p}, K(\zeta)/K)(\zeta) = \zeta^{p^{f(\mathfrak{p}/p)}} = \zeta^{\mathcal{N}\mathfrak{p}}$$

Alternatively, without the Artin map, this can be seen by the fact that the mth roots of unity are distinct in $\mathcal{O}_{K(\zeta)}$ modulo any prime lying over $\mathfrak{p}$.

Before the next lemma, we recall a result from Galois theory. It will be used at the end of the next lemma.

Fact: let ℓ_1, ℓ_2 be finite extensions of a field k. The following are equivalent:
(1): $[\ell_1\ell_2 : k] = [\ell_1 : k][\ell_2 : k]$
(2): $[\ell_1\ell_2 : \ell_1] = [\ell_2 : k]$
(3): $[\ell_1\ell_2 : \ell_2] = [\ell_1 : k]$
These conditions imply that
(4): $\ell_1 \cap \ell_2 = k$
and the converse is true if at least one of ℓ_1, ℓ_2 is Galois over k.

If ℓ_2 is Galois over k, and ℓ is an an intermediate field of ℓ_1/k, we can use the fact to conclude that $\ell_1 \cap \ell_2 = k$ implies that $\ell_1 \cap \ell\ell_2 = \ell$.

For if $\ell_1 \cap \ell_2 = k$, then $\ell \cap \ell_2 = k$, so (4) $\Rightarrow$ (2) tells us that $[\ell\ell_2 : \ell] = [\ell_2 : k]$. Also (4) $\Rightarrow$ (1) tells us that $[\ell_1\ell_2 : k] = [\ell_1 : k][\ell_2 : k]$. We then have

$$[\ell_1\ell_2 : \ell] = \frac{[\ell_1\ell_2 : k]}{[\ell : k]} = \frac{[\ell_1 : k][\ell_2 : k]}{[\ell : k]} = [\ell_1 : \ell][\ell_2 : k] = [\ell_1 : \ell][\ell\ell_2 : \ell]$$

Since $\ell_1(\ell\ell_2) = \ell_1\ell_2$, we get that $\ell_1 \cap \ell\ell_2 = \ell$ by (1) $\Rightarrow$ (4).

Lemma 13. *Let L/K be abelian, $\mathfrak{p}$ an unramified prime of K, and S a finite set of prime numbers. Then there exists an integer m, relatively prime to $\mathfrak{p}$ as well as all members of S, such that:*

(i) $L \cap K(\zeta) = K$, where ζ is a primitive mth root of unity.

(ii) $[L : K]$ divides the order of $(\mathfrak{p}, K(\zeta)/K)$.

(iii) There exists a $\tau \in \mathrm{Gal}(K(\zeta)/K)$, independent of $(\mathfrak{p}, K(\zeta)/K)$, with order also divisible by $[L : K]$.

Proof. We know that the Galois group $\mathrm{Gal}(K(\zeta)/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$, so the proof is a straightforward application of the last lemma.

Apply the previous lemma, where $a = \mathcal{N}\mathfrak{p}$, and $n = [L : K]$. Take the primes which divide m to be large enough so that they are distinct from the primes of S, the primes which ramify in L, as well as the primes over which $\mathfrak{p}$ lies. Now let ζ be a primitive mth root of unity. Then $\mathfrak{p}$ is unramified in $K(\zeta)$, and $(\mathfrak{p}, K(\zeta)/K)$ has the effect $\zeta \mapsto \zeta^{\mathcal{N}\mathfrak{p}}$.

We first claim that $L \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ (which implies $L \cap K(\zeta) = K$ by the *fact* above). This is true because $L \cap \mathbb{Q}(\zeta)$ is unramified over $\mathbb{Q}$: any prime in $\mathbb{Q}$ which ramifies in $K \cap \mathbb{Q}(\zeta)$ must also ramify in K and $\mathbb{Q}(\zeta)$, and we chose m to ensure that there are no such primes.

Thus also $K \cap \mathbb{Q}(\zeta) = \mathbb{Q}$, so by the remark just above the statement to this lemma, the canonical inclusion $\mathrm{Gal}(K(\zeta)/K) \to (\mathbb{Z}/m\mathbb{Z})^*$ is an isomorphism. Therefore for any t relatively prime to m, the map $\zeta \mapsto \zeta^t$ extends uniquely to a well defined K-automorphism of $K(\zeta)$. Taking b to be as in the previous lemma, and letting τ be the map given by $\zeta \mapsto \zeta^b$, we see that since $a = \mathcal{N}\mathfrak{p}$ and b are

independent modulo m and have order divisible by $n = [L : K]$, the automorphisms $(\mathfrak{p}, K(\zeta)/K)$ and τ are also independent in $\mathrm{Gal}(K(\zeta)/K)$, and their orders are divisible by $[L : K]$.

□

We will shortly deal with many roots of unity at time, so from now on let ζ_m denote a primitive mth unity.

Proposition 14. *(Artin's Lemma) Assume the hypotheses of the previous lemma. If L/K is cyclic, there exists an m relatively prime to all elements of S, and an abelian extension E of K, such that:*

(i) $L \cap E = K$.

(ii) $L(\zeta_m) = E(\zeta_m)$.

(iii) $L \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ and $L \cap K(\zeta_m) = K$.

(iii) $\mathfrak{p}$ splits completely in E.

Proof. Choose m as we did in the previous Lemma. So already (iii) holds, and we know in this case that the map

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

$$\phi \mapsto (\phi_{|L}, \phi_{|K(\zeta)})$$

is an isomorphism. Let σ generate $\mathrm{Gal}(L/K)$, and let τ be as in the previous lemma. Let H be the subgroup of $\mathrm{Gal}(L(\zeta)/K)$ generated by the elements (σ, τ) and $\phi = ((\mathfrak{p}, L/K), (\mathfrak{p}, K(\zeta)/K))$.

Our first claim is that ϕ is the Frobenius element $(\mathfrak{p}, L(\zeta)/K)$. If $v_1, ...v_n$ is an integral basis for L/K, and $w_1, ..., w_s$ an integral basis for $K(\zeta)/K$, then we know that $v_i w_j$ is an integral basis for $L(\zeta)/K$. It follows that ϕ has the effect

$$\phi(v_i w_j) = (\mathfrak{p}, L/K)(v_i) \cdot (\mathfrak{p}, K(\zeta)/K)(w_j) \equiv (v_i w_j)^{\mathcal{N}(\mathfrak{p})} \pmod{\mathcal{O}_{K(v)}}$$

which proves our claim.

Let E be the fixed field of H. The fact that $(\mathfrak{p}, L(\zeta)/K) \in H$ means that H contains the decomposition group $\mathrm{Gal}(L(\zeta)/K)_{\mathfrak{p}}$. Hence E is contained in the decomposition field, giving us that $\mathfrak{p}$ splits completely in E. This establishes (iv).

If $x \in L \cap E$, then x is fixed by (σ, τ). But $(\sigma, \tau)(x) = \sigma(x)$, so $\sigma(x) = x$. This implies x is fixed by every element of $\mathrm{Gal}(L/K)$, so $x \in K$. This proves (i).

Since $E \subseteq L(\zeta_m)$, of course $E(\zeta_m) \subseteq L(\zeta_m)$. Now $E(\zeta_m)$ is the compositum of $K(\zeta_m)$ and E, so $\mathrm{Gal}(L(\zeta_m)/E(\zeta_m))$ is the intersection of $\mathrm{Gal}(L(\zeta_m)/K(\zeta_m))$ and H. To prove (ii), it suffices to show that this intersection is trivial. Since $L \cap K(\zeta) = K$, restriction to L induces an isomorphism $\mathrm{Gal}(L(\zeta_m)/K(\zeta_m)) \cong \mathrm{Gal}(L/K)$, which means that $\mathrm{Gal}(L(\zeta_m)/K(\zeta_m))$ (interpreted as a subgroup of $\mathrm{Gal}(L/K) \times \mathrm{Gal}(K(\zeta_m)/K)$) is just $\mathrm{Gal}(L/K) \times \{1\}$.

To show that $\mathrm{Gal}(L/K) \times \{1\}$ intersected with H is trivial, write $(\mathfrak{p}, L/K) = \sigma^j$ for some j, and let $c = (\mathfrak{p}_v, K(\zeta)/K)$. Suppose there are integers l, k_1, k_2 such that

$$(\sigma, 1)^l = (\sigma, \tau)^{k_1}(\sigma^j, c)^{k_2}$$

Then $(1,1) = (\sigma^{k_1+k_2 j-l}, \tau^{k_1} c^{k_2})$. So $\tau^{k_1} c^{k_2} = 1$. This implies $\tau^{k_1} \in \langle c \rangle \cap \langle \tau \rangle = \{1\}$, so $\tau^{k_1} = 1$. The order of τ divides k_1, and is divisible by n, so n divides k_1. Similarly n divides k_2. Then

$$1 = \sigma^{k_1+k_2 j-l} = \sigma^{-l}$$

so $(\sigma, 1)^l$ must be the identity.

□

Artin's lemma extends to the case where we have a finite collection of primes $\mathfrak{p}_1, ..., \mathfrak{p}_r$ of K, all unramified in L. Use the lemma to find numbers $m_1, ..., m_s$, divisible by successively large primes, as well as extensions $E_1, ..., E_r$ of K, so that each pair E_i, ζ_{m_i} satisfies the conditions of Artin's lemma. Take the numbers m_i to be pairwise relatively prime, so that $\mathbb{Q}(\zeta_{m_1}, ..., \zeta_{m_r}) = \mathbb{Q}(\zeta_{m_1 \cdots m_r})$.

We quickly recall another result from Galois theory.

Fact: Let $\ell_1, ..., \ell_r$ be Galois over k. Restriction induces an injective homomorphism

$$\mathrm{Gal}(\ell_1 \cdots \ell_r/k) \to \mathrm{Gal}(\ell_1/k) \times \cdots \times \mathrm{Gal}(\ell_r/k)$$

If for each $1 \leq i \leq r$, it holds that $\ell_i \cap (\ell_1 \cdots \ell_{i-1} \ell_{i+1} \cdots \ell_r) = k$, then the injection is an isomorphism.

This is exactly the case here. We have that $L \cap \mathbb{Q}(\zeta_{m_1 \cdots m_r}) = \mathbb{Q}$, since the intersection is unramified over $\mathbb{Q}$. It follows that $K = L \cap K(\zeta_{m_1 \cdots m_r}) = L \cap K(\zeta_{m_1}, ..., \zeta_{m_r})$. Similarly $\mathbb{Q}(\zeta_{m_1}) \cap L(\zeta_{m_2}, ..., \zeta_{m_r}) = \mathbb{Q}$, the intersection being unramified over $\mathbb{Q}$, from which we get $K(\zeta_{m_1}) \cap L(\zeta_{m_1}, ..., \zeta_{m_r}) = K$.

Therefore if we set $\mathscr{L} = L(\zeta_{m_1}, ..., \zeta_{m_r})$, then $\mathscr{L}$ is the compositum of L and $K(\zeta_{m_1}), ..., K(\zeta_{m_r})$, and

$$\mathrm{Gal}(\mathscr{L}/K) \cong G \times G_1 \times \cdots \times G_r$$

where $G = \mathrm{Gal}(L/K)$ and $G_i = \mathrm{Gal}(K(\zeta_{m_i})/K)$. Note that by our choice of m_i, we can identify G_i with the $\mathrm{Gal}(\mathbb{Q}(\zeta_i)/\mathbb{Q})$, which is isomorphic to $(\mathbb{Q}/m\mathbb{Q})^*$.

Now, we know that for the Galois extension $L(\zeta_{m_i})/K$, E_i was constructed to be the fixed field of

$$H_i \subseteq G \times G_i \cong \mathrm{Gal}(L(\zeta_{m_i})/K)$$

where H_i was generated by (σ, τ_i) and $(\mathfrak{p}, L(\zeta_{m_i})/K)$. In turn, $\mathrm{Gal}(L(\zeta_{m_i})/K)$ is the quotient of $\mathrm{Gal}(\mathscr{L}/K)$ by

$$\mathrm{Gal}(\mathscr{L}/L(\zeta_{m_i})) \cong \{1\} \times G_1 \times \cdots \times G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_r$$

so one can check that E_i is also the fixed field of

$$H_i \times G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_r \subseteq \mathrm{Gal}(\mathscr{L}/K)$$

Lemma 15. *Let $E = E_1 \cdots E_s$. Then $L \cap E = K$, and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(LE/E)$.*

Proof. The second claim follows from the first, using a standard result from Galois theory. Now, $\mathrm{Gal}(\mathscr{L}/L \cap E)$ is equal to the subgroup of $\mathrm{Gal}(\mathscr{L}/L \cap E)$ generated by G and $\mathrm{Gal}(\mathscr{L}/E) = \bigcap_{i=1}^{r} \mathrm{Gal}(\mathscr{L}/E_i) = \bigcap_{i=1}^{r} H_i$. Check that

$$(\sigma, \tau_1, ..., \tau_r) \in \mathrm{Gal}(\mathscr{L}/E)$$

Also $(1, \tau_1, ..., \tau_r)$, hence $(1, \tau_1^{n-1}, ..., \tau_r^{n-1})$, is in $\mathrm{Gal}(\mathscr{L}/L)$. We then have

$$(\sigma, 1, ..., 1) = (\sigma, \tau_1, ..., \tau_r)(1, \tau_1^{n-1}, ..., \tau_r^{n-1}) \in \mathrm{Gal}(\mathscr{L}/L \cap E)$$

This shows that $\mathrm{Gal}(\mathscr{L}/K) \subseteq \mathrm{Gal}(\mathscr{L}/L \cap E)$, so $L \cap E \subseteq K$. Hence $L \cap E = K$. □

In Proposition 7, we deduced the kernel of the Artin map by showing that $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$ was contained in it. To deduce the kernel of the Artin map for a cyclic extension, we will prove the opposite inclusion, and use the global cyclic norm index equality.

Theorem 16. *Let L/K be cyclic, and $\mathfrak{f}$ the conductor of L/K. The kernel of the Artin map on $\mathrm{Id}(\mathfrak{f})$ is equal to $P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})$.*

Proof. Let $\mathfrak{f}$ be the conductor of L/K. Let $\Phi : \mathrm{Id}(\mathfrak{f}) \to \mathrm{Gal}(L/K)$ be the Artin map. By the cyclic global norm index equality, that is $[L : K] = [\mathrm{Id}(\mathfrak{f}) : P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})]$, it suffices to show that $\mathrm{Ker}\,\Phi \subseteq P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})$.

So let $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_r^{s_r}$ be in the kernel of the Artin map on $\mathrm{Id}(\mathfrak{f})$, for $\mathfrak{p}_i$ distinct primes of K which are unramified in L. Find integers $m_1, ..., m_r$ which are pairwise relatively prime and divisible by large primes, along with fields $E, E_1, ..., E_r$ so that the conditions following Artin's lemma hold.

Now $E_i \subseteq LE_i \subseteq E_i(\zeta_{m_i})$, so by Proposition (?) there exists a cycle $\mathfrak{c}_i$ of E_i, admissible for LE_i/E_i, such that the kernel of the Artin map of LE_i/E_i on $\mathrm{Id}(\mathfrak{c}_i)$ is equal to $P_{\mathfrak{c}_i}\mathfrak{N}_{LE_i/E_i}(\mathfrak{c}_i)$. In the proposition, $\mathfrak{c}_i$ is only divisible by prime ideals of E_i which divide m_i. But there is no problem with enlarging $\mathfrak{c}_i$, in particular to make it divisible by places lying over all those which divide $\mathfrak{f}$. The identity for the kernel of the Artin map will still hold. If $\mathfrak{c}_i$ is chosen large enough, we will have by the contiuity of the local norms that $\beta \equiv 1 \pmod{{}^*\mathfrak{c}_i}$ implies $N_{E_i/K}(\beta) \equiv 1 \pmod{{}^*\mathfrak{f}}$.

Let σ generate $\mathrm{Gal}(L/K)$, and let d_i be an integer such that $(\mathfrak{p}_i^{s_i}, L/K) = \sigma^{d_i}$. We know that restriction to L induces an isomorphism $\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(L/K)$, and the Artin map on LE/E is surjective, so we may find a fractional ideal $\mathfrak{b}_E$ of E, relatively prime to $\mathfrak{f}$ and all the m_i, such that σ is the restriction of $(\mathfrak{b}_E, LE/E)$ to L. But then $\sigma = (\mathfrak{b}, L/K)$, where $\mathfrak{b} = N_{E/K}(\mathfrak{b}_E)$. This gives us

$$(\mathfrak{p}_i^{s_i}, L/K) = (\mathfrak{b}^{d_i}, L/K)$$

Now $\mathfrak{b}$, being a norm from E to K, is also a norm from E_i to K. And $\mathfrak{p}_i$, splitting completely in E_i, is trivially a norm from E_i to K. Hence $\mathfrak{p}_i^{s_i}\mathfrak{b}^{-d_i}$ is equal to $N_{E_i/K}(J_i)$, for some fractional ideal J_i of E_i. Necessarily J_i is relatively prime to $\mathfrak{f}$ and all the m_i. And

$$1 = (\mathfrak{p}_i^{s_i}\mathfrak{b}^{-d_i}, L/K) = (N_{E_i/K}(J_i), L/K) = (J_i, LE_i/E_i)_{|L}$$

so $(J_i, LE_i/E_i)$, being completed determined as an automorphism of LE_i by its effect on L, must be the identity. Thus J_i, being in the kernel of the Artin map on $\mathrm{Id}(\mathfrak{c}_i)$, must be equal to

$$\beta_i N_{LE_i/E_i}(\mathcal{B}_i)$$

where $\beta_i \equiv 1 \pmod{{}^*\mathfrak{c}_i}$ and $\mathcal{B}_i$ is relatively prime to $\mathfrak{f}$ and all the m_i. We now take the norm back down to K to get

$$\mathfrak{p}_i^{s_i}\mathfrak{b}^{d_i} = N_{E_i/K}(J_i) = N_{E_i/K}(\beta_i)N_{E_i/K}(N_{LE_i/E_i}(\mathcal{B}_i))$$

with $N_{E_i/K}(\beta_i) \equiv 1 \pmod{{}^*\mathfrak{f}}$ and

$$N_{E_i/K}(N_{LE_i/E_i}(\mathcal{B}_i)) = N_{LE_i/K}(\mathcal{B}_i) = N_{L/K}(N_{LE_i/L}(\mathcal{B}_i)) \in \mathfrak{N}(\mathfrak{f})$$

Now just multiply all the $\mathfrak{p}_i^{s_i}\mathfrak{b}^{d_i}$ together to get that

$$\mathfrak{a}\mathfrak{b}^{d_1+\cdots+d_r} \in P_{\mathfrak{f}}\mathfrak{N}(\mathfrak{f})$$

We're almost done. Since

$$1 = (\mathfrak{a}, L/K) = \sigma^{d_1+\cdots+d_r}$$

we have that $n = [L : K]$ must divide $d_1 + \cdots + d_r$. Hence $\mathfrak{b}^{d_1+\cdots+d_r}$ is a norm from L, necessarily in $\mathfrak{N}(\mathfrak{f})$.

□

4.5 The Artin map for ideles

Since we have proved what we wanted for cyclic extensions, we can now do so for arbitrary abelian extensions.

Theorem 17. *Let L/K be abelian, and $\mathfrak{m}$ an admissible cycle for L/K. The Artin map, as defined on* $\mathrm{Id}(\mathfrak{m})$*, has kernel $P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})$, and*

$$[L:K] = [\mathbb{I}_K : K^* N_{L/K}(\mathbb{I}_L)] = [\mathrm{Id}(\mathfrak{m}) : P_{\mathfrak{m}}\mathfrak{N}(\mathfrak{m})]$$

Proof. Proposition 8 and Theorem 16. □

Now we can define the Artin map on ideles. Let $\mathfrak{m}$ be admissible. Recall the definition of $H_{\mathfrak{m}}$ (Section 1). We first define

$$\Phi : H_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

by

$$\Phi(\alpha) = \prod_{v \nmid \mathfrak{m}, v < \infty} (\mathfrak{p}_v, L/K)^{\mathrm{ord}_v \alpha}$$

Of course this is a finite product. There is an obvious analogy between the Artin map on $\mathrm{Id}(\mathfrak{m})$ and that on $H_{\mathfrak{m}}$, and we can immediately transfer some results over. For example, Φ is surjective, and by Theorem 16 we can see that Φ is trivial on $K^* \cap H_{\mathfrak{m}}$.

We will now extend Φ to all of $\mathbb{I}_K$. Let α be an idele. By Lemma 3, there is an $x \in K^*$ and a $\beta \in H_{\mathfrak{m}}$ such that $\alpha = x\beta$. We then define $\Phi(\alpha)$ to be $\Phi(\beta)$. This is well defined: if $x_1 \in K^*, \beta_1 \in H_{\mathfrak{m}}$, and $x\beta = x_1\beta_1$, then $\Phi(\beta\beta_1^{-1}) = 1$, because $\beta\beta_1^{-1} = xx_1^{-1} \in K^* \cap H_{\mathfrak{m}}$.

Furthermore, Φ is independent of the choice of admissible cycle $\mathfrak{m}$, because if $\mathfrak{c}$ is another admissible cycle, then $H_{\mathfrak{m}} \cap H_{\mathfrak{c}} = H_{\mathfrak{l}}$, where $\mathfrak{l}$ is the least common multiple of $\mathfrak{m}$ and $\mathfrak{c}$, and this is admissible.

Theorem 18. *The Artin map $\Phi : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ has the following properties:*

(i) Φ is surjective with kernel $K^* N_{L/K}(\mathbb{I}_L)$.

(ii) If v is unramified, and $x \in K_v^*$, then Φ maps x (interpreted as the idele $(..., 1, x, 1, ...)$) to $(\mathfrak{p}_v, L/K)^{\mathrm{ord}_v(x)}$.

(iii) Φ is continuous.

(iv) Φ is the unique continuous homomorphism $\mathbb{I}_K \to \mathrm{Gal}(L/K)$ which is trivial on K^* and satisfies (ii).

Proof. (i) and (ii) follow from looking at the isomorphism given in Theorem 6, but it is also not difficult to prove these directly using Theorem 16. (iii) follows from (i), since $K^* N_{L/K}(\mathbb{I}_L)$ is open in $\mathbb{I}_K$.

For (iv), let $A : \mathbb{I}_K \to Gal(L/K)$ be a homomorphism satisfying (i), (ii), and (iv). Each K_v^* inherits its topology as a subgroup of $\mathbb{I}_K$, so we can restrict A to a map $A_v : K_v^* \to G(L/K)$. Then A is just the product $\prod_v A_v$. When v is unramified and finite, $A_v : K_v^* \to Gal(L/K)$ does what we want by (iv).

When v is ramified and finite, restrict A_v to a continuous map $\mathcal{O}_v^* \to Gal(L/K)$. The preimage of $\{1\}$ is an open and closed subgroup of $\mathcal{O}_v^*$, necessarily containing $1 + \mathfrak{p}_v^n$ for some $n \geq 1$. We can enlarge n to a number n_v for which $1 + \mathfrak{p}_v^{n_v}$ is also contained in the group of local norms.

When v is infinite, the preimage of 1 under the map $K_v^* \to G(L/K)$ is an open and closed subgroup of K_v^*. If v is real, this can either be all of K_v^* or $(0, \infty)$. If v is complex, this has to be all of K_v^*.

In any case, we can restrict A to a homomorphism on

$$H_{\mathfrak{c}} = \prod_{v|\mathfrak{c}} W_v(\mathfrak{c}) \prod_{v \nmid \mathfrak{c}}{}' K_v^*$$

for a suitable admissible cycle $\mathfrak{c}$, and here A agrees with the global Artin map. Since $H_{\mathfrak{c}} K^* = \mathbb{I}_K$, A agrees with the global Artin map everywhere by (i).

□

Last, we will restate Proposition 1 for the idelic Artin map. The assertions are immediate.

Theorem 19. *Let L/K be abelian with Artin map $\Phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$. The following hold:*

(i) If σ is an embedding of L into $\overline{\mathbb{Q}}$ (not necessarily the identity on K), and $x \in \mathbb{I}_K$, then

$$\Phi_{\sigma L/\sigma K}(\sigma x) = \sigma \Phi_{L/K}(x) \sigma^{-1}$$

(ii) If L' is another abelian extension of K containing L, and $x \in \mathbb{I}_K$, then the restriction of $\Phi_{L'/K}(x)$ to L is $\Phi_{L/K}(x)$.

(iii) If E is a finite extension of K, and $y \in \mathbb{I}_E$, then the restriction of $\Phi_{LE/E}(y)$ to L is $\Phi_{L/K}(N_{E/K}(y))$.

(iv) If E is an intermediate field of L/K, and $y \in \mathbb{I}_E$, then $\Phi_{L/E}(y) = \Phi_{L/K}(N_{E/K}(y))$.

5 Class Groups and Class Fields

In the last section, we went to great lengths to define an idelic Artin map

$$\Phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

for L/K. This homomorphism is surjective, and its kernel is exactly $K^* N_{L/K}(\mathbb{I}_L)$. Since for $w \mid v$ the local norm maps L_w^* onto an open subgroup of K_v^*, one can see that $N_{L/K}(\mathbb{I}_L)$, and moreover $K^* N_{L/K}(\mathbb{I}_L)$, is an open subgroup of $\mathbb{I}_K$ containing K^*. We will show in this chapter that *every* open subgroup of $\mathbb{I}_K$ containing K^* is obtained from an abelian extension in this way.

In fact, the mapping

$$L \mapsto K^* N_{L/K}(\mathbb{I}_L)$$

is an order reversing bijection between finite abelian extensions of K and finite index open subgroups of $\mathbb{I}_K$ containing K^*. This is a remarkable fact, for it asserts that all information about abelian extensions of K are predicated on K's local information.

In Proposition 1, we will establish the injectivity of $L \mapsto K^* N_{L/K}(\mathbb{I}_L)$. Given L, we will refer to the kernel of the Artin map of L/K, i.e. $K^* N_{L/K}(\mathbb{I}_L)$, as the **class group** of L, and L as the **class field** of $K^* N_{L/K}(\mathbb{I}_L)$.

Proposition 1. *Let L_1, L_2 be finite abelian extensions of K with class groups H_1, H_2.*

(i) $H_1 \cap H_2$ is the class group of $L_1 L_2$.

(ii) $H_1 H_2$ is the class group of $L_1 \cap L_2$.

(iii) $L_1 \subseteq L_2$ implies $H_2 \subseteq H_1$

(iv) $H_2 \subseteq H_1$ implies $L_1 \subseteq L_2$.

(v) If E/K is finite and L/K is abelian with class group H, then $N_{E/K}^{-1}(H)$ is the class group of LE/E.

Proof. (i): Consider the composition

$$\mathbb{I}_K \xrightarrow{\Phi_{L_1 L_2/K}} \mathrm{Gal}(L_1 L_2/K) \xrightarrow{j} \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

where j is the injection $\sigma \mapsto (\sigma_{|L_1}, \sigma_{|L_2})$. By the consistency property,

$$j \circ \Phi_{L_1 L_2/K}(x) = (\Phi_{L_1/K}(x), \Phi_{L_2/K}(x))$$

so $(x, L_1 L_2/K) = 1$ if and only if $(x, L_1/K)$ and $(x, L_2/K)$ are both 1. Thus $H_1 \cap H_2$ is the kernel of the Artin map for $L_1 L_2/K$.

(ii): Let N be the class group of $L_1 \cap L_2$. Consistency (4, Proposition 1) tells us that H_1H_2 is contained in N. Now

$$[\mathbb{I}_K : H_1H_2] = \frac{[\mathbb{I}_K : H_1][\mathbb{I}_K : H_2]}{[\mathbb{I}_K : H_1 \cap H_2]} = \frac{[L_1 : K][L_2 : K]}{[L_1L_2 : K]} = [L_1 \cap L_2 : K]$$

$$= [\mathbb{I}_K : K^* N_{L_1 \cap L_2/K}(\mathbb{I}_{L_1 \cap L_2})]$$

which gives us equality. We have used (i), as well as Galois theory and basic group theory.

(iii): Suppose that $L_1 \subseteq L_2$. Since

$$N_{L_2/K}(\mathbb{I}_{L_2}) = N_{L_1/K}(N_{L_2/L_1}(\mathbb{I}_{L_2})) \subseteq N_{L_1/K}(\mathbb{I}_{L_1})$$

multiply both sides by K^* to get $H_2 \subseteq H_1$.

(iv): If $H_2 \subseteq H_1$, then $H_2 = H_1 \cap H_2$, so H_2 is the class group of L_1L_2 by (i). Thus $K^*N_{L_2/K}(\mathbb{I}_{L_1}) = H_2 = K^*N_{L_1L_2/K}(\mathbb{I}_{L_1L_2})$. Now the global norm index equality tells us that

$$[L_2 : K] = [\mathbb{I}_K : H_2] = [L_1L_2 : K]$$

so $L_2 = L_1L_2$, or $L_1 \subseteq L_2$.

(v): An element in $\mathrm{Gal}(LE/E)$ is the identity if and only if its restriction to L is the identity. But for any $x \in \mathbb{I}_E$,

$$(x, LE/E)_{|L} = (N_{E/K}(x), L/K)$$

so the assertion is obvious. □

We are a long way from proving the surjectivity of $L \mapsto K^*N_{L/K}(\mathbb{I}_L)$, but we can already find class fields of large subgroups of $\mathbb{I}_K$.

Lemma 2. *Let $H \subseteq H_1$ be open subgroups of $\mathbb{I}_K$ containing K^*. If H has a class field, then so does H_1. Specifically, if $H = K^*N_{L/K}(\mathbb{I}_L)$ for L/K abelian, then H_1 is the class group of the fixed field of H under the image of the $\Phi_{L/K}$.*

Proof. Let L_1 be the fixed field of $\Phi_{L/K}(H_1)$, so $\Phi_{L/K}(H_1) = \mathrm{Gal}(L/L_1)$. Since H_1 is a subgroup containing the kernel of $\Phi_{L/K}$, we have $H_1 = \Phi_{L/K}^{-1}(\Phi_{L/K}(H_1))$.

Now $\Phi_{L_1/K}$ is the restriction of $\Phi_{L/K}$ to L_1. So an $x \in \mathbb{I}_K$ lies in the kernel of $\Phi_{L_1/K}$ if and only if the restriction of $\Phi_{L/K}(x)$ to L_1 is trivial, if and only if $\Phi_{L/K}(x) \in \Phi_{L/K}(H_1)$, if and only if $x \in H_1$. □

5.1 Kummer Theory

We will briefly introduce the notion of duals in abelian groups, which is similar to that of dual vector spaces. There is a theory of duals over arbitrary modules, but there is no reason for us to introduce such a general concept. Let A, B be (multiplicative) abelian groups, and let

$$\tau : A \times B \to \mathbb{C}^*$$

be a bilinear mapping. This is to say that τ is a homomorphism in each slot (obviously this is different from saying that τ is a homomorphism from the product group). Normally, the dual of A (regarded as a $\mathbb{Z}$-module) is understood as the group $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z})$, but *here we will define the* ***dual*** *of A to be* $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^*)$. Denote the dual by A^*.

Lemma 3. *If A is finite, then $A^* \cong A$.*

Proof. If $|A| = m$, then a homomorphism from A into $\mathbb{C}^*$ is the same as a homomorphism into the group of mth roots of unity, which is cyclic of order m. So $A^* \cong \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}/m\mathbb{Z})$. We know that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$, where d is the greatest common divisor of m and n. Also finite direct sums commute with the functor $\mathrm{Hom}(-, \mathbb{Z}/m\mathbb{Z})$. It follows that if we decompose A into a direct sum of prime power cyclic groups $\mathbb{Z}/p^e\mathbb{Z}$ with $p^e \mid m$, we obtain the given isomorphism. □

Let n be an integer. We say that a (multiplicative) abelian group G has *exponent* n if $x^n = 1$ for all $x \in G$. An abelian extension of fields is said to be of exponent n if its Galois group is.

Let K be a number field, which contains all the nth roots of unity. If $a \in K$, and $\sqrt[n]{a} \in \mathbb{C}$ is an nth root of a (that is, a root of the polynomial $X^n - a$), then the remaining roots of $X^n - a$ are exactly $\sqrt[n]{a}\zeta^i, i = 1, 2, ..., n-1$ where $\zeta \in K$ is a primitive nth root of unity. So given an $a \in K^*$, either all or none of its n nth roots also lie in K^*.

The set

$$K^{*n} = \{x^n : x \in K^*\}$$

is a subgroup of K^*. It is the set of $a \in K$ whose nth roots all lie in K. Suppose D is a subgroup of K^*, with $K^{*n} \subseteq D$ and $[D : K^{*n}]$ finite. Let $\alpha_1, ..., \alpha_m$ be a set of coset representatives for K^{*n} in D, with $\sqrt[n]{\alpha_i} \in \mathbb{C}$ any nth root of α_i. We then set

$$K_D = K(\sqrt[n]{\alpha_1}, ..., \sqrt[n]{\alpha_m})$$

Since the nth roots of unity lie in K, we see that K_D/K is Galois, and is the same field regardless of the choice of nth root of any α_i. Furthermore each $K(\sqrt[n]{\alpha_i})$, and hence the composite K_D, is a finite abelian extension of exponent n of K (why?).

Finally, the choice of representatives α_i does not matter, because in fact K_D is equal to K adjoined with all the nth roots of all the elements of D. For if $\sqrt[n]{a}$ is an nth root of some $a \in D$,

we can write $a = x\alpha_i$ for some i and some $x \in K^{*n}$. Then $\sqrt[n]{a}$ is an nth root of x times an nth root of α_i, both of which lie in K_D.

Lemma 4. *Conversely, any finite abelian extension of K is equal to K_D for some subgroup $D \supseteq K^{*n}$ with $[D : K^{*n}]$ finite. The abelian extensions of K are then in bijection with the given subgroups.*

Proof. If L/K is abelian of exponent n, then L is a finite compositum of cyclic extensions, and every cyclic extension of K can be obtained by taking an nth root of an element in K (why?). So $L = K(\sqrt[n]{\alpha_1}, ..., \sqrt[n]{\alpha_n})$ with $\alpha_i \in K$. If we then let D be the subgroup of K^* generated by K^{*n} and $\alpha_1, ..., \alpha_n$, then $[D : K^{*n}]$ is finite with $L = K_D$.

We have established that the mapping $D \mapsto K_D$ is surjective, and injectivity is pretty clear. □

A pair (D, K_D) can also be understood as a pair (G, H), where $G = \mathrm{Gal}(K_D/K)$ and $H = K_D/K^{*n}$. For $\sigma \in G$ and $\bar{d} \in H$ for $d \in D$, we will define a bilinear mapping

$$\tau : G \times H \to \mathbb{C}^*$$

by $\tau(\sigma, d) = \frac{\sigma \sqrt[n]{d}}{\sqrt[n]{d}}$, where $\sqrt[n]{d}$ is an nth root of d. The choice of root $\sqrt[n]{d}$ does not matter: any other nth root of d is equal to $\zeta^k \sqrt[n]{d}$, and $\sigma(\zeta^k) = \zeta^k$. The choice of coset representative similarly does not matter.

Theorem 5. *There are natural isomorphisms*

$$G \cong H^*$$

and

$$H \cong G^*$$

Thus the groups G, H and their duals are all isomorphic to each other, and so

$$[K_D : K] = [D : K^{*n}]$$

Proof. Given $\sigma \in G$, we define $\sigma^* \in H^*$ by the formula $\sigma^*(\bar{d}) = \tau(\sigma, \bar{d})$. To show this homomorphism is injective, suppose that σ^* is the identity of H^*, which is to say that $\tau(\sigma, \bar{d}) = 1$ for every $\bar{d} \in H$. In other words, $\sigma \sqrt[n]{d} = \sqrt[n]{d}$ for every $d \in D$. Since K_D is generated by all nth roots of all elements of D, it follows that σ is the identity on K_D, which implies $\sigma = 1$ since K_D/K is Galois.

The injection $H \to G^*$ is similarly established. Combining a pigeonhole argument with Lemma 1, we see that the maps are also surjective, and we obtain the given isomorphisms.

□

5.2 The existence theorem

Proposition 6. *Let K be a number field which contains all the nth roots of unity, and S a finite set of places of K containing all the archimedean ones as well those which divide n. Also assume S is large enough so that $K^*\mathbb{I}_K^S = \mathbb{I}_K$. If x is an nth power in K_v^* for all $v \in S$, and $\mathrm{ord}_v(x) = 0$ for all $v \notin S$, then x is an nth power in K.*

Proof. Let $L = K(\sqrt[n]{x})$ for some nth root $\sqrt[n]{x}$ of x. Let v be a place of K which is not in S, and w a place of L lying over v. We claim that v is unramified in L. We can identify $L_w = K_v(\sqrt[n]{x})$. Since x is a unit at v, $\sqrt[n]{x}$ is an integral generator of L_w/K_v, so we can apply the theory of the different. Let $f(X) = X^n - x$, and $\mu(X)$ the minimal polynomial of $\sqrt[n]{x}$ over K_v. Then $\mu(X)$ divides $f(X)$, hence $\mu'(\sqrt[n]{x})$ divides $f'(\sqrt[n]{x}) = n\sqrt[n]{x}^{n-1}$. The different $\mathscr{D}(L_w/K_v)$ is the ideal of $\mathcal{O}_w$ generated by all $g'(\beta)$, where $\beta \in \mathcal{O}_w$, $L_w = K_v(\beta)$, and g is the minimal polynomial of β over K_v. Then

$$n\sqrt[n]{a}^{n-1}\mathcal{O}_L \subseteq \mu'(\sqrt[n]{a})\mathcal{O}_L \subseteq \mathscr{D}(L_w/K_v)$$

so

$$0 \leq \mathrm{ord}_w \mathscr{D}(L/K) \leq \mathrm{ord}_w(n\sqrt[n]{x}^{n-1}) = \mathrm{ord}_w(n) + (n-1)\,\mathrm{ord}_w(\sqrt[n]{x})$$

with $\mathrm{ord}_w(n) = \mathrm{ord}_v(n) = 0$, since all the places corresponding to primes dividing n are in S, and $\mathrm{ord}_w(\sqrt[n]{x}) = 0$ since x is a unit in O_v^*, and hence $\sqrt[n]{x}$ is a unit in O_w^*. Thus $\mathrm{ord}_w \mathscr{D}(L/K) = 0$, which implies that v is unramified. Thus the local norm $\mathcal{O}_w^* \to \mathcal{O}_v^*$ is surjective by the local norm index inequality.

Now, if v is in S, the fact that x is an nth power in K_v^* means that $L_w = K_v$ for any $w \mid v$. Thus v splits completely, and in fact we have shown that L/K is an unramified extension (so if $K = \mathbb{Q}$ and $n = 2$, we are already done). So the local norm $N_{w/v} : L_w \to K_v$ is surjective (actually, the identity map) for $v \in S$. We have ultimately shown that $\mathbb{I}_K^S \subseteq N_{L/K}(\mathbb{I}_L)$, which implies

$$\mathbb{I}_K = K^*\mathbb{I}_K^S \subseteq K^* N_{L/K}(\mathbb{I}_L)$$

and hence $\mathbb{I}_K = K^* N_{L/K}(\mathbb{I}_L)$. Thus $L = K$ by the global norm index equality.

□

Assume the hypothesis of the previous proposition. Recall that the S-units of K, denoted K_S, is the group consisting of all $x \in K^*$ for which $\mathrm{ord}_v(x) = 0$ for all $v \notin S$. If we identify K^* as being contained in the ideles, then K_S is the same thing as $K^* \cap \mathbb{I}_K^S$. Also, let

$$B = \prod_{v \in S} K_v^{*n} \prod_{v \notin S} \mathcal{O}_v^*$$

Proposition 7. *Assuming the hypothesis above, let s be the cardinality of S, and $L = K(\sqrt[n]{x} : x \in K_S)$. Then L is the class field of K^*B, and $[L : K] = n^s$.*

Proof. The field L is also equal to K adjoined with all the nth roots of $K^{*n}K_S$, so Kummer theory tells us that L/K is Galois of exponent n with $[L : K] = [K^{*n}K_S : K^{*n}]$. Obviously $K_S^n = K_S \cap K^{*n}$, and using the second isomorphism theorem we get

$$K^{*n}K_S/K^{*n} \cong K_S/(K^{*n} \cap K_S) = K_S/K_S^n$$

Let s be the cardinality of s. It is a corollary of the unit theorem (see 1, Corollary 3) that $[K_S : K_S^n] = n^s$.

We want to show that $K^*B = K^*N_{L/K}(\mathbb{I}_K)$. First, we claim that B and hence K^*B is contained in $K^*N_{L/K}(\mathbb{I}_K)$. To see this, note that by the same argument as in the previous lemma, any $v \notin S$ is unramified in L. For L is a finite compositum of fields of the form $K(\sqrt[n]{x})$ for $x \in K_S$, we proved that v was unramified in $K(\sqrt[n]{x})$, and a finite compositum of unramified extensions is unramified. Thus the local norm $N_{w/v} : \mathcal{O}_w^* \to \mathcal{O}_v^*$ is surjective for $v \notin S$. Also for $v \in S$, if $\alpha \in K_v^*$ is an nth power, the fact that $\mathrm{Gal}(L/K)$ has exponent n means that α (viewed as an idele) lies in the kernel of the Artin map, i.e. in $K^*N_{L/K}(\mathbb{I}_L)$. It follows that for $x \in B$, we may write x as

$$(\alpha_1^n, ..., \alpha_s^n, N_{w_1/v_1}(\alpha_{v_1}), N_{w_2/v_2}(\alpha_{v_2}), ...)$$

($v_1, v_2, ...$ are the places not in S), and this is clearly contained in $K^*N_{L/K}(\mathbb{I}_L)$.

Now that we have shown one inclusion, equality will follow once we show that the index $[\mathbb{I}_K : K^*B]$ is equal to $[\mathbb{I}_K : K^*N_{L/K}(\mathbb{I}_L)] = [L : K] = n^s$. The previous lemma tells us that $B \cap K^* = K_S^n$. Also $\mathbb{I}_K^S \cap K^* = K_S$, so $[\mathbb{I}_K^S \cap K^* : B \cap K^*] = [K_S : K_S^n]$, which as we said equals n^s.

Also, $\mathbb{I}_K^S$ modulo B is clearly isomorphic to $\prod_{v \in S} K_v^*/K_v^{*n}$. Since K contains the nth roots of unity, the formula from 3, Theorem 10 tells us that $[K_v^* : K_v^{*n}] = \frac{n^2}{||n||_v}$. We specified that n is a unit outside of S, so the product formula tells us that $1 = \prod_{v \in S} ||n||_v$. Hence

$$[\mathbb{I}_K^S : B] = \prod_{v \in S} \frac{n^2}{||n||_v} = n^{2s}$$

We then have

$$[\mathbb{I}_K : K^*B] = [K^*\mathbb{I}_K^S : K^*B] = \frac{[\mathbb{I}_K^S : B]}{[\mathbb{I}_K^S \cap K^* : B \cap K^*]} = \frac{n^{2s}}{n^s} = n^s$$

□

Corollary 8. *Let K be a number field which contains the nth roots of unity, and H an open*

subgroup of $\mathbb{I}_K$ which contains K^*. If $\mathbb{I}_K/H$ has exponent n, then H has a class field.

Proof. The nth power of any idele will be in H. Take S, B as in the previous proposition. Recall that we may embed K_v^* in $\mathbb{I}_K$ by the mapping $x \mapsto (..., 1, x, 1, ...)$. Under this mapping, we have $\mathcal{O}_v^* \subseteq H$ for almost all v (why?), so we may enlarge S to include all those v for which this is not the case. Let $S = \{v_1, ..., v_t\}$. Given an $x \in B$, we may write x as

$$y \cdot \prod_{i=1}^{t} (..., 1, x_{v_i}, 1, ...)$$

where $y_v = 1$ for $v \in S$ and $y_v \in \mathcal{O}_v^*$ for $v \notin S$. The elements x_{v_i} are nth powers, so we can plainly see that $x \in H$. So B, and hence K^*B, is contained in H. By Lemma 2, the fact that K^*B has a class field means that H also has one.

□

We're now ready to prove the surjectivity of the mapping $L \mapsto K^*\mathbb{I}_K$. But before we do, we prove another result which will be used in local class field theory. Although logically the statement of following proposition belongs in the next section, its proof is so similar to the arguments in Proposition 7 that we place it here.

Proposition 9. *Let L/K be abelian with class field H, and v_0 a place of K for which $K_{v_0}^* \subseteq H$. Assume that K contains the nth roots of unity and $\mathrm{Gal}(L/K) \cong \mathbb{I}_K/H$ has exponent n. Then v_0 splits completely in L.*

Proof. The proposition is still true if we don't assume that K contains the nth roots of unity or that L/K has exponent n. The general case will be proved with local class field theory, and Lang's proof (which we are following) requires this special case.

Let S be a finite set of places containing v_0, all the archimedean and ramified places, all those dividing n, and enough other places so that $\mathbb{I}_K = K^*\mathbb{I}_K^S$. We let

$$B_1 = K_{v_0}^* \times \prod_{v \in S \setminus \{v_0\}} K_v^{*n} \times \prod_{v \notin S} \mathcal{O}_v^*$$

$$B_2 = K_{v_0}^{*n} \times \prod_{v \in S \setminus \{v_0\}} K_v^* \times \prod_{v \notin S} \mathcal{O}_v^*$$

$$B = \prod_{v \in S} K_v^{*n} \prod_{v \notin S} \mathcal{O}_v^*$$

We see that $B_1 \cap B_2 = B$. We will use the same computations involving B which we did in Proposition 7. Since $\mathbb{I}_K/H$ has exponent n, we have $K^*B_1 \subseteq H$ (just look at it locally), so the

class field L_1 to K^*B_1 contains L. We will construct L_1 explicitly and show that v_0 splits completely here. What we want will follow: v_0 will split completely in L.

Let $D_1 = K^* \cap B_1$ and $D_2 = K^* \cap B_2$. We have

$$K_S^n \subseteq D_1 \cap K^{*n} \subseteq B \cap K^{*n} = K_S^n$$

where the last equality follows from Proposition 6. Hence $D_1 \cap K^{*n} = K_S^n$, and by an identical argument, $D_2 \cap K^{*n} = K_S^n$.

Now, consider the fields $K(\sqrt[n]{D_1})$ and $K(\sqrt[n]{D_2})$. We have

$$[K(\sqrt[n]{D_2}) : K] = [D_2K^{*n} : K^{*n}] = [D_2 : D_2 \cap K^{*n}] = [D_2 : K_S^n]$$

where the first equality is the correspondence from Kummer theory. By an identical argument, $[K(\sqrt[n]{D_1}) : K] = [D_1 : K_S^n]$.

We let H_1 be the class field of $K(\sqrt[n]{D_2})/K$. By a standard argument, for example the one invoked in the proof of Proposition 7, $K(\sqrt[n]{D_2})/K$ is unramified outside of S. Also, v_0 splits completely in $K(\sqrt[n]{D_2})$. This is clear, because $K_{v_0}(\sqrt[n]{D_2})/K_{v_0}$ is obtained from K_{v_0} by adjoining roots of the equation $X^n - x$, where $x \in D_2$ is already an nth power in K_{v_0}. Thus $K^*B_1 \subseteq H_1$ (just look at it locally; clearly $K_{v_0}^*$ is contained in the kernel of the Artin map, since any element therein is trivially a local norm). Thus

$$[K(\sqrt[n]{D_2}) : K] = [\mathbb{I}_K : H_1] \leq [\mathbb{I}_K : K^*B_1]$$

$$= [K^*\mathbb{I}_K^S : K^*B_1] = \frac{[\mathbb{I}_K : B_1]}{[K^* \cap \mathbb{I}_K^S : K^* \cap B_1]}$$

Now $\mathbb{I}_K^S/B_1$ is clearly isomorphic to $\prod_{v \in S \setminus \{v_0\}} K_v^*/K_v^{*n}$. Also,

$$[K^* \cap \mathbb{I}_K^S : K^* \cap B_1] = [K_S : D_1] = \frac{[K_S : K_S^n]}{[D_1 : K_S^n]} = \frac{n^s}{[K(\sqrt[n]{D_1}) : K]}$$

where s is the cardinality of S. The numerator of this last expression comes from the unit theorem, and the denominator we just proved from Kummer theory. Thus

$$[K(\sqrt[n]{D_2}) : K] \leq [\mathbb{I}_K : K^*B_1] \leq \frac{\prod_{v \in S \setminus \{v_0\}} [K_v^* : K_v^{*n}]}{n^s} [K(\sqrt[n]{D_1}) : K]$$

By an identical argument, $K(\sqrt[n]{D_1})/K$ is unramified outside of S, with all the places in $S \setminus \{v_0\}$

splitting completely, so the class field of $K(\sqrt[n]{D_1})/K$ contains K^*B_2, getting us

$$[K(\sqrt[n]{D_1}):K] \leq [\mathbb{I}_K : K^*B_2] = \frac{[K_{v_0}^* : K_{v_0}^{*n}]}{n^s}[K(\sqrt[n]{D_2}):K]$$

By Proposition 7, $\prod_{v\in S}[K_v^* : K_v^{*n}] = n^{2s}$, so we multiply to get

$$[K(\sqrt[n]{D_2}):K][K(\sqrt[n]{D_1}):K] \leq [\mathbb{I}_K : K^*B_1][\mathbb{I}_K : B_2] \leq [K(\sqrt[n]{D_1}):K][K(\sqrt[n]{D_2}):K]$$

so we must have equality. Not only above: we can see that every inequality we have written in the proof must be an equality. In particular, $[\mathbb{I}_K : H_1] = [\mathbb{I}_K : K^*B_1]$, so K^*B_1 must be the class field of $K(\sqrt[n]{D_2})$. Since v_0 splits completely in $K(\sqrt[n]{D_2})$, we are done.

□

Theorem 10. *(Takagi existence theorem) Let K be a number field, and H an open subgroup of $\mathbb{I}_K$ containing K^*. Then H has a class field.*

Proof. We prove a special case first. Suppose L is a cyclic extension of K. Since H contains K^*, the preimage $N_{L/K}^{-1}(H)$ is an open subgroup of $\mathbb{I}_L$ containing L^*. We claim that if $N_{L/K}^{-1}(H)$ has a class field (over L), then H will also have a class field over K. For suppose F/L is the class field of $N_{L/K}^{-1}(H)$, so $N_{L/K}^{-1}(H) = L^*N_{F/L}(\mathbb{I}_F)$. We have

$$N_{F/K}(\mathbb{I}_F) = N_{L/K}(N_{F/L}(\mathbb{I}_F)) \subseteq N_{L/K}(L^*N_{F/L}(\mathbb{I}_F)) = N_{L/K}(N_{L/K}^{-1}(H)) \subseteq H$$

and so $K^*N_{F/K}(\mathbb{I}_F) \subseteq H$. We will want to use Lemma 4 to conclude that H has a class field (namely the fixed field of the image of H under the Artin map $\Phi_{F/K}$). But we can only do this we establish that F/K is abelian.

To show F/K is Galois, let ϕ be a K-embedding of F into $\mathbb{C}$. It suffices to show that $\phi(F) = F$. Since ϕ maps L to itself, it also uniquely extends to a K_v-automorphism of F_w for any extension of places $w \mid v$. It is easy to see then that $\phi N_{L/K}^{-1}(H) = N_{L/K}^{-1}(H)$. We remarked earlier that $\phi N_{L/K}^{-1}(H)$ will be the class field of $\phi(F)$ over $\phi(L) = L$. By uniqueness, it follows that $\phi(L) = L$.

To show F/K is abelian, we already know that $\mathrm{Gal}(F/L)$ is abelian. So it suffices to show that $\tau\sigma = \sigma\tau$, where τ is an arbitrary element of $\mathrm{Gal}(F/L)$ and σ is an element of $\mathrm{Gal}(F/K)$ whose restriction to L generates $\mathrm{Gal}(L/K)$. The Artin map is surjective, so we can find an $x \in \mathbb{I}_L$ for which $\tau = (x, F/L)$. The idele norm $N_{L/K}$ of $\sigma(x)/x$ is $1 \in H$, so $x \in N_{L/K}^{-1}(H)$. But $N_{L/K}^{-1}(H)$ is the kernel of the Artin map $\Phi_{F/L}$, so $(\sigma(x), F/L)) = (x, F/L)$. Thus:

$$\sigma\tau\sigma^{-1} = \sigma(x, F/L)\sigma^{-1} = (\sigma(x), \sigma(F)/\sigma(L)) = (\sigma(x), F/L) = \sigma$$

For the general case, we know that $\mathbb{I}_K/H$ is finite, so it must have some exponent n. Letting ζ

be a primitive nth root of unity, there exist fields $F_1, F_2, ...$ such that each extension in the chain

$$K \subseteq F_1 \subseteq \cdots \subseteq F_r = K(\zeta)$$

is cyclic. The group $H_1 = N^{-1}_{K(\zeta)/K}(H)$ is an open subgroup of $\mathbb{I}_{K(\zeta)}$ which contains $K(\zeta)^*$, and furthermore one can see that $\mathbb{I}_{K(\zeta)}/H_1$ has exponent n. Thus H_1 has a class field over $F_r = K(\zeta)$ by Corollary 6. But

$$H_1 = N^{-1}_{F_r/F_{r-1}}(N^{-1}_{F_{r-1}/K}(H))$$

with F_r/F_{r-1} cyclic, so the argument we have given just above shows that $N^{-1}_{F_{r-1}/K}(H)$ has a class field over F_{r-1}. But

$$N^{-1}_{F_{r-1}/K}(H) = N^{-1}_{F_{r-1}/F_{r-2}}(N^{-1}_{F_{r-2}/K}(H))$$

with F_{r-1}/F_{r-2} cyclic, so $N^{-1}_{F_{r-2}/K}(H)$ has a class field over F_{r-2}. Iterating this argument, we obtain a class field for H.

□

6 Some local class field theory

In global class field theory, one gives a correspondence between abelian extensions of a given number field K and open subgroups of the ideles which contain K^*. Local class field theory gives an analogous correspondence between abelian extensions of a given local field and open subgroups of its units. We will not prove all the main theorems of local class field theory. We will, however, prove the main results about local norm index equalities.

To begin with, we recall that every finite extension of $\mathbb{Q}_p$ occurs as the completion of some number field. In fact, every abelian extension of p-adic fields E/F can be obtained from an abelian extension of global fields. To see this, let L_0 be a number field whose completion at some place w_0 is E. We can regard L_0 as a dense subfield of E. Then let L be the composite of all σL_0, where $\sigma \in \mathrm{Gal}(E/F)$. Then L is also dense in E, and if we take K to be the fixed field of $\mathrm{Gal}(E/F)$ in L, then K will be dense in F. Then w_0 lies over a place v of K for which $K_v = F$, and we also have $L_w = E$ for any w lying over w_0. Work out the details as an exercise.

Thus to discuss abelian extensions of local fields, we will begin by taking abelian extensions of number fields. This allows us to bring in machinery from global class field theory.

Lemma 1. *Let L/K be an abelian extension of number fields. If v is a place of K which splits completely in L, then $K_v^* \subseteq K^* N_{L/K}(\mathbb{I}_L)$.*

Proof. For a place w of L lying over v, we have $L_w = K_v$, so the local norm $N_{w/v}$ is just the identity map. Thus any $x \in K_v^*$ is equal to the norm of the local idele $(x, 1, ..., 1) \in \bigoplus_{w|v} L_w^*$.

The converse is also true, but it is harder to prove. We do it later this in this section. □

Just as we have defined a global Artin map $\Phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$, for places w/v we will define a corresponding **local Artin map** $\Phi_{w/v} : K_v^* \to \mathrm{Gal}(L_w/K_v)$. There is a natural way to define this from the global map, namely via the composition

$$K_v^* \to \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

The Galois group of L_w/K_v is essentially just the decomposition group $\mathrm{Gal}(L/K)_v$, each K-automorphism of L therein extending uniquely to a K_v-automorphism of L_w. Our first goal is then to show that the above composition actually maps K_v^* into the decomposition group. This is done as follows:

Let Z be the decomposition field. For an $x \in K_v^*$, we want to show that $(x, L/K)$ is in $\mathrm{Gal}(L/K)_v$. Since v splits completely in Z, $x = N_{Z/K}(y)$ for some $y \in \mathbb{I}_Z$. But then

$$(x, L/K) = (N_{Z/K}(y), LZ/K) = (y, L/Z) \in \mathrm{Gal}(L/Z) = \mathrm{Gal}(L/K)_v$$

When v is unramified, it is easy to see what the Artin map does: there exists an admissible subgroup W depending on a set S containing only ramified places, so $\Phi_{w/v}(u\pi_v^m) = (\mathfrak{p}_v, L/K)^m$. When v is ramified, the local map is more mysterious. Given an $x \in K_v^*$, one finds some $y \in K_v^*$ for which the product xy lies in H, so then $\Phi(x) = \prod_{v' \notin S} (\mathfrak{p}_{v'}, L/K)^{\mathrm{ord}_{v'}(xy)}$. Other treatments of local class field theory give a more explicit description of the local Artin map.

The main result proved in the next theorem immediately gives the full complete splitting theorem. But its proof makes use of the special case we just considered.

Proposition 2. *Let L/K be abelian, v a place of K. The local Artin map $K_v \to \mathrm{Gal}(L/K)_v$ is surjective.*

Proof. Let Z be the decomposition field of v in L/K. If the image of K_v^* under the Artin map is properly contained in $\mathrm{Gal}(L/K)_v = \mathrm{Gal}(L/Z)$, then the fixed field of this image properly contains Z. We may then find a subfield F of this latter fixed field which has prime degree p over Z.

Let v_0 be a place of Z lying over v. Since v splits completely in Z, the fields K_v and Z_{v_0} are the same.

It follows that if the local Artin map $K_v^* \to \mathrm{Gal}(L/K)_v$ is not surjective, neither is the composition $Z_{v_0}^* \to \mathbb{I}_Z \to \mathrm{Gal}(L/Z)$. Hence neither is the composition $Z_{v_0}^* \to \mathbb{I}_Z \to \mathrm{Gal}(F/Z)$. But $\mathrm{Gal}(F/Z)$ has prime order, so the map we just mentioned is trivial.

Now, let ζ be a primitive pth root of unity, and v_1 a place of $Z(\zeta)$ lying over v_0. If $x \in Z(\zeta)_{v_1}^*$, then the restriction of $(x, F(\zeta)/Z(\zeta))$ to F is

$$(N_{Z(\zeta)/Z}(x), F/Z) = (N_{v_1/v_0}(x), F/Z) = 1$$

Thus $(x, F(\zeta)/Z(\zeta))$ is trivial on F and, since it already fixes ζ, it must be the identity on $F(\zeta)$. Hence the Artin map $\Phi_{F(\zeta)/Z(\zeta)}$ is trivial on $Z(\zeta)_{v_1}^*$, i.e. $Z(\zeta)_{v_1}^*$ is contained in the class group of $F(\zeta)/Z(\zeta)$.

Of course $Z(\zeta)$ contains the pth roots of unity. And $\mathbb{I}_{Z(\zeta)}$ modulo $Z(\zeta)^* N_{F(\zeta)/Z(\zeta)}(\mathbb{I}_{F(\zeta)})$ has exponent p. This is clear, because any extension of completions of $F(\zeta)$ over $Z(\zeta)$ has degree either 1 or p. So we may apply the case of the splitting theorem we just proved above to get that v_1 must split completely in $F(\zeta)$. Now, $e_v(F/K) = e_{v_0}(F/Z)$ divides

$$e_v(F(\zeta)/Z) = e_v(F(\zeta)/Z(\zeta)) e(Z(\zeta)/Z) = e(Z(\zeta)/Z)$$

which itself divides $[Z(\zeta) : Z]$, which divides $p - 1$. But $e_v(F/Z)$ is either 1 or p, so it must be 1. Similarly the inertia $f_v(F/Z)$ is 1. Thus v splits completely in F, which is a contradiction, since Z is the largest subfield of L in which v splits completely.

□

Corollary 3. *(Complete splitting theorem Let L/K be an abelian extension, and v a place of K. Then v splits completely in L if and only if K_v^* is contained in the class group of L/K.*

Proof. We already proved the implication $\Rightarrow$. Conversely if K_v^* is contained in the class group of L/K, i.e. the kernel of the Artin map $\Phi_{L/K}$, then $(x, L/K) = 1$ for all $x \in K_v^*$. But every member of $\mathrm{Gal}(L/K)_v$ is mapped to by some $x \in K_v^*$ by the previous theorem. Hence $\mathrm{Gal}(L/K)_v$ is trivial, i.e. v splits completely. □

Corollary 4. *For an abelian extension of p-adic fields K/k, we have*

$$[K : k] = [k^* : N_{K/k}(K^*)]$$

Proof. This local principle is proved using global arguments, so let us write our extension of fields L_w/K_v as we have been instead of K/k. We already have "half" of each of the three claims, namely the local norm inequalities and the fact that $N_{w/v}(L_w^*)$ is clearly contained in the kernel of the Artin map. By the surjectivity in Proposition 12 we have:

$$[L_w : K_v] = |\operatorname{Gal}(L_w/K_v)| = [K_v^* : \operatorname{Ker} \Phi_{w/v}] \leq [K_v^* : N_{w/v}(L_w^*)] \leq [L_w : K_v]$$

This also shows that $N_{w/v}(L_w^*)$ is exactly the kernel of the local Artin map. □

Just as we have formulated a local condition for v to split completely, we also have a local condition on when v is merely unramified.

Theorem 5. *The image of $\mathcal{O}_v^*$ under the local Artin map is the inertia group. Moreover, if $H = K^* N_{L/K}(\mathbb{I}_L)$, then v is unramified if and only if $\mathcal{O}_v^* \subseteq H$.*

Proof. Let T be the inertia field, and $w/v'/v$ an extension of places for $K \subseteq T \subseteq L$. All the ramification of v occurs in the extension L/T, which has degree $e(w/v) = e(w/v')$. Hence if we take a prime element in L_w and apply the norm $N_{w/v'}$, we obtain an associate in $\mathcal{O}_{v'}$ of its $e(w/v')$th power, which is prime in $\mathcal{O}_{v'}$. So there is a uniformizer π of T which is a norm, i.e. which is in the kernel of the local Artin map $T_{v'}^* \to \mathrm{Gal}(L/T)_{v'} = \mathrm{Gal}(L/T)$ (all the splitting happens in T/K, so $\mathrm{Gal}(L/T)$ is its own decomposition group with respect to v').

We know that the local Artin map is surjective, and here the map is trivial on a uniformizer. It follows that surjectivity is accomplished by the units $\mathcal{O}_{v'}^*$, i.e. the image of $\mathcal{O}_{v'}^*$ under the Artin map of L/T is $\mathrm{Gal}(L/T)$. But the image of $\mathcal{O}_{v'}^*$ under the Artin map of L/T is the same as the image of $N_{T/K}(\mathcal{O}_{v'}^*) = N_{v'/v}(\mathcal{O}_{v'}^*)$ under the Artin map of L/K. The fact that v is unramified in T gives us that $N_{v'/v}(\mathcal{O}_{v'}^*) = \mathcal{O}_v^*$, so the first claim is proved.

For the second claim, the fact that the mapping from $\mathcal{O}_v^*$ to the inertia group is surjective means that $\mathcal{O}_v^*$ is contained in H if and only if the inertia group is trivial, if and only if v is unramified. □

Corollary 6. *For an abelian extension of p-adic fields K/k, we have*

$$[\mathcal{O}_k^* : N_{K/k}(\mathcal{O}_K^*)] = e(K/k)$$

The main result of local class field theory (if we avoid infinite extensions) is this:

Let E be a p-adic field. If F is a finite abelian extension of E, there is a well defined surjective homomorphism $E^* \to \mathrm{Gal}(F/E)$, called the local Artin map, whose kernel is $N_{F/E}(F^*)$. The map $F \mapsto F^*$ gives an order preserving bijection between open subgroups of $\mathcal{O}_E^*$ and finite abelian extensions of E.

As far as we know, we cannot *quite* prove the main result of local class field theory using the global ones. Everything we are doing is in terms of global parameters. We obtain the local Artin map for an abelian extension of local fields E/F by assuming $E = L_w, F = K_v$, and L/K abelian. The local Artin map $F^* \to \mathrm{Gal}(E/F)$ is then just the restriction of the global Artin map from L/K. So we have the immediate problem of showing that this local map is independent of the global parameters. We were unsuccessful in proving this. Let us state the result we want.

Theorem 7. *Let E/F be an abelian extension of p-adic fields. The Artin map $\Phi_{E/F} : F^* \to \mathrm{Gal}(E/F)$ is defined by finding an abelian extension of number fields L/K and an extension of places $w \mid v$ such that $L_w = E$ and $K_v = F$. The Artin map is independent of the chosen global extension L/K.*

The usual way of resolving this problem is to develop local class field theory in a purely local fashion, e.g. Lubin-Tate formal groups. Assuming this is done, we easily get the following results:

Proposition 8. *Let E/F be an abelian extension of p-adic fields. The following properties hold:*

(i) If $\sigma : E \to \overline{F}$ is an embedding (not necessarily the identity on F), and $x \in F^*$, then $\Phi_{\sigma E/\sigma F}(\sigma x) = \sigma \Phi_{E/F}(x) \sigma^{-1}$.

(ii) If E' is an abelian extension of F containing E, and $x \in F^*$, then the restriction of $\Phi_{E'/F}(x)$ to E is $\Phi(E/F)$.

(iii) If M is a finite extension of F, and $y \in M^*$, then the restriction of $\Phi_{ME/M}(y)$ to F is $\Phi_{E/F}(N_{M/F}(y))$.

(iv) If M is an intermediate field of E/F, and $y \in M^*$, then the restriction of $\Phi_{E/M}(y)$ to K is $\Phi_{E/F}(N_{M/F}(y))$.

Proof. Restrict the global Artin map. □

We know that the kernel of the Artin map $\Phi_{E/F} : F^* \to \mathrm{Gal}(E/F)$ is $N_{E/F}(E^*)$. As in the

global case, we call $N_{E/F}(E^*)$ the class group belonging to E, and E the class field of the open subgroup $N_{E/F}(E^*)$.

Proposition 9. *The map $E \mapsto N_{E/F}(E^*)$ gives an order preserving injection from the (finite) abelian extensions of F into the open subgroups of F^*. The class group of a compositum (resp. intersection) of abelian extensions is the intersection (resp. compositum) of the class groups.*

Proof. Same as in the global case. □

The surjectivity of the correspondence $E \mapsto N_{E/F}(E^*)$ is, as in Section 5, the difficult part. Given an open subgroup H of finite index in F^*, we want to find an abelian extension E of F for which $N_{E/F}(E^*) = H$. Fortunately, the proofs from 5, Lemma 2 and 5, Theorem 10 carry over identically to local fields, and allow us to reduce to the case where F contains the nth roots of unity, and H is of exponent n (that is, $F^{*n} \subseteq H$).

Theorem 10. *The correspondence $E \mapsto N_{E/F}(E^*)$ is surjective.*

Proof. We just mentioned how to reduce the problem to where F contains the nth roots of unity, and our given open subgroup H of finite index in F^*, which we want to show is the norm group of some finite abelian extension, can be assumed to contain F^{*n}. As in 5, Lemma 2, all we have to do is argue that F^{*n} itself has a class field. Let E be the adjunction to F of all the nth roots of elements of F. By Kummer theory, this is a finite abelian extension of F with

$$[F^* : F^{*n}] = [E : F] = |\operatorname{Gal}(E/F)|$$

Now $\operatorname{Gal}(E/F)$ has exponent n, so F^{*n} is contained in the kernel $K = N_{E/F}(E^*)$ of the Artin map for E/F. But also

$$[E : F] = [F^* : K]$$

so in fact $F^{*n} = K$. □

7 Applications of global class field theory

7.1 The Kronecker-Weber theorem

Let $\mathfrak{c}$ be a cycle of K. Without reference to any admissibility, we can define the subgroups $H_\mathfrak{c}, W_\mathfrak{c} \subseteq \mathbb{I}_K$ defined earlier. Now $W_\mathfrak{c}$ is open, so $K^*W_\mathfrak{c}$ is an open subgroup of $\mathbb{I}_K$ containing K^*. Hence there exists a unique class field M to $K^*W_\mathfrak{c}$, this is to say a finite abelian extension of K such that $K^*W_\mathfrak{c}$ is the kernel of the Artin map for M/K. We call M the **ray class field** of $\mathfrak{c}$. There is *not* a bijection between cycles and abelian extensions: we can have $K^*W_\mathfrak{c} = K^*W_{\mathfrak{c}'}$ for a different cycle $\mathfrak{c}'$.

Proposition 1. *Let L be another abelian extension of K. Then $L \subseteq M$ if and only if $\mathfrak{c}$ is admissible for L/K.*

Proof. First suppose that $\mathfrak{c}$ is admissible for L/K. Then, the Artin map for L/K is trivial on $W_\mathfrak{c}$. Just look at how the Artin map is defined on the ideles. Thus the Artin map for L/K is trivial on $K^*W_\mathfrak{c}$. Thus the kernel of the Artin map for M/K is contained in the kernel of that for L/K. By the order reversing correspondence of class groups and class fields, we get $L \subseteq M$.

Conversely, suppose that $L \subseteq M$. Recall our definition of $W_\mathfrak{c}$:

$$W_\mathfrak{c} = \prod_{v|\mathfrak{c}} W_\mathfrak{c}(v) \prod_{v\nmid\mathfrak{c}} U_v$$

where $W_\mathfrak{c}$ is $1 + \mathfrak{p}_v^{\mathfrak{c}(v)}$ or $(0, \infty)$, and U_v is $\mathcal{O}_v^*$ or K_v^*, depending on whether v is finite or infinite. Already the generalized ramified places of L/K divide $\mathfrak{c}$: if v ramifies in L, then it ramifies in M, and it is clear that $\mathfrak{c}$ has to be divisible by all the generalized ramified places of M/K in order for $W_\mathfrak{c}$ to be contained in the kernel of the Artin map on M/K. For if v ramifies in M, then the local Artin map for M/K on $\mathcal{O}_v^*$ (or K_v^* if v is real and ramified) is not the trivial map.

For $v \mid \mathfrak{c}$, let $x \in W_\mathfrak{c}(v)$. To complete the proof that $\mathfrak{c}$ is admissible, we must show that x is a local norm at v. If we look at the idele $\alpha = (x, 1, 1, ...) \in W_\mathfrak{c}$, then $\Phi_{M/K}(\alpha)$, and hence $\Phi_{L/K}(\alpha)$, is trivial. But for $w \mid v$, we have

$$1 = \Phi_{M/K}(\alpha) = \Phi_{w/v}(x)$$

where $\Phi_{w/v}$ is the local Artin map. But the kernel of the local Artin map for L_w/K_v is the norm group of L_w^*, so x must be a norm.

□

This proposition gives a clearer picture of why admissibility is important. Earlier, we saw it was essential to the transfer principle between ideles and ideals, and now, we see it as a tool in classifying abelian extensions: any open subgroup of $\mathbb{I}_K$ contains $W_\mathfrak{c}$ for some large subgroup $\mathfrak{c}$ (prove this as an exercise), so every abelian extension of K is contained in a ray class field.

Proposition 2. *Let $\mathfrak{c}$ be a cycle of K. There are isomorphisms*

$$\mathbb{I}_K/K^*W_{\mathfrak{c}} \cong H_{\mathfrak{c}}/(K^* \cap H_{\mathfrak{c}})W_{\mathfrak{c}} \cong \mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}}$$

Proof. For the first map, we have a surjective homomorphism

$$H_{\mathfrak{c}} \to \mathbb{I}_K/K^*W_{\mathfrak{c}}$$

by the identity $\mathbb{I}_K = K^*H_{\mathfrak{c}}$. The kernel of this map is $H_{\mathfrak{c}} \cap K^*W_{\mathfrak{c}}$, which clearly contains $(K^* \cap H_{\mathfrak{c}})W_{\mathfrak{c}}$. Conversely if $x\alpha \in H_{\mathfrak{c}} \cap K^*W_{\mathfrak{c}}$ for $x \in K^*$ and $\alpha \in W_{\mathfrak{c}} \subseteq H_{\mathfrak{c}}$, then x is in $H_{\mathfrak{c}}$, hence $K^*H_{\mathfrak{c}}$. This establishes the first isomorphism.

The second isomorphism is even easier to establish. □

The next theorem gives a very important example of a ray class field. We will prove it using a cardinality argument, the previous lemma, and the following ray class group: if m is an integer, and $\mathfrak{c}$ is the cycle of $\mathbb{Q}$ which is the formal product of m and the unique infinite place of $\mathbb{Q}$, then the quotient $\mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$.

To see this, note that we can identify $\mathrm{Id} = \mathrm{Id}(\mathbb{Q})$ with the group of nonzero rational numbers, and under this identification, $\mathrm{Id}(\mathfrak{c})$ consists of those positive rational numbers which are units at the primes dividing m. Any positive rational number $\frac{a}{b}$, for $a, b \in \mathbb{N}$, Then $P_{\mathfrak{c}}$ just consists of those positive rational numbers $\frac{a}{b}$ (for $a, b \in \mathbb{N}$) with $ab^{-1} \equiv 1 \pmod{m}$, where b^{-1} is an inverse of b modulo m. Thus $P_{\mathfrak{c}}$ is the kernel of the surjective homomorphism

$$\mathrm{Id}(\mathfrak{c}) \to (\mathbb{Z}/m\mathbb{Z})^*, \frac{a}{b} \mapsto ab^{-1}$$

If $\mathfrak{c}$ consisted only of m, and not the infinite place, then $\mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$ modulo the subgroup $\{1, -1\}$.

Proposition 3. *Let $K = \mathbb{Q}$, and let m be an integer. Let $\mathfrak{c}$ be the cycle which is the formal product of m with the unique infinite place. Then $\mathbb{Q}(\zeta_m)$ is the ray class field of $\mathbb{Q}^*W_{\mathfrak{c}}$.*

Proof. First suppose that m is a prime power, say p^e. Since we do not yet know that $\mathfrak{c}$ is admissible, let e_1 be a larger integer than e such that $\mathfrak{c}_1$, the formal product of p^{e_1} with the unique infinite place, is admissible for $\mathbb{Q}(\zeta_m)$. Let $x \in 1 + p^e\mathbb{Z}_p$. If we look at the idele $\alpha = (x, 1, 1, ...)$, we can fine-tune the proof of (?) to produce a *positive integer* a with the property that $a\alpha \equiv 1 \pmod{{}^*\mathfrak{c}_1}$ (and hence $a\alpha \equiv 1 \pmod{{}^*\mathfrak{c}}$). In that case, we know how to compute the Artin map of $a\alpha = (ax, a, a, ...)$. It is just the map

$$\zeta_{p^e} \mapsto \zeta_{p^e}^a$$

Now ax and x are both $\equiv 1 \pmod{p^e}$. We can conclude that $a \equiv 1 \pmod{p^e}$ as well. Hence

$\zeta_{p^e}^a = \zeta_{p^e}$, and we then have

$$\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(x,1,1,...) = \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(ax,a,a,...) = (\zeta_{p^e} \mapsto \zeta_{p^e}^a) = 1$$

Similarly if x is a positive real number, one can see that the Artin map on $(...,1,1,x)$ is the identity. This proves that $W_{\mathfrak{c}}$, and hence $\mathbb{Q}^* W_{\mathfrak{c}}$, is contained in the kernel of the Artin map on $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ in the prime power case.

Now we return to the general case. Write $m = p_1^{e_1} \cdots p_s^{e_s}$, and let $\mathfrak{c}$ be as we defined it above: the formal product of m with the infinite place. For any i, let $x \in 1 + p_i^{e_i}\mathbb{Z}_{p_i}$. Interpret x as the idele $(x,1,1...)$. The restriction of $(x, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ to $\mathbb{Q}(\zeta_{p_i^{e_i}})$ is $(x, \mathbb{Q}(\zeta_{p_i^{e_i}})/\mathbb{Q})$, and we just proved this to be trivial. For $j \neq i$, the restriction of $(x, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ to $\mathbb{Q}(\zeta_{p_j^{e_j}})$ is still the identity, because p_i is unramified in $\mathbb{Q}(\zeta_{p_j^{e_j}}$, and x is a unit here at p_i. If x is a positive real number, it's easy to see that $(x, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ is trivial. This shows, by multiplicativity, that the Artin map for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is trivial on $W_{\mathfrak{c}}$. Thus

$$\mathbb{Q}^* W_{\mathfrak{c}}$$

is contained in the kernel of the Artin map for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, i.e. $\mathbb{Q}^* N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathbb{I}_{\mathbb{Q}(\zeta_m)})$. This shows already that $\mathfrak{c}$ is admissible for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. But by the previous lemma, combined with the remark (somewhere),

$$[\mathbb{I}_{\mathbb{Q}} : \mathbb{Q}^* W_{\mathfrak{c}}] = [\mathrm{Id}(\mathfrak{c}) : P_{\mathfrak{c}}] = \varphi(m)$$

At the same time,

$$[\mathbb{I}_{\mathbb{Q}} : N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathbb{I}_{\mathbb{Q}(\zeta_m)})] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$$

so $\mathbb{Q}^* W_{\mathfrak{c}}$ is equal to the kernel.

□

Corollary 4. *If m is an integer, then the formal product of m with the unique infinite place of $\mathbb{Q}$ is an admissible cycle for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.*

Proof. This was proved near the end of Proposition 3, as it follows from Proposition 1 and the fact that $\mathbb{Q}^* W_{\mathfrak{c}}$ is contained in the kernel of the Artin map. We mention this result by itself, since it implies that the elements of $1 + p_i^{e_i}\mathbb{Z}_{p_i}$ are local norms from $\mathbb{Q}_{p_i}(\zeta)$, which isn't obvious without class field theory. □

Theorem 5. *(Kronecker-Weber Theorem) Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

Proof. Every abelian extension of a given number field is contained in some ray class field, and Proposition 3 says that ray class fields of $\mathbb{Q}$ are cyclotomic extensions. □

7.2 The Artin map for infinite abelian extensions

We have noted that the Artin map on ideles is continuous, but we have not really explored the consequences. Continuity becomes important in the study of infinite abelian extensions. This section assumes some familiarity with inverse limits and profinite groups, and in particular the topology of infinite Galois groups. To review: a profinite group is an inverse limit of discrete topological groups. A profinite group is Hausdorff, compact, and totally disconnected.

Given a number field K, let K^{ab} be the **maximal abelian extension** of K, which is the compositum of all abelian extensions of K. For abelian extensions $L \subseteq L'$ of K, let $\pi_{L'L} : \mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$ be the restriction homomorphism. Then the groups $\mathrm{Gal}(L/K)$ form an inverse system, and $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, together with the restriction maps to each L, is the inverse limit of the groups $\mathrm{Gal}(L/K)$. In fact, if we restict the inverse system to only contain $\mathrm{Gal}(L/K)$ for L *finite abelian* over K, then $\mathrm{Gal}(L^{\mathrm{ab}}/K)$ is still an inverse limit of the system. Thus $\mathrm{Gal}(L^{\mathrm{ab}}/K)$ is profinite.

The mapping $L \mapsto \mathrm{Gal}(K^{\mathrm{ab}}/L)$ is a bijection between closed subgroups of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and intermediate fields of K^{ab}/K, i.e. abelian extensions of K. Under this mapping, finite abelian extensions of K correspond to open subgroups, since $[\mathrm{Gal}(K^{\mathrm{ab}}/K) : \mathrm{Gal}(K^{\mathrm{ab}}/L)] = |\mathrm{Gal}(L/K)| < \infty$, and closed subgroups of finite index are open.

Proposition 1. *There is a unique surjective open homomorphism*

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

called the ***Artin map****, with the property that for any finite abelian extension L of K, $\pi_L \circ \Phi = \Phi_{L/K}$, where $\pi_L : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$ is the restriction map. This map induces other surjective open homomorphisms $C_K, C_K^1 \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$.*

Proof. For L/K finite abelian, we have the Artin map

$$\Phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

which is a surjective open continuous mapping whose kernel is $K^* N_{L/K}(\mathbb{I}_L)$. By the universal mapping property of inverse limits, these Artin maps induce a unique topological group homomorphism $\Phi : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ with the given commutativity property. By a general result about profinite groups, the fact that each $\Phi_{L/K}$ is surjective means that the image of Φ is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

The kernel of Φ is the intersections of all the kernels of $\Phi_{L/K}$, so $\operatorname{Ker}\Phi$ contains K^*. Thus Φ induces a similar unique homomorphism with dense image $\overline{\Phi} : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, also called the Artin map. Now, we may identify as topological groups

$$C_K = C_K^1 \times (0, \infty)$$

where we can identify C_K^1 with $(xK^*, 1)$. Under this identification, we have

$$\overline{\Phi}(xK^*, 1) = \overline{\Phi}(xK^*) = \Phi(x)$$

Actually, we have $\overline{\Phi}(xK^*, \rho) = \Phi(x)$ for any $xK^* \in C_K^1$, because $\overline{\Phi}(1 \cdot K^*, \rho) = 1$. This is because ρ can be written as $(\sqrt[n]{\rho})^n$ for every n. This shows that the image of the Artin map of C_K is the same as the image of its restriction to C_K^1.

It follows that the image under the Artin map of C_K^1, and hence under C_K and $\mathbb{I}_K$, is all of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. This is because C_K^1 and hence its image is compact, and the image, being dense, must then be everything. Since each $\Phi_{L/K}$ is an open map, it follows that Φ and hence $\overline{\Phi}$ are also open maps. □

Being a direct summand, C_K^1 can be treated as both a subgroup and a quotient, in the way we have identified it. The 'projection' map $C_K \to C_K^1$, given by $(x, \rho) \mapsto (x, 1)$ is an open map, and the induced topological group structure from this quotient map (that is, from its isomorphism with C_K modulo the kernel $\{1\} \times (0, \infty)$) is the same as its topological group structure as a subgroup of C_K. The induced Artin map on C_K^1 from the first isomorphism theorem, is the same as the restriction to C_K^1 of the Artin map $\overline{\Phi}$ which we mentioned in the lemma.

Proposition 2. *Let M be an abelian extension of K, not necessarily finite. The restriction of the Artin map Φ to $\mathrm{Gal}(M/K)$ has kernel*

$$H_M = \bigcap_L \mathrm{Ker}\, \Phi_{L/K}$$

where L runs over all finite abelian extensions of K which are contained in M.

Proof. This just follows from the properties of inverse limits: $\mathrm{Gal}(M/K)$ is the inverse limit of the topological groups $\mathrm{Gal}(L/K)$, where L/K is finite abelian and $L \subseteq M$. The Artin maps $\Phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ induce a unique homomorphism $\Phi_{M/K} : \mathbb{I}_K \to \mathrm{Gal}(M/K)$ by the universal mapping property for inverse limits. The kernel of this map is clearly H_M. It is easy to see that this map is just the restriction of Φ to M. □

Theorem 3. *The Artin map $\Phi : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ induces an order reversing bijection between abelian extensions of K and closed subgroups of $\mathbb{I}_K$ containing $H_{K^{\mathrm{ab}}}$, given by $M \mapsto H_M$. Under this mapping, finite extensions of K correspond to open subgroups. If W is a given closed subgroup of $\mathbb{I}_K$ containing $H_{K^{\mathrm{ab}}}$, then it corresponds to the fixed field of $\Phi(W)$.*

Proof. The kernel of the Artin map $\Phi : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is $H_{K^{\mathrm{ab}}}$, so the Artin map, being surjective and open, induces an isomorphism of topological groups $\mathbb{I}_K/H_{K^{\mathrm{ab}}} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$. (Finite) abelian extensions of K correspond to closed (open) subgroups of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, which correspond

to closed (open) subgroups of $\mathbb{I}_K$ containing H_A. The statement about W is similar to the proof of (?). $\square$

7.3 Maximal Unramified Extensions

Let L/K be an abelian extension of number fields with class group H. If M/K is another abelian extension with class group H', we know that a finite place of v of K is unramified in M if and only if $\mathcal{O}_v^* \subseteq H'$. It follows that $\mathcal{O}_v^* H$ is the smallest open subgroup of $\mathbb{I}_K$ containing H and $\mathcal{O}_v^*$. Hence the class field M of $\mathcal{O}_v^* H$ is the largest intermediate field of L/K which is abelian over K and in which v is unramified. For v infinite, replace every $\mathcal{O}_v^*$ with K_v^* to get an analogous statement for infinite places.

Similarly, a place v of K splits completely in M if and only if $K_v^* \subseteq H'$. Thus the class group of $K_v^* H$ is the largest intermediate field of L/K which is abelian over K and in which v splits completely.

Now, if we look at the open subgroup

$$\mathbb{I}_K^{S_\infty} = \prod_{v|\infty} K_v^* \prod_{v<\infty} \mathcal{O}_v^*$$

then $H := K^* \mathbb{I}_K^{S_\infty}$ is an open subgroup containing K^* as well as $\mathcal{O}_v^*$ (resp K_v^* if $v \mid \infty$) for every place v. It follows that every place of K is unramified in the class field to H, and this class field is the maximal abelian extension of K with respect to this property.

The class field M to H is called the **Hilbert class field** of K. We discuss some of its immediate properties:

Proposition 6. *Let K be a number field, and M its Hilbert class field.*

(i) The Artin map on $\mathrm{Id}(K)$ induces an isomorphism of $\mathrm{Gal}(M/K)$ with the ideal class group of K.

(ii) K is its own Hilbert class field if and only if $\mathcal{O}_K$ is a principal ideal domain.

(iii) If $\mathfrak{p}$ is a prime ideal of K, then $\mathfrak{p}$ splits in M as a product of h/f primes, where h is the class number of K, and f is the smallest number such that $\mathfrak{p}^f$ is principal.

Proof. Since every place of K is unramified in M, we already have a well defined Artin map $\mathrm{Id} \to \mathrm{Gal}(M/K)$. Since $K^* \mathbb{I}_K^{S_\infty}$ is the kernel of the Artin map on $\mathbb{I}_K$, we see that the 'empty cycle' $\mathfrak{c} = 1$ is admissible for M/K, and here $P_\mathfrak{c}$ is just the group of principal ideals P.

Therefore, we know that P is contained in the kernel of the Artin map. But it is easy to see that we have an isomorphism $\mathbb{I}_K / K^* \mathbb{I}_K^{S_\infty} \cong \mathrm{Id}\,/P$, whence

$$[M : K] = [\mathbb{I}_K : K^* \mathbb{I}_K^{S_\infty}] = [\mathrm{Id} : P]$$

Therefore the kernel of the Artin map on Id is the group of principal ideals, and we get an isomophism $\mathrm{Id}\,/P \cong \mathrm{Gal}(M/K)$. This proves (i), and (ii) and (iii) easily follow.

□

We will mention one more theorem about the Hilbert class field, but we will not prove it.

Theorem 7. *Every fractional ideal of K becomes principal in the Hilbert class field.*

Proof. See *Class Field Theory* by Artin and Tate. □

8 Reciprocity Laws

One of the goals of class field theory is to describe how prime ideals of a number field K split in a given abelian extension L of K. The Law of Artin Reciprocity implies, for every abelian extension of number fields L/K, the existence of an algorithm determining the splitting behavior of all unramified primes of K. It does not tell us what this algorithm is exactly. We will explain:

Let $\mathfrak{c}$ be a cycle of K. Recall the definitions $\mathrm{Id}(\mathfrak{c}), P_{\mathfrak{c}}$. The quotient $\mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}}$ is called the group of **$\mathfrak{c}$-ideal classes**. Proposition 2, Chapter 8 shows that this group is finite, for it is isomorphic to $\mathbb{I}_K/K^*W_{\mathfrak{c}}$, and $K^*W_{\mathfrak{c}}$ is an open subgroup of the ideles containing K^*. For a detailed treatment of the structure of $\mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}}$, see Lang.

Let L be an abelian extension of K, and let $\mathfrak{c}$ be a cycle for L/K, divisible by all the ramified primes, with the property that $P_{\mathfrak{c}}$ is contained in the kernel of the Artin map on $\mathrm{Id}(\mathfrak{c})$. This happens, for example, when $\mathfrak{c}$ is admissible for L/K, in which case the whole kernel is $P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c})$. Given such a cycle $\mathfrak{c}$, it follows that we have a well defined surjective homomorphism:

$$\mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}} \to \mathrm{Gal}(L/K)$$

$$\mathfrak{a}P_{\mathfrak{c}} \mapsto (\mathfrak{a}, L/K)$$

Hence the splitting of any prime ideal of K, relatively prime to $\mathfrak{c}$, is completely determined by its representative class modulo $P_{\mathfrak{c}}$.

To be more specific, let $\mathfrak{a}_1, ..., \mathfrak{a}_t$ be a complete set of representatives for $P_{\mathfrak{c}}$ in $\mathrm{Id}(\mathfrak{c})$. Let $n = [L : K]$. Let m_i be the order of $(\mathfrak{a}_i, L/K)$ in $\mathrm{Gal}(L/K)$. A prime ideal $\mathfrak{p}$ of K, relatively prime to $\mathfrak{c}$, splits as a product of n/f primes in L, where f is the order of $(\mathfrak{p}, L/K)$. If we want to determine this number f, we need only deduce the class of $\mathfrak{p}$ modulo $P_{\mathfrak{c}}$. For example, if $\mathfrak{p}P_{\mathfrak{c}} = \mathfrak{a}_1 P_{\mathfrak{c}}$, then $(\mathfrak{p}, L/K) = (\mathfrak{a}_1, L/K)$, so $\mathfrak{p}$ splits into n/m_1 primes in L.

8.1 The Hilbert Symbol

The rest of this chapter is primarily based on the notes of Peter Stevenhagen [citation].

Let F be a local field of characteristic 0 ($\mathbb{R}, \mathbb{C}$, or a p-adic field) which contains the nth roots of unity. Kummer theory tells us that there is a bijection between the subgroups $F^{*n} \subseteq D \subseteq F^*$ for which $[D : F^{*n}]$ is finite, and finite abelian extensions E of F having exponent n. Given D, the field E is obtained by adjoining to F all the nth roots of elements in D, and moreover $[D : F^{*n}] = [E : F]$.

Since F is a local field, $[F^* : F^{*n}]$ is finite (for example when F is p-adic, we gave an explicit formula for this index). This tells us that there is a unique maximal abelian extension of F of exponent n, and it is of finite degree over F (on the other hand, the maximal abelian extension of F, without regard to exponent, is of infinite degree over F when F is p-adic).

Let E be this maximal abelian extension of exponent n. So $E = F(\sqrt[n]{x} : x \in F^*)$. Recall we have a pairing:

$$\mathrm{Gal}(E/F) \times F^*/F^{*n} \to \mathbb{C}^*$$

into the group of nth roots of unity, given by $(\sigma, \bar{x}) \mapsto \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}}$. Now if $x^n \in F^{*n}$, the fact that $\mathrm{Gal}(E/F)$ has exponent n tells us that

$$\Phi_{E/F}(x^n) = \Phi_{E/F}(x)^n = 1$$

where $\Phi_{E/F}$ is the local Artin map. Thus F^{*n} is contained in $N_{E/F}(E^*)$, the kernel of the Artin map. But by Kummer theory and local class field theory,

$$[F^* : F^{*n}] = [E : F] = [F^* : N_{E/F}(E^*)]$$

so in fact $F^{*n} = N_{E/F}(E^*)$. The local Artin map gives an isomorphism $\mathrm{Gal}(E/F) \cong F^*/N_{E/F}(E^*) = F^*/F^{*n}$, and we obtain a pairing:

$$\langle -, - \rangle : F^* \times F^* \to F^*/N_{E/F}(E^*) \times F^*/F^{*n} \to \mathrm{Gal}(E/F) \times F^*/F^{*n} \to \mathbb{C}^*$$

which we call the **Hilbert symbol** at F.

Lemma 1. *Let F be a field of characteristic 0 containing the nth roots of unity, and let $\beta \in F^*$. Then $F(\sqrt[n]{\beta})/F$ is cyclic, and every element in F of the form $x^n - \beta$ is a norm from $F(\sqrt[n]{\beta})$.*

Proof. Fix a specific nth root $\sqrt[n]{\beta}$, and let $G = \mathrm{Gal}(F(\sqrt[n]{\beta}/F)$. The map $\sigma \mapsto \frac{\sigma \sqrt[n]{\beta}}{\sqrt[n]{\beta}}$ is a homomorphism from G to the group of nth roots of unity. Since an element of G is completely determined by its effect on $\sqrt[n]{\beta}$, this map is an injection. Hence G and its image are cyclic, with order say, d. Fix a generator σ of G. Then the image of σ has order d, so there exists a primitive nth root of unity ζ such that $\sigma \sqrt[n]{\beta} = \zeta^{n/d} \sqrt[n]{\beta}$. By induction and the fact that σ fixes nth roots of unity (for they lie in F) we have that $\sigma^k(\sqrt[n]{\beta}) = \zeta^{\frac{n}{d}k} \sqrt[n]{\beta}$.

Now for $0 \leq j \leq \frac{n}{d} - 1$, the norm of $x - \zeta^j \sqrt[n]{\beta}$ is

$$\prod_{k=0}^{d-1} \sigma^k(x - \zeta^j \sqrt[n]{\beta}) = \prod_{k=0}^{d-1} (x - \zeta^j \zeta^{\frac{n}{d}k} \sqrt[n]{\beta})$$

So the norm of $\prod_{j=0}^{\frac{n}{d}-1} (x - \zeta^j \sqrt[n]{\beta})$ is

$$\prod_{j=0}^{\frac{n}{d}-1} \prod_{k=0}^{d-1} (x - \zeta^{j+\frac{n}{d}k} \sqrt[n]{\beta}) = \prod_{i=0}^{n-1} (x - \zeta^i \sqrt[n]{\beta}) = x^n - \beta$$

□

Lemma 2. *Let K be a number field, v a place of K, and E^v the maximal abelian extension of K_v of exponent n. For $\alpha, \beta \in K_v^*$, let*

$$\langle \alpha, \beta \rangle_v = \frac{\Phi_{E^v/K_v}(\alpha)(\sqrt[n]{b})}{\sqrt[n]{b}}$$

be the Hilbert symbol at K_v. Then the following properties hold for any $\alpha, \beta \in K_v^*$:

(i) $\langle \alpha, \beta \rangle_v = 1$ if and only if α is a norm from $K_v(\sqrt[n]{\beta})$.

(ii) If v is finite, and α, β, n are units in $\mathcal{O}_v$, then $\langle \alpha, \beta \rangle_v = 1$.

(iii) $\langle \alpha, -\alpha \rangle_v = 1$, and $\langle \alpha, 1-\alpha \rangle_v = 1$ for $\alpha \neq 1$.

(iv) $\langle \alpha, \beta \rangle_v = \langle \beta, \alpha \rangle_v$.

Proof. The restriction of the Artin map for E^v/K_v to $K_v(\sqrt[n]{\beta})$ is the same as the Artin map for $K_v(\sqrt[n]{\beta})/K_v$. Fixing β and varying α, we see that we can just work with this latter Artin map. So $\langle \alpha, \beta \rangle_v = 1$ if and only if $(\alpha, K_v(\sqrt[n]{\beta})/K_v)$ fixes $\sqrt[n]{\beta}$, if and only if $(\alpha, K_v(\sqrt[n]{\beta})/K_v)$ fixes all of $K_v(\sqrt[n]{\beta})$, if and only if α is in the kernel of the Artin map for $K_v(\sqrt[n]{\beta})/K_v$, if and only if α is a norm from $K_v(\sqrt[n]{\beta})$. This proves (i).

For (ii), we can argue as we did in the proof of (?) that $K_v(\sqrt[n]{\beta})/K_v$ is unramified when n, β are units at v, in which case the norm map on the unit groups is surjective. Hence α is a norm, so $\langle \alpha, \beta \rangle_v = 1$ by (i).

By Lemma 1, $0^n - (-\alpha) = \alpha$ is a norm from $K_v(\sqrt[n]{-\alpha})$, so $\langle \alpha, -\alpha \rangle_v = 1$ by (i). Similarly, $1^n - \alpha = 1 - \alpha$ is a norm from $K_v(\sqrt[n]{\alpha})$, so $\langle 1-\alpha, \alpha \rangle_v = 1$. This proves (iii).

Finally, (iv) follows from (iii). We have

$$1 = \langle \alpha\beta, -\alpha\beta \rangle_v = \langle \alpha, -\alpha \rangle_v \langle \alpha, \beta \rangle_v \langle \beta, \alpha \rangle_v \langle \beta, -\beta \rangle_v = \langle \alpha, \beta \rangle_v \langle \beta, \alpha \rangle_v$$

□

For each place v of K, the Hilbert symbol at v depends on the Artin map of the local field E^v. Globally, there is no reason to expect that the fields E^v have anything to do with one another for different places v. However, if we fix a $\beta \in K^*$, then $L = K(\sqrt[n]{\beta})$ is a global field which we can use to compute $\langle -, \beta \rangle_v$ for any v.

Specifically: as we mentioned in the last proof, the restriction of the Artin map Φ_{E^v/K_v} to L_w, for any place $w \mid v$, is $\Phi_{L_w/K_v} = \Phi_{w/v}$, and therefore

$$\langle \alpha, \beta \rangle_v = \frac{\Phi_{w/v}(\alpha)(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$$

Hilbert Reciprocity expresses the relationship between the different Hilbert symbols:

Theorem 3. *(Law of Hilbert Reciprocity) For any $\alpha, \beta \in K^*$,*

$$\prod_v \langle \alpha, \beta \rangle_v = 1$$

Proof. Our first claim is that

$$\prod_v \Phi_{w/v}(\alpha) = 1$$

where $L = K(\sqrt[n]{\beta})$ and w is a place of L lying over v. Let S be the set of places containing all the archimedean places, all those which ramify in L, and all those for which α is not a unit. Then $\Phi_{w/v}(\alpha) = 1$ whenever $v \notin S$, as α, being a unit in the unramified extension L_w/K_v, is a norm. This shows that the product of the $\Phi_{w/v}(\alpha)$ is already a finite product. Let x be the idele of K which is α at all $v \in S$, and 1 otherwise. Let y be the idele which is 1 at all $v \in S$, and α for $v \notin S$. Then $xy = \alpha$, where α is embedded diagonally in $\mathbb{I}_K$. Now $(y, L/K)$ is easily seen to be 1, for y is in the largest admissible subgroup and a unit everywhere. Then

$$1 = (\alpha, L/K) = (x, L/K)(y, L/K) = (x, L/K) = \prod_{v \in S} \Phi_{w/v}(\alpha) = \prod_v \Phi_{w/v}(\alpha)$$

Hilbert Reciprocity is then just a consequence of bimultiplicativity.

So we see that all the really hard work was already done when we proved Artin reciprocity.

□

One way of interpreting Artin reciprocity is the following: for an admissible cycle $\mathfrak{m}$ of an abelian extension of K, the splitting of a prime ideal of K, relatively prime to $\mathfrak{m}$ is determined by its class modulo $P_{\mathfrak{m}}$. In this way, Artin reciprocity states the existence of an algorithm for deducing how prime ideals split in a given extension. This is a wonderful result, yet in some ways it is still unsatisfactory. First of all, it is highly nonconstructive. Second, Artin reciprocity is so general that it looks nothing like reciprocity, in the classical sense.

A "nice" reciprocity law should give a much more clear indication of the relationship distinct primes have with one another. Preferably, it should be expressible with a symbol involving two or more primes, and describe in an elegant way what happens when the roles of the primes are interchanged.

In proving the main results of class field theory, the principal difficulty, after proving the fundamental inequalities, is showing, for an admissible cycle $\mathfrak{c}$, that the idelic Artin map on $H_{\mathfrak{c}}$ is trivial on $K^* \cap H_{\mathfrak{c}}$ (equivalently, the Artin map on $\mathrm{Id}(\mathfrak{c})$ is trivial on $P_{\mathfrak{c}}$). This allows us to give a well defined Artin map on $\mathbb{I}_K$, which is necessarily also trivial on K^*. Notice that this fact is exactly what we needed to prove the law of Hilbert reciprocity.

8.2 Computations of some Hilbert symbols

The general idea to give a formula for a Hilbert symbol is the following: F will be a local field with group of units U (let $U = F^*$ if F is archimedean). We will analyze the restricted Hilbert symbol:

$$\langle -, - \rangle : U \times U \to \mathbb{C}^*$$

by finding a finite index subgroup N of U such that $\langle x, y \rangle = 1$ whenever x *or* y is in U. This induces a well defined pairing

$$U/N \times U/N \to \mathbb{C}^*$$

Thus for any $(x, y) \in U \times U$, the symbol $\langle x, y \rangle$ is completely determined by the representative classes of x and y in U/N.

For our first example, we take $F = \mathbb{R}$.

Proposition 4. *Taking $n = 2$, the Hilbert symbol:*

$$\mathbb{R}^* \times \mathbb{R}^* \to \{-1, 1\}$$

is given by the formula

$$\langle x, y \rangle = (-1)^{\frac{x-1}{2}\frac{y-1}{2}}$$

where x is the sign function.

Proof. Let $N = (0, \infty)$. We claim that $\langle x, y \rangle$ is trivial whenever x or y is in N. If y is in N, then $\mathbb{R}(\sqrt{y}) = \mathbb{R}$, so the Artin map is trivial.

If x is in N, then whether or not y is in N (i.e. whether or not $\mathbb{R}(y)$ is equal to $\mathbb{R}$ or $\mathbb{C}$), x is a norm from $\mathbb{R}(y)$, so x is in the Artin map $\mathbb{R}(y)/\mathbb{R}$.

By the discussion at the beginning of this section, we only have to compute the Hilbert symbol at different coset representatives. The only thing we haven't already computed is $\langle -1, -1 \rangle$. But this is clearly -1, since $\mathbb{R}(-1) = \mathbb{C}$, and -1 is not a norm from $\mathbb{C}$.

□

Proposition 5. *Let $n = 2$. If $F = \mathbb{Q}_2$, and U its group of units, then the Hilbert symbol $U \times U \to \{-1, 1\}$ is given by*

$$\langle x, y \rangle = (-1)^{\frac{x-1}{2}\frac{y-1}{2}}$$

Proof. Clearly U is equal to $U_1 = 1 + 2\mathbb{Z}_2$. And

$$U_2 = 1 + 4\mathbb{Z}_2 = \{x \in \mathbb{Z}_2 : x \equiv 1 \pmod 4\}$$

Furthermore $U_1 \setminus U_2 = \{x \in \mathbb{Z}_2 : x \equiv 3 \pmod 4\}$. It is easy to see that $U^2 \subseteq U_2$, which implies $U^2 = U_2$, since U has the same degree over both of these subgroups (check this).

Now suppose x or y is in U_2. If y is in U_2, then y is a square, so $\mathbb{Q}_2(\sqrt{y}) = \mathbb{Q}_2$, which immediately implies $\langle x, y\rangle = 1$. If x is in U_2, then x is a square, and hence a norm, from $\mathbb{Q}_2(\sqrt{y})$. So also $\langle x, y\rangle = 1$.

Thus we have a well defined pairing $U/U_2 \times U/U_2 \to \{-1, 1\}$, and all we have left to compute is $\langle x, y\rangle$ when neither x nor y is in U_2, i.e. when $x \equiv y \equiv 3 \pmod 4$. Reducing to coset representatives, we only have to compute $\rangle -1, -1\rangle$. In this case, $\mathbb{Q}_2(\sqrt{-1}) = \mathbb{Q}_2(i)$ is a proper extension of $\mathbb{Q}_2$ (e.g. 2 ramifies in $\mathbb{Q}(i)$). Verify that the norm group, i.e. the kernel of the Artin map $\mathbb{Q}_2(i)/\mathbb{Q}_2$ is $U^2 = U_2$. Since $-1 \notin U_2$, clearly $\langle -1, -1\rangle = 1$.

What we have shown is that $\langle x, y\rangle$ is 1 if x or y is $\equiv 1 \pmod 4$, and it is -1 otherwise. The formula given in the statement of the proposition says exactly this. □

Lemma 6. *Let K be a number field containing the nth roots of unity. Let v be finite, $\mathfrak{p} = \mathfrak{p}_v$, $U = \mathcal{O}_v^*$, and $U_k = 1 + \mathfrak{p}^k$. If $U_{i+j} \subseteq U^n$, then $a \in U_i, b \in U_j$ implies $\langle a, b\rangle_v = 1$.*

8.3 The power residue symbol

In this section we let $A = \mathcal{O}_K$. Let $\mathfrak{p}$ be a prime of K which does not divide n. Recall that the nth roots of unity are distinct modulo $\mathfrak{p}$. This can be argued as follows: if not, then $\zeta^j \equiv 1 \pmod{\mathfrak{p}}$ for some $1 \leq j \leq n-1$. Evaluate both sides of the expression

$$1 + X + \cdots + X^{n-1} = \frac{X^n - 1}{X - 1} = \prod_{i=1}^{n-1}(X - \zeta^i)$$

at 1, then reduce modulo $\mathfrak{p}$. This implies

$$n \equiv \prod_{i=1}^{n-1}(1 - \zeta^i) \equiv 0 \pmod{\mathfrak{p}}$$

which is a contradiction. Note also that n divides $\mathcal{N}(\mathfrak{p}) - 1$. This is clear, because $(\mathcal{O}_K/\mathfrak{p})^*$ has $\mathcal{N}(\mathfrak{p}) - 1$ elements, and ζ modulo $\mathfrak{p}$ generates a subgroup of order n.

Let $A_{\mathfrak{p}}$ be the localization of A at $\mathfrak{p}$. The inclusion $A \subseteq A_{\mathfrak{p}}$ induces an isomorphism of the residue fields $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ and $A/\mathfrak{p}$, so the nth roots of unity are also distinct modulo $\mathfrak{p}A_{\mathfrak{p}}$. Now if $\alpha \in K^*$ is a unit at $\mathfrak{p}$, then it lies in $A_{\mathfrak{p}}$, and it remains nonzero when reduced modulo $\mathfrak{p}A_{\mathfrak{p}}$. We then set

$$(\frac{\alpha}{\mathfrak{p}})_n$$

to be the unique nth root of unity to which $\alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}}$ is congruent modulo $\mathfrak{p}A_{\mathfrak{p}}$. Clearly $\alpha^{\frac{\mathcal{N}(\mathfrak{p})-1}{n}}$ is

indeed an nth root of unity in this residue field. We call $(\frac{\alpha}{\mathfrak{p}})_n$ the **nth power residue symbol** of α at $\mathfrak{p}$.

We have only defined this symbol for $\mathfrak{p}$ relatively prime to both n and α. If $\mathfrak{p}$ *does* divide n or α, then we set $(\frac{\alpha}{\mathfrak{p}})_n = 1$. In this way we can extend the denominator of the power residue symbol to arbitrary fractional ideals:

$$(\frac{\alpha}{\mathfrak{a}})_n = \prod_{\mathfrak{p}} (\frac{\alpha}{\mathfrak{a}})_n^{\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{a}}$$

Obviously this is a finite product. Given $\beta \in K^*$, by $(\frac{\alpha}{\beta})_n$ we mean $(\frac{\alpha}{\beta\mathcal{O}_K})_n$.

Proposition 7. *The following properties hold for $\alpha, \beta \in K^*$:*

(i) The symbol $(\frac{\alpha}{\_})_n$ is a homomorphism in the argument of the denominator from the group of fractional ideals of K to the group of nth roots of unity.

(ii) If $\mathfrak{a}$ is a fractional ideal of K, and $\alpha_1, \alpha_2 \in K^*$ are both relatively prime to $\mathfrak{a}$, then

$$(\frac{\alpha_1\alpha_2}{\mathfrak{a}})_n = (\frac{\alpha_1}{\mathfrak{a}})_n (\frac{\alpha_2}{\mathfrak{a}})_n$$

(iii) If $\mathfrak{a}$ is relatively prime to α, then

$$(\frac{\alpha}{\mathfrak{a}})_n = \frac{(\mathfrak{a}, K(\sqrt[n]{\alpha})/K)(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}$$

(iv)

$$(\frac{\alpha}{\beta})_n = \prod_v \langle \beta, \alpha \rangle_v$$

where v runs through all the finite places which do not divide α or n.

(v) For $\mathfrak{p}$ prime not dividing α or n, $(\frac{\alpha}{\mathfrak{p}})_n = 1$ if and only if $\mathfrak{p}$ splits completely in $K(\sqrt[n]{\alpha})$.

Proof. (i) and (ii) follow easily from the definition of power residue symbol. For (iii), it suffices by (i) to prove the case where $\mathfrak{a}$ is equal to a prime ideal $\mathfrak{p}$, relatively prime to α and n. In this case, $\mathfrak{p}$ is unramified in $K(\sqrt[n]{\alpha})$ by the usual argument (?), so $\sigma := (\mathfrak{p}, K(\sqrt[n]{\alpha})/K)$ has the effect

$$\sigma\alpha \equiv \alpha^p \pmod{\mathfrak{p}A_{\mathfrak{p}}}$$

for any $\alpha \in A_{\mathfrak{p}}$ (normally, this is stated as taking place in the larger ring of integers $\mathcal{O}_{K(\sqrt[n]{\alpha}}$, but we are only concerned with $A = \mathcal{O}_K$ right now; also, it is a trivial matter to check that this also holds in the localization $A_{\mathfrak{p}}$). Now modulo $\mathfrak{p}A_{\mathfrak{p}}$,

$$\frac{\sigma\sqrt[n]{\alpha}}{\sqrt[n]{\alpha}} \equiv \frac{\sqrt[n]{\alpha}^p}{\sqrt[n]{\alpha}} = \sqrt[n]{\alpha}^{p-1} = \alpha^{\frac{p-1}{n}} \equiv (\frac{\alpha}{\mathfrak{p}})_n$$

so the right and left hand sides, both being roots of unity, must be equal.

(iv) follows from (iii). For (v), $(\frac{\alpha}{\mathfrak{p}})_n = 1$ if and only if $\sigma := (\mathfrak{p}, K(\sqrt[n]{\alpha})/K)$ fixes $\sqrt[n]{\alpha}$, if and only if σ fixes all of $K(\sqrt[n]{\alpha})$, if and only if σ is the identity in $\mathrm{Gal}(K(\sqrt[n]{\alpha})/K)$. But the order of σ is the inertial degree of $\mathfrak{p}$.

□

As a consequence of (iii), we see that the homomorphism $(\frac{\alpha}{-})_n$ is well defined on the quotient $\mathrm{Id}(\mathfrak{c})/P_{\mathfrak{c}}$, where $\mathfrak{c}$ is an admissible cycle for $K(\sqrt[n]{\alpha})/K$ divisible by the places dividing n and α. That is, if $\mathfrak{p}_1, \mathfrak{p}_2$ are prime ideals which are relatively prime to $\mathfrak{c}$, then $(\frac{\alpha}{\mathfrak{p}_1})_p = (\frac{\alpha}{\mathfrak{p}_2})_p$. For by admissibility, $P_{\mathfrak{c}}$ is contained in the kernel of the Artin map on $\mathrm{Id}(\mathfrak{c})$.

Theorem 8. *(Power reciprocity law) For $\alpha \in K^*$, let $S(\alpha)$ denote the set of places which either divide n or occur in the factorization of α. For any $\alpha, \beta \in K^*$,*

$$(\frac{\alpha}{\beta})_n (\frac{\beta}{\alpha})_n^{-1} = \prod_{v \in S(\alpha) \cap S(\beta)} \langle \alpha, \beta \rangle_v$$

Proof. (iv), Proposition 6 says that

$$(\frac{\alpha}{\beta})_n = \prod_{v \notin S(\alpha)} \langle \beta, \alpha \rangle_v$$

which we can write as

$$\prod_{v \in S(\beta) \setminus S(\alpha)} \langle \beta, \alpha \rangle_v \prod_{v \notin S(\beta) \cup S(\alpha)} \langle \beta, \alpha \rangle_v$$

For the v which are neither in $S(\beta)$ nor $S(\alpha)$, v is unramified in $K(\sqrt[n]{\alpha})$, and β is a unit at v. The local Artin map on an unramified extension being trivial on the units, we conclude that $\langle \beta, \alpha \rangle_v = 1$. Therefore

$$(\frac{\alpha}{\beta})_n = \prod_{v \in S(\beta) \setminus S(\alpha)} \langle \beta, \alpha \rangle_v$$

On the other hand, (iv), Proposition 6 also tells us that

$$(\frac{\beta}{\alpha})_v^{-1} = \prod_{v \notin S(\beta)} \langle \alpha, \beta \rangle_v^{-1} = \prod_{v \in S(\beta)} \langle \alpha, \beta \rangle_v$$

where the second equality follows from Hilbert reciprocity. And (iv), Lemma 2, tells us that $\langle \beta, \alpha \rangle_v \langle \alpha, \beta \rangle_v = 1$ for each v, so

$$(\frac{\alpha}{\beta})_n (\frac{\beta}{\alpha})_n^{-1} = \prod_{v \in S(\beta) \setminus S(\alpha)} \langle \beta, \alpha \rangle_v \prod_{v \in S(\beta)} \langle \alpha, \beta \rangle_v = \prod_{v \in S(\alpha) \cap S(\beta)} \langle \alpha, \beta \rangle_v$$

□

8.4 Eisenstein reciprocity

In this section we prove a very general reciprocity law for $K = \mathbb{Q}(\zeta)$, where ζ is a primitive pth root of unity, and p is an odd prime number. Recall that any prime number q, distinct from p, is unramified in K, and its inertial degree is its multiplicative order modulo p. As for p itself, it is totally ramified, with $\lambda := 1 - \zeta$ the unique prime element in $\mathcal{O}_K$ lying over it, up to associates.

We call an $\alpha \in \mathcal{O}_K$ **primary** if it is not a global unit, it is relately prime to p, and it is congruent modulo ζ^2 to a rational integer. Although K is a complex field, the notion of being primary allows us to introduce an analagous notion of sign. Indeed, for any $\alpha \in \mathcal{O}_K$, there is a unique pth root of unity ζ^c for which $\alpha\zeta^c$ is primary:

Proof. The inertial degree of p is 1, so the inclusion $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\lambda\mathcal{O}_K$ is an isomorphism. Hence there exists an $a \in \mathbb{Z}$ for which $\alpha \equiv a \pmod{\lambda}$. Then $\frac{\alpha - a}{\lambda} \in \mathcal{O}_K$, so again there exists a $b \in \mathbb{Z}$ for which $\frac{\alpha-a}{\lambda} \equiv b \pmod{\lambda}$, hence $\alpha \equiv a + b\lambda \pmod{\lambda^)}$. Since α is relatively prime to λ, a is not divisible by p, so there is a unique solution $c \in \{0, 1, ..., p-1\}$ to the congruence $a \equiv bX \pmod{p}$. Modulo λ^2 we have:

$$\zeta^c = (1 - \lambda)^c \equiv 1 - c\lambda$$

and so

$$\alpha\zeta^c \equiv (a + b\lambda)(1 - c\lambda) \equiv a + (b - ac)\lambda \equiv a$$

The uniqueness of c is clear, for it is the only integer which makes $(b - ac)\lambda$ vanish modulo λ^2, and $a + k\lambda, k \in \mathbb{Z}$ is never an integer unless $k = 0$. □

Eisenstein reciprocity says that if $\alpha \in \mathcal{O}_K$ is primary, and $a \in \mathbb{Z}$ is relatively prime to p and α, then

$$(\frac{\alpha}{a})_p = (\frac{a}{\alpha})_p$$

Without class field theory, this equality follows from the Stickleberger relation, which describes the prime ideal decomposition of a certain Gauss sum. See Ireland and Rosen for a proof done in this way. In [9], Peter Schmidt shows how Eisenstein reciprocity follows from Hilbert reciprocity. We reproduce his argument here:

Lemma 9. *Let q, r be rational numbers not divisible by p. Then $(\frac{q}{r})_p = 1$.*

Proof. Remember that we are in the field $K = \mathbb{Q}(\zeta)$. By multiplicativity, we may assume that r is a prime number. Let J be any prime ideal of $\mathcal{O}_K$ lying over r. First suppose that r splits completely in K. Then $r\mathcal{O}_K = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma J$, so

$$(\frac{q}{r})_p = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} (\frac{q}{\sigma J})_p = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\frac{q}{J})_p = N_{K/\mathbb{Q}}(\frac{q}{J})_p$$

and the norm of a pth root of unity for p odd is 1. (we have to still show that you can take σ in and out of the power symbol)

Now suppose that r does not split completely in K. Then $r-1$ is not divisible by p. Now the congruence $q \equiv X^p \pmod{r}$ is solvable if and only if $q^{\frac{r-1}{d}} \equiv 1 \pmod{r}$, where d is the greatest common divisor of $r-1$ and p. In this case $d=1$, so the given congruence is solvable. So there is a $y \in \mathbb{Z}$ for which $q \equiv y^p$ modulo r, hence modulo J. So

$$(\frac{q}{J})_p \equiv q^{\frac{\mathcal{N}(J)-1}{p}} \equiv y^{\mathcal{N}(J)-1} \equiv 1 \pmod{J}$$

Since $(\frac{q}{r})_p$ is a product of various $(\frac{q}{J})_p$, for prime ideals J lying over r, we can conclude that $(\frac{q}{r})_p = 1$.

□

Theorem 10. *(Law of Eisenstein Reciprocity) If $\alpha \in \mathcal{O}_K$ is primary, and $a \in \mathbb{Z}$ is relatively prime to p and α, then*

$$(\frac{\alpha}{a})_p = (\frac{a}{\alpha})_p$$

Proof. Let v be the place of K corresponding to λ, and U the units of $\mathcal{O}_v$. The power reciprocity law tells us that

$$(\frac{\alpha}{a})_p (\frac{a}{\alpha})_p^{-1} = \langle \alpha, a \rangle_v$$

so we just have to show that $\langle \alpha, a \rangle_v = 1$. Since α is primary, there is an integer k such that $\alpha \equiv k \pmod{\lambda^2}$. Clearly k is a unit in $\mathcal{O}_v$, so $\frac{\alpha}{k} \in U_2 = 1 + \lambda^2 \mathcal{O}_v$. Also $a^{p-1} \equiv 1 \pmod{p}$, so $a^{p-1} \in 1 + p\mathcal{O}_v = 1 + \lambda^{p-1}\mathcal{O}_v = U_{p-1}$. It follows by lemma (?) that $\langle \frac{\alpha}{k}, a^{p-1} \rangle_v = 1$, provided that $U_{p+1} \subseteq U^p$. But this is immediate from Hensel's lemma.

Now

$$1 = \langle \frac{\alpha}{k}, a^{p-1} \rangle_v = \langle \frac{\alpha}{k}, a \rangle_v^{p-1}$$

which implies $\langle \frac{\alpha}{k}, a \rangle_v = 1$ as well, since $p-1$ is relatively prime to p. But

$$\langle \frac{\alpha}{k}, a \rangle_v = \langle \alpha, a \rangle_v \langle k, a \rangle_v^{-1}$$

and the power reciprocity law gives

$$\langle k, a \rangle_v = (\frac{a}{k})_p (\frac{k}{a})_p^{-1} = 1 \cdot 1 = 1$$

by Lemma 9. □

Eisenstein reciprocity, along with its various specifications (cubic reciprocity, biquadratic reciprocity) allows us to deduce how primes of $K = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_p)$ split in extensions of the form

$\mathbb{Q}(\zeta, \sqrt[p]{\alpha})$, for $\alpha \in \mathcal{O}_K$. Without loss of generality, we may assume that α is primary, for multiplying it by a pth root of unity does not change the extension. The easiest case is when a is a rational prime number with full inertial degree in K, and α is a primary prime of $\mathcal{O}_K$. In this case, we have that the number of primes in $K(\sqrt[p]{a})$ lying over $\alpha \in \mathcal{O}_K$ is the same as the number of primes in $K(\sqrt[p]{\alpha})$ lying over $a\mathcal{O}_K$. We see immediately many circumstances which complicate the situation in general, for example lack of unique factorization in K.

A Haar Measure

Most of the proof techniques involving the the Haar measure don't show up again when we apply the results to proofs in class field theory, and in general proofs about the Haar measure are pretty tedious and boring. So we leave most of the proofs out here. It is our intention to write enough so that the interested reader can work out the details themselves, or seek out the given references.

Let X be a locally compact topological space. A *Borel measure* μ on X is a measure on the Borel subsets of X (that is, the σ-algebra generated by the open sets). If $E \subseteq X$, we say that μ is outer regular on E if $\mu(E)$ can be approximated from above by open sets, i.e. $\mu(E)$ is the infimum of all $\mu(U)$, where U runs through the open sets containing E. We say that μ is inner regular on E if $\mu(E)$ can be approximated from below by compact sets. A **Radon measure** is a nonzero Borel measure which is finite on compact sets, outer regular on Borel sets, and inner regular on open sets.

Let $C_c(X)$ denote the set of continuous functions of compact support $X \to \mathbb{C}$. Then $C_c(X)$ is a complete normed vector space over $\mathbb{C}$ with norm

$$||f||_\infty = \sup_{x \in X} |f(x)|$$

Let also $C_c^+(X)$ denote the set of $f \in C_c(X)$ such that $f(x) \in [0, \infty)$ for all $x \in X$, but $f \neq 0$.

Theorem 1. *(Riesz-representation theorem) Let μ be a Radon measure on X. Define a positive linear functional $T : C_c(X) \to \mathbb{C}$ by*

$$T(f) = \int_X f d\mu$$

Then $\mu \mapsto T$ gives a bijection between Radon measures on X and positive linear functionals on $C_c(G)$.

Proof. See e.g. Rudin, or Hewitt and Ross. □

Now suppose that G is a locally compact topological group. To make life easy, *we'll always suppose that G is abelian*, since we don't consider nonabelian topological groups in these notes. A Radon measure μ on G is called a **Haar measure** if for any Borel set $E \subseteq G$ and any $x \in G$,

$$\mu(xE) = \mu(E)$$

Theorem 2. *Every locally compact topological group G admits a Haar measure μ. The measure is unique in the sense that if μ' is another Haar measure on G, then there exists a $\lambda > 0$ such that*

$$\mu(E) = \lambda \mu'(E)$$

for all Borel sets E.

Proof. See any good book on harmonic analysis. □

If $f \in C_c(G)$, and $x \in G$, define the left shift $L_x(f) \in C_c(G)$ by the formula $L_x(f)(g) = f(x^{-1}g)$.

Proposition 3. *Let μ be a Radon measure on G. Then μ is a Haar measure if and only if for all $x \in G$ and all $f \in C_c^+(G)$,*

$$\int_G L_x(f) d\mu = \int_G f\mu$$

Proof. See Fourier Analysis on Number Fields, Ramakrishnan and Valenza, Proposition 1-7. □

Let G have Haar measure μ, and let H be a closed subgroup of G. Then, one can show that the Borel sets of H are the same as the Borel sets of G which are contained in H. A natural question is: when is the restriction of μ to the Borel sets of H a Haar measure on H? Obviously this is not always the case, for example the Haar measure on $\mathbb{R}$ is the Lebesgue measure, and the Haar measure on $\mathbb{Z}$ is the counting measure.

Proposition 4. *Let H be a closed subgroup of G. The following are equivalent:*

(i) H is open.

(ii) $\mu(H) > 0$.

(iii) The restriction of μ to H is a Haar measure on H.

Proof. (Sketch) One can show, as a consequence of inner-regularity, that all open sets have nonzero measure, so (i) ⇒ (ii). We leave (ii) ⇒ (iii) as an exercise. Just check the conditions of being a Haar measure one by one. For (iii) ⇒ (i), we refer to a result of Steinhaus, which shows that a closed subgroup has nonnegative measure if and only if it is open. □

We now discuss products. Let X, Y be locally compact Hausdorff spaces with Radon measures μ and τ. We know that $X \times Y$ is locally compact Hausdorff.

Proposition 5. *Given $F \in C_c(X \times Y)$ and $y \in Y$, the function $F(-, y) : X \to \mathbb{C}$ is in $C_c(X)$. Similarly if $x \in X$, the function $F(x, -) : Y \to \mathbb{C}$ is in $C_c(Y)$. We have*

$$\int_X \int_Y F(x,y) d\tau(y) d\mu(x) = \int_Y \int_X F(x,y) d\mu(x) d\tau(y)$$

and the map $F \mapsto \int_X \int_Y F(x,y) d\tau(y) d\mu(x)$ defines a positive linear functional on $C_c(X \times Y)$.

Proof. See Hewitt and Ross, Theorem 13.2. Note that this is accomplished without the use of Fubini's theorem. In fact, the approach in the book avoids the usual construction of the product measure. □

As a result, the Riesz representation theorem gives us a unique Borel measure ρ on $X \times Y$ for which

$$\int_{X\times Y} F d\rho = \int_X \int_Y F(x,y) d\tau(y) d\mu(x) = \int_Y \int_X F(x,y) d\mu(x) d\tau(y)$$

for all $F \in C_c(X \times Y)$. A special version of Fubini's theorem (Hewitt and Ross, Theorem 13.8) gives us that the above equality holds whenever $F : X \times Y \to \mathbb{C}$ is *measurable*.

Corollary 6. *If G_1, G_2 are locally compact topological groups with Haar measures μ, τ, then there is a unique Haar measure ρ on $G_1 \times G_2$, called the* ***product measure*** *with the property that*

$$\rho(E_1 \times E_2) = \mu(E_1)\tau(E_2)$$

whenever $E_1 \subseteq X, E_2 \subseteq Y$ are Borel sets.

Proof. Proposition 5 already gives us ρ as a Radon measure. Now for any $F \in C_c(X \times Y)$, and any $(x_1, x_2) \in G_1 \times G_2$, we have

$$\int_{G_1\times G_2} L_{(x_1,x_2)}(F) d\rho = \int_{G_1} \int_{G_2} L_{(x_1,x_2)}(F)(g_1,g_2) d\tau(g_2) d\mu(g_1)$$

$$= \int_{G_1} \int_{G_2} F(x_1^{-1}g_1, x_2^{-1}g_2) d\tau(g_2) d\mu(g_2)$$

We can interchange these integrals and use Proposition 3 to see that this is just

$$\int_{G_1} \int_{G_2} F(g_1,g_2) d\tau(g_1) d\mu(g_2) = \int_{G_1\times G_2} F d\rho$$

so Proposition 3 tells us that ρ must be a Haar measure. Finally for the Borel sets E_1, E_2, we have

$$\rho(E_1 \times E_2) = \int_{G_1\times G_2} 1_{E_1\times E_2} d\rho = \int_{G_1} \int_{G_2} 1_{E_1} \cdot 1_{E_2} d\tau d\mu$$

which is clearly $\mu(E_1)\tau(E_2)$. □

Of course the result extends to a finite collection $G_1, G_2, ..., G_t$ of topological groups. If $\mu_1, ..., \mu_t$ are Haar measures on these groups, let $\mu_1 \times \cdots \times \mu_t$ be the product measure.

Lemma 7. *Let G_1, G_2 be locally compact groups with Haar measures μ_1, μ_2. Let H_1, H_2 be open subgroups of G_1, G_2, so the restriction of μ_i to the Borel sets of H_i gives a Haar measure on H_i by Proposition 3. Let λ_i be the restriction of μ_i to H_i. Then the restriction of $\mu_1 \times \mu_2$ to $H_1 \times H_2$ is $\lambda_1 \times \lambda_2$.*

Proof. Since $H_1 \times H_2$ is an open subgroup of $G_1 \times G_2$, the restriction of $\mu_1 \times \mu_2$ to $H_1 \times H_2$ gives a Haar measure. Now just use uniqueness. □

Now we show how the Haar measure on the ideles/adeles is constructed. We return to the construction in (?): we are given a set of indices v, and a collection of locally compact topological groups G_v. For all v except those belonging to a finite set S_∞), suppose that H_v is a compact open subgroup of G_v. Let μ_v be a Haar measure on G_v. For $v \notin S_\infty$, the fact that H_v is open and compact tells us that $\mu_v(H_v)$ has finite and nonzero measure, and that the restriction of μ_v to the Borel sets of H_v defines a Haar measure λ_v on H_v. We normalize μ_v so that $1 = \mu_v(H_V) = \lambda_v(H_v)$.

We will always let S be a finite sets of indices containing S_∞. Let

$$H_S = \prod_{v \notin S} H_v$$

$$G_S = (\prod_{v \in S} G_v) \times H_S$$

$$G = \bigcup_S G_S$$

where G is taken in the direct limit topology. Then H_S, G_S, G are all locally compact groups (in fact H_S is compact), and G_S is open in G, so the product topology on G_S coincides with the subspace topology from G.

Theorem 8. *Since H_S is compact, let λ_S be the Haar measure on H_S which gives it measure 1. Define a Haar measure μ_S on G_S as the product of the measures $\mu_v : v \in S$ with λ_S. Then there is a unique Haar measure μ on G with the property that the restriction of μ to any subspace G_S is μ_S. In particular, if $S \supseteq S_\infty$ is any finite set of indices, and $E_v : v \in S$ are Borel, then*

$$\mu((\prod_{v \in S} E_v) \times H_S) = \prod_{v \in S} \mu_v(E_v)$$

Proof. Exercise, or alternatively Proposition 5-5 of Ramakrishnan and Valenza. The main idea is that if $S_1 \subseteq S_2$, and, $S_2 \setminus S_1 = \{v_1, ..., v_t\}$, then the restriction of μ_{S_2} to

$$G_{S_1} = \prod_{v \in S_1} G_v \times \prod_{i=1}^{t} H_{v_i} \times H_{S_2}$$

is

$$\prod_{v \in S_1} \mu_v \times \lambda_{v_1} \times \cdots \times \lambda_{v_t} \times \lambda_{S_2}$$

which one can show is $\prod_{v \in S_1} \mu_v \times \lambda_{S_1} = \mu_{S_1}$. □

Theorem 9. *(i) Let $f : G \to \mathbb{C}$ be integrable or continuous. Then*

$$\int_G f d\mu = \lim_{S \supseteq S_\infty} \int_{G_S} f d\mu_S$$

(ii) Let S_0 be a finite set of indices containing S_∞, and suppose that for each v we have a continuous integrable function f_v on G_v such that $f_{v|H_v} = 1_{H_v}$ for all $v \notin S_0$. Define

$$f(g) = \prod_v f_v(g_v)$$

(note that for each $g \in G$, $f(g)$ is a finitely product, since almost all of the componets of g lie in H_v). Then f is continuous on G. If S is a finite set of indices containing S_0, then

$$\int_{G_S} d\mu_S = \prod_{v \in S} \int_{G_v} f_v d\mu_v$$

and

$$\int_G f = \prod_v \int_{G_v} f_v d\mu_v$$

and $f \in L^1(G)$, provided that the right hand product is finite.

Proof. Ramakrishnan and Valenza, Proposition 5-6. □

Theorem 10. *Let G be an (abelian!) topological group with Haar measure μ. Let H be a closed subgroup of G.*

(i) If $\phi : G \to \mathbb{C}$ is measurable, then the function $\overline{\phi} : G/H \to \mathbb{C}$ given by

$$\overline{\phi}(gH) = \int_H \phi(gh) d\mu(h)$$

is also measurable.

(ii) It is possible to choose a Haar measure $\overline{\mu}$ on G/H such that for any measurable ϕ:

$$\int_{G/H} \overline{\phi} d\overline{\mu} = \int_G \phi d\mu$$

Proof. Couldn't find a reference for this one. □

B Topological Tensor Product

Let A, B be commutative rings containing a field K, with A/K finite dimensional and $v_1, ..., v_n$ a basis. The tensor product $A \otimes_K B$ is then a right B-module, in fact a B-algebra, having basis $v_1 \otimes 1, ..., v_n \otimes 1$. Multiplication in the ring $A \otimes_K B$ is defined on generators by $(x \otimes y)(x' \otimes y') = xx' \otimes yy'$.

Suppose further that B is a topological ring (addition and multiplication are continuous functions $B \otimes B \to B$). The mapping

$$v_1 \otimes b_1 + \cdots + v_n \otimes b_n \mapsto (b_1, ..., b_n)$$

gives a bijection between $A \otimes_K B$ and $\prod_{i=1}^{n} B$. Using this bijection, we define a topology on $A \otimes_K B$ from the product topology on $\prod_{i=1}^{n} B$.

Lemma 1. *Addition and multiplication in $A \otimes_K B$ are continuous with respect to this topology. Furthermore, the topology does not depend on the choice of basis for A/K.*

Now we take K as a finite extension of $\mathbb{Q}$, v a place of K, and L a finite extension of K having degree n. There exists some $\beta \in L$ for which $L = K(\beta)$, with minimal polynomial $\mu \in K[X]$. Usually μ will not remain irreducible in the polynomial ring of the completion K_v, and will factor as a product $\mu_1 \cdots \mu_g$ of irreducibles here. In a fixed algebraic closure of K_v, choose a root β_i of each factor μ_i.

Lemma 1. *There is an isomorphism of K_v algebras:*

$$L \otimes_K K_v \to K_v(\beta_1) \oplus \cdots \oplus K_v(\beta_g)$$

Proof. Since $L = K(\beta)$, we have $L \otimes_K K_v = K_v(\beta \otimes 1)$. So every element of the tensor product is the evaluation of a polynomial $h \in K_v[X]$ at $\beta \otimes 1$. Therefore for each i we have a K_v-algebra homomorphism $L \otimes_K K_v \to K_v(\beta_i)$ given by $\beta \otimes 1 \mapsto \beta_i$. Obviously each such homomorphism is surjective, and we obtain our mapping

$$\Delta : L \otimes_K K_v \to K_v(\beta_1) \oplus \cdots \oplus K_v(\beta_g)$$

To show Δ is injective, suppose that $h \in K_v[X]$ is a polynomial for which

$$(0, ..., 0) = \Delta(h(\beta \otimes 1)) = (h(\beta_1), ..., h(\beta_g))$$

Then h is divisible in $K_v[X]$ by the irreducible polynomials $\mu_1, ..., \mu_n$, and hence their product μ, as they are distinct. Since $\mu(\beta \otimes 1) = 0$, we conclude that $h(\beta \otimes 1)$ must also be zero.

Surjectivity follows from here, since Δ is a K_v-linear transformation, and both sides have dimension n.

□

We use the tensor product to discuss extensions of v to places of L. If w is a place of L, we usually regard L as a subset of its completion L_w. When dealing with more than one place at a time, this may cause confusion if we are not careful. For example, if $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$, then there are two (real) places w_1 and w_2 lying over the unique real place of $\mathbb{Q}$. If we identify the completions L_{w_1} and L_{w_2} with $\mathbb{R}$, then it would not be right to say that L is a "subset" of both L_{w_1} and L_{w_2}; rather, L would be a subset of only one of them, say L_{w_1} and would embed algebraically and topologically into the other by the formula $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Alternatively, one could take w_2 to be the absolute value on L given by $|a+b\sqrt{2}|_{w_2} = |a+b\sqrt{2}|$ and literally take the completion of L_{w_2}.

It is a fact that an absolute value on a *complete* field admits a unique extension to a given finite separable extension. So for each i, there is a unique extension of K_v to $K_v(\beta_i)$. If we are regarding K as a subset of its completion K_v (usually, this is harmless), there is a natural topological/algebraic injection $L = K(\beta) \mapsto K_v(\beta_i)$. This is how we obtain an absolute value on L which extends the one we began with on K (in fact, this is how all the places of L which lie over v can be obtained). Moreover, $K_v(\beta_i)$ is exactly the completion of L under its embedding here: we identify L with $K(\beta_i)$, and it is obvious that its closure is $K_v(\beta_i)$.

Theorem 2. *The mapping*

$$\Delta : L \otimes_K K_v \to K_v(\beta_1) \oplus \cdots \oplus K_v(\beta_g)$$

is a homeomorphism and isomorphism of K_v-algebras, where the right hand side is taken in the product topology.

Proof. The codomain, which is an n-dimensional K_v-module, becomes a normed space over K_v with the norm $||(h_1(\beta_1), ..., h_g(\beta_j))|| = \text{Max}\,|h_i(\beta_i)|$. The topology induced by this norm is the product topology. Since Δ is a K_v-module isomorphism, we obtain a norm $||\cdot||_0$ on $L \otimes_K K_v$ by setting $||x||_0 = ||\Delta(x)||$.

So, there is *some* on topology $L \otimes_K K_v$ (namely, the one induced by $||\cdot||_0$) for which Δ is an isometry, hence a homeomorphism. We want to show that this topology is the one we originally had, namely the one induced from the product topology. But considering the K_v-isomorphism $L \otimes_K K_v \to \bigoplus_{i=1}^{n} K_v$, the topology from $||\cdot||_0$ is corresponds to a norm topology on the latter direct sum. But all norms on a finite dimensional space are equivalent, and they all induce the product topology. So Δ is an isometry, hence a homemorphism, of the requisite topological spaces.

□

So far we have described Δ by its effect on a polynomial in the variable $\beta \otimes 1$. This has been useful for the proofs above, but Δ can actually be described more naturally. Let $\sigma_1, ..., \sigma_g$ be the K-embeddings of L into $K(\beta_1), ..., K(\beta_g)$. If $v_1, ..., v_n$ is any basis for L/K, then Δ can be given by the formula

$$v_1 \otimes c_1 + \cdots + v_n \otimes c_n \mapsto (c_1\sigma_1(v_1) + \cdots + c_n\sigma_1(v_n), ..., c_1\sigma_n(v_n) + \cdots + c_n\sigma_n(v_n))$$

This can be seen by writing each basis element v_i as a polynomial in β.

If X, Y are complete metric spaces and $f : A \to B$ is uniformly continuous for some $A \subseteq X, B \subseteq Y$, then f extends uniquely to a uniformly continuous function $\overline{A} \to \overline{B}$. Thus given a place w lying over v, and a K-embedding $\sigma : L \to \mathbb{C}$, the fact that σ is uniformly continuous (it is an isometry between $L, |\cdot|_w$ and $\sigma L, |\cdot|_{\sigma w}$) implies that it extends uniquely to a K_v-isomorphism $L_w \to \sigma L_{\sigma(w)}$. In particular, suppose L/K is Galois with Galois group $G = \mathrm{Gal}(L/K)$. The decomposition group $G_w = \{\sigma \in G : \sigma(w) = w\}$ is isomorphic to the Galois group of L_w/K_v, and the isomorphism is obtained by extending a K-automorphism $L \to L$ to a K_v-automorphism of the completions $L_w \to L_w$. But even when σ is not in G_w, we still get a K_v isomorphism $L_w \to L_{\sigma(w)}$. The Galois group acts transitively on the primes lying over v, so all the completions $L_w : w \mid v$ are isomorphic. When v is finite, this gives another perspective for why ramification and inertia for a given place v do not depend on the choice of place lying over v (as these are algebraic invariants for an extension of p-adic fields).

Let v be a place of K corresponding to the prime ideal $\mathfrak{p}$. Let $A = \mathcal{O}_K, B = \mathcal{O}_L$, and let $\omega_1, ..., \omega_n$ be a basis for L/K. To simplify the argument I'm about to make, assume $\omega_i \in B$ (although it will remain true without this assumption).

For a finite dimensional vector space V over a field F, a Dedekind domain A of which the quotient field is F, and a symmetric, nondegenerate bilinear form on V (usually some variant of the trace function), we can define the discriminant Disc of any A-module which is contained in V and spans the whole space. The discriminant will be a fractional ideal of A. For the complete definitions, see Frohlich, Algebraic Number Theory. As we go along we will make use of several results from this same section.

If we let W be the free A-module

$$A\omega_1 + \cdots + A\omega_n$$

then $W \subseteq B$, hence $W_\mathfrak{p} \subseteq B_\mathfrak{p}$. Here $W_\mathfrak{p}$ is the localization at $\mathfrak{p}$ as an A-module, i.e.

$$W_\mathfrak{p} = A_\mathfrak{p}\omega_1 + \cdots + A_\mathfrak{p}\omega_n$$

Thus $\mathrm{Disc}(W_{\mathfrak{p}}/A_{\mathfrak{p}}) \subseteq \mathrm{Disc}(B_{\mathfrak{p}}/A_{\mathfrak{p}})$. But

$$\mathrm{Disc}(W_{\mathfrak{p}}/A_{\mathfrak{p}}) = \mathrm{Disc}(W/A)A_{\mathfrak{p}}, \mathrm{Disc}(B_{\mathfrak{p}}/A_{\mathfrak{p}}) = \mathrm{Disc}(B/A)A_{\mathfrak{p}}$$

and these are equal for almost all primes (at almost all primes each discriminant is a unit at $\mathfrak{p}$). This implies $B_{\mathfrak{p}} = W_{\mathfrak{p}}$ for almost all $\mathfrak{p}$.

Suppose $\mathfrak{p}$ is a prime for which $B_{\mathfrak{p}} = W_{\mathfrak{p}}$. Any A-module $M \subseteq L$ which spans L, or $A_{\mathfrak{p}}$-module for that matter, injects into $L \otimes_K K_v$ by the formula $x \mapsto x \otimes 1$. Let $\overline{M}$ be the image of M under this mapping. Since $\mathcal{O}_v$ (embedded in $L \otimes_K K_v$ as $y \mapsto 1 \otimes y$) is the completion of $A_{\mathfrak{p}}$, we have that $\mathcal{O}_v\overline{M} = \mathcal{O}_v\overline{M_{\mathfrak{p}}}$.

Consider the ring isomorphism/homeomorphism

$$L \otimes_K K_v \to \prod_{w|v} L_w$$

Under this mapping, $\mathcal{O}_v\overline{B} = \mathcal{O}_v\overline{B_{\mathfrak{p}}}$ corresponds to $\prod_{w|v} \mathcal{O}_w$ (section 4, Lemma 2 in Frohlich). But we assumed that $B_{\mathfrak{p}} = W_{\mathfrak{p}}$, where

$$\mathcal{O}_v\overline{W_{\mathfrak{p}}} = \mathcal{O}_v(\omega_1 \otimes 1) + \cdots + \mathcal{O}_v(\omega_n \otimes 1)$$

Furthermore using the basis ω_i, we have an (additive) topological group isomorphism

$$\prod_{i=1}^{n} K_v \to L \otimes_K K_v$$

$$(c_1, ..., c_n) \mapsto \omega_1 \otimes c_1 + \cdots \omega_n \otimes c_n$$

wherein the subgroup $\mathcal{O}_v\overline{W_{\mathfrak{p}}}$ corresponds to the product $\prod_{i=1}^{n} \mathcal{O}_v$. Let us state this all as a theorem:

Theorem. *Fix a basis $\omega_1, ..., \omega_n$ for L/K. This basis induces, for every place v, an isomorphism of topological groups*

$$\prod_{i=1}^{n} K_v \to \prod_{w|v} L_w$$

where, for almost all places v, restriction induces another topological group isomorphism

$$\prod_{i=1}^{n} \mathcal{O}_v \to \prod_{w|v} \mathcal{O}_w$$