ALGEBRAIC NUMBER THEORY (I)

YIHANG ZHU

Contents

The **goal of this course** is the statements of global and local class field theory, and applications. We will *not* prove class field theory.

The **main reference** which we will follow closely is Rabinoff's notes for a course at Harvard, 2012. Classical references include [CF+67], [Neu99], and [Ser79]. Some other online lecture notes (e.g. J. Milne's notes [Mil20]) can be helpful too.

Preliminaries. Algebra 1, Algebra 2, Number Fields (roughly the first two chapters of [Neu99], or the first two chapters of [Ser79]; this corresponds to a first course on algebraic number theory).

Overview

The goal of class field theory is to classify abelian extensions of a global or local field.

A *global field* refers to a field which is either a finite extension of $\mathbb{Q}$, or a finite extension of $\mathbb{F}_p(t)$, where p is a prime.

A *local field* refers to a field which is either a finite extension of $\mathbb{Q}_p$ (the field of p-adic numbers), or a field of the form $\mathbb{F}_q(\!(t)\!) = \operatorname{Frac} \mathbb{F}_q[\![t]\!]$.

An *abelian extension* means a Galois extension L/K (finite or infinite) such that $\mathrm{Gal}(L/K)$ is abelian.

Ideal theoretic formulation of global class field theory. Let K be a global field. By a *modulus*, we mean a formal product of the form $\mathfrak{m} = v_1^{n_1} \cdots v_k^{n_k}$, where v_i are places of K and n_i are non-negative integers. It should satisfy the following conditions:

(1) v_i cannot be a complex place.
(2) If v_i is a real place, then $n_i \in \{0, 1\}$.

Recall that the class group of K is the cokernel of a natural map from $K^\times$ to the free abelian group $\mathbb{Z}[V_{K,f}]$ generated by the non-archimedean places of K. Given $\mathfrak{m}$ as above, we can define a certain subgroup $\{x \in K^\times \mid x \equiv 1 \mod \mathfrak{m}\}$ of $K^\times$, and a map from it to the free abelian group generated by the non-archimedean places of K *not appearing* in $\mathfrak{m}$. The cokernel is denoted by $\mathrm{Cl}_\mathfrak{m}$, called the *ray class group* associated with $\mathfrak{m}$. This turns out to be a *finite* abelian group.

There is an obvious way to define divisibility relation $\mathfrak{m}|\mathfrak{m}'$, for two moduli $\mathfrak{m}, \mathfrak{m}'$. For $\mathfrak{m}|\mathfrak{m}'$, there is a natural surjection $\mathrm{Cl}_{\mathfrak{m}'} \to \mathrm{Cl}_\mathfrak{m}$. As such, the $\mathrm{Cl}_\mathfrak{m}$ for varying $\mathfrak{m}$ form a projective system of finite abelian groups.

By a *generalized class group*, we mean a quotient group of $\mathrm{Cl}_{\mathfrak{m}}$ for some choice of $\mathfrak{m}$. If $\mathfrak{m}|\mathfrak{m}'$, then each quotient group of $\mathrm{Cl}_{\mathfrak{m}}$ is naturally identified with a quotient group of $\mathrm{Cl}_{\mathfrak{m}'}$ via the projection $\mathrm{Cl}_{\mathfrak{m}'} \to \mathrm{Cl}_{\mathfrak{m}}$. Modulo this equivalence relation, we let $\mathscr{S} = \mathscr{S}_K$ be the set of all generalized class groups.

Theorem 0.0.1 (Takagi)**.** *There is a natural bijection from the set of all finite abelian extensions of K (inside a fixed algebraic closure $\overline{K}$) to the set $\mathscr{S}$.*

Theorem 0.0.2 (Artin)**.** *If L/K corresponds to G under the above bijection, then there is a canonical isomorphism* $\mathrm{Gal}(L/K) \xrightarrow{\sim} G$*.*

Adelic formulation of global class field theory. Let K be a global field. The group of ideles[1] for K is a certain subgroup $\mathbb{A}_K^\times = \mathbb{I}_K$ of $\prod_v K_v^\times$, where v runs over all places of K, and K_v is the completion of K with respect to v. The advantage of $\mathbb{A}_K^\times$ over the full $\prod_v K_v^\times$ is that it is a Hausdorff *locally compact* abelian topological group. The diagonal embedding $K^\times \hookrightarrow \prod_v K_v^\times$ factors through $\mathbb{A}_K^\times$, and we define $C_K := \mathbb{A}_K^\times / K^\times$, called the *idele class group* of K. For any finite extension L/K, there is a norm map $\mathrm{N}_{L/K} : C_L \to C_K$.

Theorem 0.0.3. *There is a canonical continuous homomorphism $\phi_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, satisfying the following conditions. (Here K^{ab} is the maximal abelian extension of K in $\overline{K}$, which is infinite over K.)*

1. *(Reciprocity) For any finite abelian extension L/K, let $\phi_{L/K}$ be the composition of ϕ_K with the natural projection $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$. Then $\phi_{L/K}$ is surjective, and its kernel is the image of $\mathrm{N}_{L/K} : C_L \to C_K$.*
2. *(Existence Theorem) We have a bijection from the set of finite abelian extensions of K in $\overline{K}$ to the set of open and finite index subgroups of C_K, sending L/K to $\mathrm{N}_{L/K}(C_L)$.*
3. *Some functoriality properties of ϕ_K when K changes.*

Local class field theory. Let K be a local field. The role played by C_K in the global case is played by $K^\times$ in the local case. Note that $K^\times$ is also a Hausdorff locally compact abelian group.

Theorem 0.0.4. *There is a canonical continuous homomorphism $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, satisfying the following conditions.*

1. *(Reciprocity) For any finite abelian extension L/K, let $\phi_{L/K}$ be the composition of ϕ_K with the natural projection $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$. Then $\phi_{L/K}$ is surjective, and its kernel is the image of $\mathrm{N}_{L/K} : L^\times \to K^\times$. Moreover, if L/K is unramified (in which case $\mathrm{Gal}(L/K)$ is a cyclic group generated by the Frobenius), then $\phi_{L/K}$ sends any uniformizer in $K^\times$ to the Frobenius.*
2. *(Existence Theorem) We have a bijection from the set of finite abelian extensions of K in $\overline{K}$ to the set of open and finite index subgroups of $K^\times$, sending L/K to $\mathrm{N}_{L/K}(L^\times)$.*
3. *Some functoriality properties of ϕ_K when K changes.*

Note the similarity to the theorem in the global case.

[1] The word "idele" is an abbreviation of "ideal element"

1. Review of global and local fields

1.1. **Places.** Recall that an *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the axioms:

(1) $|x| = 0$ iff $x = 0$;
(2) $|xy| = |x||y|, \forall x, y \in K$;
(3) $|x + y| \leq |x| + |y|, \forall x, y \in K$.

If the strong triangle inequality holds:

$$|x + y| \leq \max(|x|, |y|), \quad \forall x, y \in K$$

then we call $|\cdot|$ *non-archimedean.* Otherwise we call it *archimedean.*

An absolute value $|\cdot|$ makes K a metric space by $d(x, y) = |x - y|$, and hence a topological space. It in fact makes K a topological field. We also **always assume** that $|\cdot|$ takes at least three different values (i.e., at least one extra value other than $0, 1$), which is equivalent to requiring that the corresponding topology on K is not discrete.

Two absolute values $|\cdot|$ and $|\cdot|'$ are called *equivalent* if there exists $e > 0$ such that $|\cdot|' = |\cdot|^e$. A *place* of K refers to an equivalence class of absolute values.

Exercise 1.1.1. Let K be a field.

(1) Show that two absolute values $|\cdot|$ and $|\cdot|'$ on K are equivalent if and only if they define the same topology on K.
(2) Show that they are not equivalent if and only if there exists $x \in K$ such that $|x| < 1$ and $|x|' \geq 1$.
(3) Prove the *Approximation Lemma*: Let $|\cdot|_1, \dots, |\cdot|_n$ be pairwise non-equivalent absolute values on K. For any $x_1, \dots x_n \in K$ and $\epsilon > 0$, there exists $y \in K$ such that $|y - x_i|_i < \epsilon$ for all $1 \leq i \leq n$.

Exercise 1.1.2. Prove that for an absolute value $|\cdot|$ on a field K, the following conditions are equivalent:

(1) $|\cdot|$ is archimedean (i.e., strong triangle inequality does not always hold).
(2) There exists a real number $0 < e \leq 1$ such that $|n| = n^e$ for all $n \in \mathbb{Z}_{\geq 1}$. (In particular K has characteristic zero.)
(3) There exists $n \in \mathbb{Z}_{>1}$ such that $|n| > 1$.

(Hint: For the equivalence of (2) and (3), first prove that for any $a, b \in \mathbb{Z}_{\geq 2}$, we have $|a| \leq \max(1, |b|^{\log_b a})$ by considering the base b expansion of a^k. For (1) $\Rightarrow$ (3), consider binomial expansion of $(1 + x)^k$, for $x \in K$.)

Note: Clearly this exercise implies that the only archimedean place on $\mathbb{Q}$ is the usual one. For the exercise, you are not allowed to use this fact.

Fact 1.1.3. *Let K be a field. Then there is a surjection from* $\mathrm{Hom}(K, \mathbb{C})$ *(field homomorphisms) to the set of archimedean places of K, sending $\phi : K \to \mathbb{C}$ to the composition of ϕ with the usual absolute value on $\mathbb{C}$. Two elements of* $\mathrm{Hom}(K, \mathbb{C})$ *are sent to the same place if and only if they differ by complex conjugation.*

The key point is to show that for any archimedean place of K, the completion $\widehat{K}$ of K with respect to it is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. By Exercise 1.1.2, K must contain $\mathbb{Q}$, and the restriction of the place to $\mathbb{Q}$ is the usual archimedean place of $\mathbb{Q}$. Hence $\widehat{K}$ is a Banach $\mathbb{R}$-algebra. The desired result then follows from the Gelfand–Mazur theorem, which states that the only Banach $\mathbb{R}$-algebras which are fields are $\mathbb{R}$ and $\mathbb{C}$.

1.2. **Global fields.** A *global field* refers to a field which is either a finite extension of $\mathbb{Q}$, or a finite extension of $\mathbb{F}_p(t)$, where p is a prime. In the former case the field is called a *number field*, and in the latter case a *global function field*.

Exercise 1.2.1. Let K be a global function field of characteristic p. Show that there exists an embedding $\mathbb{F}_p(t) \hookrightarrow K$ which makes K a finite *separable* extension of $\mathbb{F}_p(t)$. (Hint: you may use the fact that K has transcendence degree 1 over $\mathbb{F}_p$, i.e., any maximal subset of K which is algebraically independent over $\mathbb{F}_p$ has exactly one element. You may also induct on the inseparable degree.)

Let K be a global field. Let V_K denote the set of all places of K, $V_{K,\infty}$ the set of all infinite (i.e. archimedean) places of K, and $V_{K,f}$ the set of all finite (i.e. non-archimedean) places of K.

For each $v \in V_K$, we define a normalized "absolute value" $\|\cdot\|_v : K \to \mathbb{R}_{\geq 0}$ as follows.

If v is a real place corresponding to $\phi : K \hookrightarrow \mathbb{R}$, let $\|\cdot\|_v$ be the usual absolute value on $\mathbb{R}$ pulled back to K via ϕ. This represents v.

If v is a complex place corresponding to $\phi : K \hookrightarrow \mathbb{C}$ (not factoring through $\mathbb{R}$), the usual absolute value on $\mathbb{C}$ pulled back to K via ϕ represents v. Let $\|\cdot\|_v$ be the *square* of it. It is *not* an absolute value, since the triangle inequality is not satisfied.

If $v \in V_f$, let $|\cdot|$ be a representative of v. Recall that a *discrete valuation* on K is a non-zero group homomorphism $\mathrm{ord} : K^\times \to \mathbb{Z}$ such that $\mathrm{ord}(x+y) \geq \min(\mathrm{ord}(x), \mathrm{ord}(y))$ for all $x, y \in K^\times$. By convention, we always set $\mathrm{ord}(0) = +\infty$. If ord is surjective, we say it is normalized. For the given $|\cdot|$, there is a unique real number $0 < \alpha < 1$ and a unique normalized discrete valuation $\mathrm{ord}_v : K^\times \to \mathbb{Z}$ such that $|x| = \alpha^{\mathrm{ord}_v(x)}$ for all $x \in K^\times$. Moreover, ord_v depends only on v, not on the representative $|\cdot|$.

Given $v \in V_f$, we define the valuation ring $\mathcal{O}_{K,(v)} := \{x \in K \mid \mathrm{ord}_v(x) \geq 0\}$. It is a subring of K, and a DVR with unique maximal ideal $\mathfrak{m}_v = \{x \in K \mid \mathrm{ord}_v(x) > 0\}$. We define the residue field of v to be $k_v := \mathcal{O}_{K,(v)}/\mathfrak{m}_v$, i.e., the residue field of the DVR $\mathcal{O}_{K,(v)}$. This is always a finite field for a global field K. Define

$$\|\cdot\|_v := (\# k_v)^{-\mathrm{ord}_v(\cdot)}.$$

This is our normalized representative of v.

Fact 1.2.2 (Product formula)**.** *For all $x \in K^\times$, we have $\prod_{v \in V_K} \|x\|_v = 1$. Here $\|x\|_v = 1$ for almost all v.*

1.3. **The ring of S-integers.** Let S be a non-empty finite subset of V_K containing $V_{K,\infty}$. We define the ring of S-integers to be

$$\mathcal{O}_{K,S} := \{f \in K \mid \forall v \in V_K - S, \mathrm{ord}_v(f) \geq 0\}.$$

This is a Dedekind domain whose fraction field is K, and there is a bijection

$$V_K - S \xrightarrow{\sim} \{\text{non-zero prime ideals of } \mathcal{O}_{K,S}\} = |\operatorname{Spec} \mathcal{O}_{K,S}|$$

sending v to $\mathfrak{p}_v := \{f \in \mathcal{O}_{K,S} \mid \mathrm{ord}_v(f) > 0\}$. Here $|\operatorname{Spec} \mathcal{O}_{K,S}|$ denotes the set of closed points of $\operatorname{Spec} \mathcal{O}_{K,S}$. The residue field of $\mathfrak{p}_v$ is the residue field of v, so it is independent of S.

If S' is another finite subset of V_K containing S, then we have $\mathcal{O}_{K,S} \subset \mathcal{O}_{K,S'}$, and the corresponding map $\operatorname{Spec} \mathcal{O}_{K,S'} \to \operatorname{Spec} \mathcal{O}_{K,S}$ is an open immersion, compatible with the bijections $|\operatorname{Spec} \mathcal{O}_{K,S}| \cong V_K - S$ and $|\operatorname{Spec} \mathcal{O}_{K,S'}| \cong V_K - S'$.

If K is a number field, there is a minimal choice of S, namely $S = V_{K,\infty}$. In this case $\mathcal{O}_{K,S}$ is the usual ring of integers $\mathcal{O}_K$, namely the integral closure of $\mathbb{Z}$ in K. Thus every $\operatorname{Spec} \mathcal{O}_{K,S}$ is an open subscheme of $\operatorname{Spec} \mathcal{O}_K$ by deleting finitely many closed points.

If K is a global function field of characteristic p, let k be the algebraic closure of $\mathbb{F}_p$ in K. Then k is a finite field, called the field of constants in K. There is a unique (up to isomorphism) smooth, projective, geometrically connected (meaning that $X_{\bar{k}}$ is connected) curve X over k such that K is the field of rational functions $k(X)$ on X. This X plays the role of $\operatorname{Spec} \mathcal{O}_K$ in the number field case, in the sense that every $\operatorname{Spec} \mathcal{O}_{K,S}$ is obtained from X by deleting finitely many closed points. (However, X is not affine.) More precisely, there is a canonical bijection

$$|X| \xrightarrow{\sim} V_K, \quad x \mapsto v_x.$$

Here $|X|$ denotes the set of closed points, and v_x is the place corresponding to the discrete valuation $\operatorname{ord}_x : K^\times \to \mathbb{Z}$ sending f to its "order of zero"[2] at x. The valuation ring $\mathcal{O}_{K,(v_x)}$ (resp. residue field k_{v_x}) of v_x is equal to the local ring $\mathcal{O}_{X,x}$ (resp. residue field $k(x)$) defined in algebraic geometry. For any finite non-empty subset S of V_K, we view S as a finite set of closed points of X, and obtain the open subscheme $X - S \subset X$. Then $X - S$ is an affine scheme (which is not true if $S = \emptyset$), and identified with $\operatorname{Spec} \mathcal{O}_{K,S}$.

Let K be any global field, and S as above. As for any Dedekind domain, we can consider the class group $\operatorname{Cl}(\mathcal{O}_{K,S})$ of $\mathcal{O}_{K,S}$, defined as the group of fractional ideals modulo the group of principal fractional ideals. By the identification $V_K - S \cong |\operatorname{Spec} \mathcal{O}_{K,S}|$, the class group is also the cokernel of the map

$$K^\times \to \mathbb{Z}[V_K - S], \quad f \mapsto \sum_{v \in V_K - S} \operatorname{ord}_v(f)[v].$$

Here $\mathbb{Z}[V_K - S]$ denotes the free abelian group generated by the set $V_K - S$, whose elements are finite $\mathbb{Z}$-linear combinations of the symbols $[v]$ for $v \in V_K - S$. As before, we denote by ord_v the normalized discrete valuation corresponding to (the non-archimedean) v. If K is a global function field $K = k(X)$, we can even consider the cokernel of

$$K^\times \to \mathbb{Z}[V_K], \quad f \mapsto \sum_{v \in V_K} \operatorname{ord}_v(f)[v].$$

This is nothing but the class group (or Picard group) of X.

For more on the geometric point of view towards global function fields, see [Neu99, Ch. I, §§13–14] for a brief introduction, and [GW20, §15] for a more thorough treatment. (The bijection $V_K \xrightarrow{\sim} |X|$ is not discussed in [GW20], but it is an easy consequence of the valuative criterion for properness and the fact that if $v_1, v_2 \in V_K$ are such that $\mathcal{O}_{K,(v_1)} \subset \mathcal{O}_{K,(v_2)}$, then $v_1 = v_2$ (Exercise).)

1.4. **Extensions of global fields.** Let L/K be a finite separable extension of global fields. Then we have a map $V_L \to V_K$ by restriction of absolute values. If $w \mapsto v$, we write $w|v$. This map has finite fibers.

Fix a finite non-empty subset $S \subset V_K$ containing $V_{K,\infty}$, and let T be the inverse image of S in V_L. Then we have $\mathcal{O}_{K,S} \subset \mathcal{O}_{L,T}$.

Fact 1.4.1. *$\mathcal{O}_{L,T}$ is a finite projective $\mathcal{O}_{K,S}$-module.*

[2] Since X is over a non-algebraically closed field k, the rigorous definition of ord_x is that it is the canonical normalized discrete valuation associated with the DVR $\mathcal{O}_{X,x}$, the local ring of X at x.

Fix $v \in V_K - S$, corresponding to a non-zero prime ideal $\mathfrak{p} = \mathfrak{p}_v$ of $\mathcal{O}_{K,S}$. We can consider the decomposition of $\mathfrak{p}$ in $\mathcal{O}_{L,T}$:

$$\mathfrak{p}\mathcal{O}_{L,T} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where $\mathfrak{P}_i$ are distinct non-zero prime ideals of $\mathcal{O}_{L,T}$. Let $w_i \in V_L - T$ be the element corresponding to $\mathfrak{P}_i$. For each w_i, the inclusion $\mathcal{O}_{L,T} \to \mathcal{O}_{L,(w_i)}$ induces an isomorphism $\mathcal{O}_{L,T}/\mathfrak{P}_i \xrightarrow{\sim} k_{w_i}$. Similarly, we have $\mathcal{O}_{K,S}/\mathfrak{p} \xrightarrow{\sim} k_v$. These isomorphisms are compatible with the natural field extensions $\mathcal{O}_{K,S}/\mathfrak{p} \hookrightarrow \mathcal{O}_{L,T}/\mathfrak{P}_i$ and $k_v \hookrightarrow k_{w_i}$ (induced by $\mathcal{O}_{K,(v)} \hookrightarrow \mathcal{O}_{L,(w_i)}$). Define $f_i := [k_{w_i} : k_v] = [\mathcal{O}_{L,T}/\mathfrak{P}_i : \mathcal{O}_{K,S}/\mathfrak{p}]$.

Fact 1.4.2. *The set $\{w_1, \ldots, w_g\}$ is equal to $\{w \in V_L \mid w|v\}$, so it depends only on v, not on S. For each $1 \le i \le g$, the integers e_i, f_i depend only on v and w_i, not on S. We write $e(w_i/v), f(w_i/v)$ for them. We have*

$$\sum_{w \in V_L, w|v} e(w/v) f(w/v) = [L : K].$$

The last numerical identity can be understood more conceptually as follows. If $w|v$, then the completion L_w of L with respect to the place w, is naturally a field extension of the completion K_v. It also contains L, so it is a $L \otimes_K K_v$-algebra. We denote the structure map $L \otimes_K K_v \to L_w$ by i_w.

Fact 1.4.3 (Relationship between global and local extensions)**.** *The maps i_w induce an isomorphism of K_v-algebras*

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{w, w|v} L_w, \quad x \mapsto (i_w(x))_w.$$

Moreover, $e(w/v)$ and $f(w/v)$ depend only on the extension of local fields L_w/K_v, as they are the ramification index and residue extension degree of L_w/K_v (see later). We have $[L_w : K_v] = e(w/v)f(w/v)$.

Taking dimensions over K_v, we obtain

$$[L : K] = \sum_{w \in V_L, w|v} [L_w : K_v] = \sum_w e(w/v)f(w/v). \tag{1.1}$$

The first assertion in the above fact is also true for an archimedean place v. In this case, we define $e(w/v)$ to be $[L_w : K_v]$, and define $f(w/v)$ to be 1. Then (1.1) still holds.

1.5. **Galois theory for global fields.** Let L/K be a finite Galois extension of global fields. Let $G = \mathrm{Gal}(L/K)$. Then G acts on V_L by $g|\cdot| = |g^{-1}(\cdot)|$. Then for each $v \in V_K$, G permutes $\{w \in V_L \mid w|v\}$. For each such w, define the decomposition group $D(w/v)$ to be the stabilizer of w in G.

For $g \in D(w/v)$, as an automorphism of L it preserves the absolute value $\|\cdot\|_w$, and so it extends by continuity to a unique automorphism $\tilde{g}$ of L_w. Since K is dense in K_v with respect to $\| \mathrm{cot} \|_w$, we have $\tilde{g} \in \mathrm{Aut}(L_w/K_v)$. Hence we have a homomorphism

$$\phi : D(w/v) \to \mathrm{Aut}(L_w/K_v), \quad g \mapsto \tilde{g}.$$

By Fact 1.6.1 below, every $h \in \mathrm{Aut}(L_w/K_v)$ automatically preserves $\|\cdot\|_w$ on L_w, and so its restriction to L is an element of $D(w/v)$. This gives an inverse of ϕ, and so ϕ is an isomorphism.

If O is a G-orbit in the set $\{w \in V_L \mid w|v\}$, then

$$\sum_{w \in O} \#D(w/v) = \#G = [L:K] \overset{(1.1)}{=} \sum_{w \in V_L, w|v} [L_w : K_v].$$

But $\#D(w/v) = \#\operatorname{Aut}(L_w/K_v) \leq [L_w : K_v]$, so we conclude that

- The G-action on $\{w \in V_L \mid w|v\}$ is transitive.
- Each L_w/K_v is a finite Galois extension, with Galois group identified with $D(w/v)$.

From the transitivity, it easily follows that in the current Galois case, $e(w/v)$ and $f(w/v)$ depend only on v and L/K, not on w. We write them as $e(L/v), f(L/v)$. Moreover, $D(w/v)$ for different choices of $w|v$ are conjugate. If G is abelian, then they are all equal, and we denote them by $D(L/v)$.

1.6. **Completely valued fields.** By a completely valued field, we mean a field together with an absolute value $(K, |\cdot|)$ such that K is complete with respect to the topology defined by $|\cdot|$ (i.e., every Cauchy sequence converges, which is a condition depending only on the topology). As always we assume that $|\cdot|$ takes at least three values, so K is not discrete. Often we will only remember the topology of K, not $|\cdot|$. In other words, we remember only the equivalence class of $|\cdot|$.

Fact 1.6.1 (See [Bou87] Ch. I, §2)**.** *Let K be a completely valued field, and let V be a finite dimensional topological K-vector space (i.e., V is equipped with a topology such that the addition map $V \times V \to V$ and scalar multiplication map $K \times V \to V$ are continuous) which is Hausdorff. Then every K-subspace of V is closed, and every K-vector space isomorphism $K^n \xrightarrow{\sim} V$ is automatically a homeomorphism (where K^n has the product topology).*

Fact 1.6.2. *Every archimedean completely valued field is topologically isomorphic to $\mathbb{R}$ and $\mathbb{C}$.*

The proof was already discussed below Fact 1.1.3.

For a non-archimdean completely valued field $(K, |\cdot|)$, one of the most important facts is Hensel's lemma. Let $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ and $\mathfrak{m}_K = \{x \in K \mid |x| < 1\}$. Then $\mathcal{O}_K$ is a subring of K, and $\mathfrak{m}_K$ is its unique maximal ideal. Define the residue field $k := \mathcal{O}_K/\mathfrak{m}_K$. Denote the natural map $\mathcal{O}_K[X] \to k[X]$ by $f \mapsto \bar{f}$.

Theorem 1.6.3 (Hensel's Lemma)**.** *Let $f \in \mathcal{O}_K[X]$ be such that its image $\bar{f}$ in $k[X]$ is non-zero. Suppose we have $\bar{f} = \bar{g}\bar{h}$ for $\bar{g}, \bar{h} \in k[X]$ which are coprime. Then there exist $g, h \in \mathcal{O}_K[X]$ lifting $\bar{g}, \bar{h}$ such that $\deg g = \deg \bar{g}$, $f = gh$. (But $\deg h$ may not equal $\deg \bar{h}$.)*

Proof. Without loss of generality we may assume that $\bar{g}$ is monic. Let $g_1 \in \mathcal{O}_K[X]$ be a monic lift of $\bar{g}$, so $\deg g_1 = \deg \bar{g}$. Since g_1 is monic, we can divide f by g_1 with remainder and get $f = g_1 h_1 + r_1$ with $h_1, r_1 \in \mathcal{O}_K[X], \deg r_1 < \deg g_1$. Then $\bar{g}\bar{h}_1 + \bar{r}_1 = \bar{f} = \bar{g}\bar{h}$. Since $\deg \bar{r}_1 \leq \deg r_1 < \deg g_1 = \deg \bar{g}$, it follows that $\bar{h}_1 = \bar{h}$ and $\bar{r}_1 = 0$. Since $\bar{g}$ and $\bar{h}$ are coprime, there exist $a_0, b_0 \in \mathcal{O}_K[X]$ such that $a_0 h_1 + b_0 g_1 \in 1 + \mathfrak{m}_K[X]$. Let $\pi \in \mathfrak{m}_K$ be such that $r_1 \in \pi\mathcal{O}_K[X]$ and $a_0 h_1 + b_0 g_1 \in 1 + \pi\mathcal{O}_K[X]$. We induct on $n \in \mathbb{Z}_{\geq 1}$ to construct $g_n \in \mathcal{O}_K[X]$ such that

- g_n is a monic lift of $\bar{g}$. In particular $\deg g_n = \deg \bar{g}$.
- If $n \geq 2$, then $g_n \in g_{n-1} + \pi^{n-1}\mathcal{O}_K[X]$.
- Dividing f by g_n with remainder:

$$f = g_n h_n + r_n, \quad h_n, r_n \in \mathcal{O}_K[X], \quad \deg r_n < \deg g_n,$$

we have $r_n \in \pi^n \mathcal{O}_K[X]$.

The base case $n = 1$ is already done. Suppose g_n has been constructed. Then we also have h_n, r_n, and $r_n \in \pi^n \mathcal{O}_K[X]$. Write $r_n = \pi^n s_n, s_n \in \mathcal{O}_K[X]$. We claim that $a_0 h_n + b_0 g_n \equiv 1 \mod \pi$. We have $g_n \equiv g_1 \mod \pi$ and $r_n \equiv 0 \mod \pi$, so $f \equiv g_1 h_n \mod \pi$. But also $f \equiv g_1 h_1 \mod \pi$. Since g_1 is monic, its image in $(\mathcal{O}_K/\pi)[X]$ is not a zero-divisor. Hence $h_n \equiv h_1 \mod \pi$. This proves the claim. By the claim, there exist $a_n, b_n \in \mathcal{O}_K[X]$ (e.g. $a_n = a_0 s_n, b_n = b_0 s_n$) such that

$$a_n h_n + b_n g_n \equiv s_n \mod \pi.$$

Moreover, we may replace a_n by the remainder of a_n divided by g_n, and assume that $\deg a_n < \deg g_n$. Set

$$g_{n+1} = g_n + \pi^n a_n.$$

We check that it has the desired properties. Only the last one is non-obvious. Write

$$a_n h_n + b_n g_n = s_n + \pi t_n, \quad t_n \in \mathcal{O}_K[X].$$

We have

$$g_{n+1}(h_n + \pi^n b_n) = g_n h_n + \pi^n (s_n + \pi t_n) + \pi^{2n} a_n b_n \equiv f \mod \pi^{n+1}.$$

This implies the last desired property (but h_{n+1} may not be $h_n + \pi^n b_n$.) We have finished constructing the g_n's.

Since $\deg g_n$ is constant, the second property above implies that the limit $g = \lim_n g_n$ exists in $\mathcal{O}_K[X]$, and is monic. It is a lift of $\bar{g}$. Divide f by g with remainder:

$$f = gh + r, \quad \deg r < \deg g.$$

Then the image of r in $(\mathcal{O}_K/\pi^n)[X]$ is divisible by the image of g, since the image of f is divisible by the latter. As g is monic and $\deg r < \deg g$, this is possible only when $r \equiv 0 \mod \pi^n$. This holds for all n, so $r = 0$. Comparing $f = gh$ and $\bar{f} = \bar{g}\bar{h}$, we see that h is a lift of $\bar{h}$. □

Fact 1.6.4. *Let $(K, |\cdot|_K)$ be a completely valued field, and let L/K be a finite field extension. Then there is a unique absolute value $|\cdot|_L$ on L whose restriction to K is $|\cdot|_K$. The valued field $(L, |\cdot|_L)$ is also complete. Moreover, we have $|x|_L = |\mathrm{N}_{L/K} x|_K^{1/[L:K]}$ for all $x \in K$.*

The uniqueness of $|\cdot|_L$ and the completeness of $(L, |\cdot|_L)$ follow easily from Fact 1.6.1. For the existence, we need to check that the formula $|\mathrm{N}_{L/K} x|_K$ gives an absolute value on L. If K is archimedean, then it is either $\mathbb{R}$ or $\mathbb{C}$, and this is trivial. In the non-archimedean case, this is shown in the exercise below.

Exercise 1.6.5. Let $(K, |\cdot|)$ be a non-archimedean completely valued field.

1. Use Hensel's lemma to show that if $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ is a power of an irreducible polynomial, then $\max_{i=0}^n |a_i| = \max(|a_n|, |a_0|)$.
2. Let L/K be a finite extension. Show that the function $L \to \mathbb{R}_{\geq 0}, x \mapsto |\mathrm{N}_{L/K}(x)|$ is a non-archimedean absolute value on L. (Hint: in order to check $|\mathrm{N}_{L/K}(x + 1)| \leq \max(1, |\mathrm{N}_{L/K}(x)|), \forall x \in L$, relate both $\mathrm{N}_{L/K}(x+1)$ and $\mathrm{N}_{L/K}(x)$ to the characteristic polynomial of $L \to L, y \mapsto xy$. Then use (1).)

Exercise 1.6.6. Prove the first assertion in Fact 1.4.3 by using Facts 1.6.1 and 1.6.4 in the following steps.

1. Each i_w is surjective.
2. For any K, any field extension K'/K, and any finite separable extension L/K, the K'-algebra $L \otimes_K K'$ is a product of finite field extensions of K'. (Hint: apply the Primitive Element Theorem to L/K.)

(3) There is a one-to-one correspondence between the L_w's and the field factors of $L \otimes_K K'$.

By Fact 1.6.4, the absolute value on K extends uniquely to any algebraic extension L/K. Clearly if two elements of L are conjugate over K (i.e., having the same minimal polynomial), then they have the same absolute value.

In the following, whenever we consider a finite extension of completely valued fields, the absolute values are always assumed to be compatible, up to equivalence.

For a non-archimedean completely valued field $(K, |\cdot|)$, we can further divide into the *discretely valued* case and the *non-discretely valued* case, according as whether $|K^\times|$ is a discrete subgroup of $\mathbb{R}_{>0}$. In the discretely valued case, there exists a unique $0 < \alpha < 1$ and a unique normalized discrete valuation $\mathrm{ord}_K : K^\times \to \mathbb{Z}$ such that $|\cdot| = \alpha^{\mathrm{ord}_K(\cdot)}$. Moreover ord_K depends only on the equivalence class of $|\cdot|$. In this case, $\mathcal{O}_K$ is a DVR, and it is complete in the sense that the natural map

$$\mathcal{O}_K \to \varprojlim_{n\geq 1} \mathcal{O}_K/\mathfrak{m}_K^n$$

is an isomorphism.

Conversely, for any field K, any normalized (or just non-zero) discrete valuation ord_K on K, if the resulting $\mathcal{O}_K = \{x \in K \mid \mathrm{ord}_K(x) \geq 0\}$ (which is a DVR) is complete, then $(K, \alpha^{\mathrm{ord}_K})$ for any $0 < \alpha < 1$ is a completely discretely valued field.

Remark 1.6.7. If K is a completely discretely valued field and L/K is a finite extension, then the unique extension of absolute value makes L a completely discretely valued field.

1.7. Local fields.

Fact 1.7.1. *A non-archimedean completely valued field K is locally compact if and only if it is discretely valued and the residue field is finite.*

Remark 1.7.2. Every archimedean completely valued field (i.e. $\mathbb{R}$ or $\mathbb{C}$) is locally compact. By Fact 1.6.1, if K is a locally compact completely valued field, then so is any finite extension of it as the latter is homeomorphic to K^n.

Definition 1.7.3. A *local field* is a completely valued field which is locally compact.

Fact 1.7.4. *An archimedean local field is $\mathbb{R}$ or $\mathbb{C}$. A non-archimedean local field is either a finite extension of $\mathbb{Q}_p$ or is isomorphic to $\mathbb{F}_q((t))$, with valuation given by $\mathrm{ord}(\sum_{i=n}^{+\infty} a_i t^i) = n$, where $n \in \mathbb{Z}$ and $a_n \neq 0$.*

1.8. **More on polynomials (not using completeness).** Let $(K, |\cdot|)$ be a completely valued field. Define

$$\mathrm{ord}(\cdot) = -C \log |\cdot| : K^\times \to \mathbb{R},$$

where $C \in \mathbb{R}_{>0}$ is a constant. Then ord is a valuation. By Fact 1.6.4, it extends uniquely to a valuation

$$\mathrm{ord} : \bar{K}^\times \to \mathbb{R}, \quad x \mapsto \frac{1}{[K(x):K]} \mathrm{ord}(\mathrm{N}_{K(x)/K}(x)).$$

Given a non-zero $f \in K[X]$, one is thus interested in $\mathrm{ord}(\alpha)$ for the roots α of f in $\bar{K}$.

Write $f(X) = a_0 + a_1 X + \cdots + a_n X^n$. The *Newton polygon* of f is defined to be the lower convex hull of the set $\{(i, \mathrm{ord}(a_i)) \in \mathbb{R}^2 \mid 0 \leq i \leq n, a_i \neq 0\}$. Let $\{s_i\}$ be the slopes of it, and let n_i be the multiplicity of s_i, i.e., the horizontal distance (within $[0, n]$) traveled by the segment of slope s_i.

Theorem 1.8.1 (Newton Polygon)**.** *There are precisely n_i roots α of f in $\bar{K}$ (counting multiplicity) such that* $\mathrm{ord}(\alpha) = -s_i$.

Proof. [Neu99, Ch. II, (6.3)]. □

Remark 1.8.2. The proof only uses strong triangle inequality and root-coefficient relations. Thus we can drop the assumption that K is complete if we assume that f splits over K.

The following result is elementary.

Theorem 1.8.3 (Eisenstein criterion)**.** *Let $(K, |\cdot|)$ be a discretely valued field (not necessarily complete). Thus $\mathcal{O}_K$ is a DVR with maximal ideal $\mathfrak{m}_K$. Let $f = X^n + a_{n_1} X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$. If $a_0 \cdots, a_{n-1} \in \mathfrak{m}_K$ and $a_0 \mathcal{O}_K = \mathfrak{m}_K$, then f is irreducible. (Here irreducibility in $\mathcal{O}_K[X]$ or in $K[X]$ are equivalent.)*

Polynomials satisfying the assumption are called *Eisenstein.*

1.9. **Extensions of completely discretely valued fields.** Let L/K be a finite extension of completely discretely valued fields. Let l and k denote the residue fields of L and K. Then l is a finite extension of k. Define the *residue degree*

$$f(L/K) := [l : k].$$

Recall that an element $x \in K$ is called a uniformizer of K if $x \in \mathfrak{m}_K$ and $x\mathcal{O}_K = \mathfrak{m}_K$. Equivalently, $\mathrm{ord}_K(x) = 1$, where ord_K is normalized to be surjective. Define the *ramification index*

$$e(L/K) := \mathrm{ord}_L(x) \in \mathbb{Z}_{\geq 1},$$

where ord_L is normalized to be surjective. Equivalently, if $|\cdot|$ denotes the absolute value on L, we have $e(L : K) = [|L^\times| : |K^\times|]$ where $|L^\times|$ and $|K^\times|$ are subgroups of $\mathbb{R}_{>0}$. Equivalently,

$$\mathfrak{m}_K \mathcal{O}_L = \mathfrak{m}_L^{e(L/K)}.$$

Fact 1.9.1 ([Ser79, II.2])**.** *The $\mathcal{O}_K$-module $\mathcal{O}_L$ is free of rank $[L : K]$. It is the integral closure of $\mathcal{O}_K$ in L. We have $e(L/K)f(L/K) = [L : K]$.*

Definition 1.9.2. The extension L/K is called *unramified*, if $e(L/K) = 1$ and l/k is separable. It is called *totally ramified*, if $e(L/K) = [L : K]$.

Theorem 1.9.3. *Let K be a completely discretely valued field.*

(1) *Every finite unramified extension of K is separable. There is an equivalence of categories from the category of finite unramified extensions of K to the category of finite separable extensions of the residue field k, sending L/K to the residue extension l/k. In other words, every finite separable extension of k can be realized as the residue extension of a (unique up to isomorphism) finite unramified extension of K, and if $L/K, L'/K$ are finite unramified then* $\mathrm{Hom}_K(L, L') \xrightarrow{\sim} \mathrm{Hom}_k(l, l')$.

(2) *Moreover, if L/K is a finite unramified extension with residue field l, and M/K is a finite extension with residue field m, then we have* $\mathrm{Hom}_K(L, M) \xrightarrow{\sim} \mathrm{Hom}_k(l, m)$.

(3) *Let l/k be a finite separable extension, so by the primitive element theorem $l \cong k[X]/(\bar{f}(X))$ for a monic irreducible separable $\bar{f}(X) \in k[X]$. Let $f(X) \in \mathcal{O}_K[X]$ be a monic lift of $\bar{f}$. Then $L = K[X]/(f(X))$ is a finite unramified extension of K whose residue extension is isomorphic to l/k, and we have $\mathcal{O}_L = \mathcal{O}_K[\bar{X}]$.*

(4) *If L/K is finite totally ramified and π_L is a uniformizer of L, then $L = K(\pi_L)$, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, and the monic minimal polynomial of π_L over $\mathcal{O}_K$ is Eisenstein. Conversely, for any Eisenstein polynomial $f(X) \in \mathcal{O}_K[X]$, the extension $L = K[X]/(f(X))$ over K is totally ramified, and $\bar{X}$ is a uniformizer of L.*

Remark 1.9.4. Let L/K be a finite unramified extension, and $\alpha \in \mathcal{O}_L$ be such that its image $\bar{\alpha}$ in l generates l over k. Let $f(X) \in \mathcal{O}_K[X]$ be the monic minimal polynomial of α. Then the image $\bar{f} \in k[X]$ must be divisible by the minimal polynomial of $\bar{\alpha}$ over k, and hence be equal to the latter since $[k(\bar{\alpha}) : k] = [l : k] = [L : K] \geq \deg f$. Then by (3), we have a map between unramified extensions $\phi : K[X]/(f(X)) \to L, \bar{X} \to \alpha$, inducing an isomorphism between the residue fields. By (1), ϕ must itself be an isomorphism. Thus, by (3) again, we conclude that $L = K(\alpha)$ and $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Definition 1.9.5. Let K be a completely discretely valued field. An algebraic extension L/K is called *unramified*, if every finite subextension L'/K is unramified.

If we fix a separable closure K^s of K, then it easily follows from Theorem 1.9.3 that there is a unique maximal unramified subextension K^{ur}/K in K^s. Note that the unique extension of ord_K (normalized) to K^{ur} is still valued in $\mathbb{Z}$ (instead of $\mathbb{Q}$). The residue field of K^{ur} is a separable closure of k. Typically K^{ur} is not finite over K. When it is infinite over K, it is not complete. Its completion is denoted by $\breve{K}$.

Example 1.9.6. Assume that K has positive characteristic. Then a choice of a uniformizer of K corresponds to an isomorphism $k(\!(t)\!) \xrightarrow{\sim} K$, sending t to the uniformizer. Fix such an isomorphism. Then for any finite separable l/k, the corresponding finite unramified extension is $l(\!(t)\!)/k(\!(t)\!)$.

Example 1.9.7. Assume that K has characteristic zero, and perfect residue field k. Let $p = \mathrm{char}(k)$. Let $W(k)$ be the ring of Witt vectors (see [Ser79, II.5]). Then $W(k)$ is a complete DVR containing $\mathbb{Z}$ such that p is a uniformizer and its residue field is k. There is a canonical embedding $W(k) \hookrightarrow \mathcal{O}_K$ lifting the identity map on k, and the resulting $\mathrm{Frac}\, W(k) \hookrightarrow K$ is a finite totally ramified extension of completely discretely valued fields. (Here $\mathrm{Frac}\, W(k)$ is equipped with the unique discrete valuation such that the valuation ring is $W(k)$.) For any finite (automatically separable) extension l/k, the corresponding finite unramified extension L/K is $L = K \otimes_{W(k)} W(l)$.

Example 1.9.8. Let L/K be a finite extension such that the residue extension l/k is separable. Then we have a unique maximal unramified subextension L'/K in L. The residue field of L' is l. We have $[L' : K] = f(L/K)$. A uniformizer of K stays as a uniformizer of L', so $e(L/L') = e(L/K) = [L : K]/f(L/K) = [L : L']$. Hence L/L' is totally ramified. Thus we have "broken down" the extension L/K into an unramified extension L'/K and a totally ramified extension L/L'.

Corollary 1.9.9. *Let L/K be a finite unramified extension, with residue extension l/k. If l/k is Galois, then so is L/K, and we have* $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(l/k)$.

Proof. By the equivalence of categories, the natural map $\mathrm{Aut}(L/K) \to \mathrm{Aut}(l/k)$ is an isomorphism. If l/k is Galois, then these groups have cardinality $[l : k]$, and this is equal to $[L : K]$ since L/K is unramified. □

1.10. **Galois theory for local fields.** Let L/K be a finite Galois extension of non-archimedean local fields. Let l/k be the residue extension, and $G = \mathrm{Gal}(L/K)$. The action of G on L preserves ord_L, so it stabilizes $\mathcal{O}_L$ and $\mathfrak{m}_L^i$ for all $i \geq 1$.

Definition 1.10.1. The ramification subgroups of G are $G_i = \ker(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{i+1}))$, for $i \in \mathbb{Z}, i \geq -1$.

Thus G_i are normal subgroups of G, and we have

$$G = G_{-1} \supset G_0 \supset G_1 \supset \cdots .$$

Clearly $\bigcap_i G_i = 1$. Since G is finite, this implies that $G_m = 1$ for some finite m.

The subgroup $G_0 = \ker(G \to \mathrm{Gal}(l/k))$ is called the *inertia subgroup*. The extension L^{G_0}/K is the maximal unramified extension of K inside L, and it is Galois of Galois group $G/G_0 \cong \mathrm{Gal}(l/k)$. The extension L/L^{G_0} is totally ramified, and it is Galois of Galois group G_0.

The subgroup G_1 is called the *wild inertia*, while G_0/G_1 is called *tame inertia*. In fact, let $p = \mathrm{char}(k)$. Then G_1 is the unique p-Sylow subgroup of G_0. The extension L^{G_1}/L^{G_0} is totally ramified and *tamely ramified* in the sense that its degree is coprime to p. It is the maximal subextension of L/L^{G_0} which is tamely ramified. In general, a finite extension of K is called *tamely ramified* if the ramification index is coprime to p. Thus L^{G_1}/K is the maximal subextension of L/K which is tamely ramified.

Define $U_L = U_L^0 = \mathcal{O}_L^\times$, and $U_L^i = 1 + \mathfrak{m}_L^i$ for $i \geq 1$. These are abelian groups under multiplication.

Choose a uniformizer π_L of L. For $i \geq 0$ we have injective group homomorphisms

$$G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1}, \quad s \mapsto \frac{s(\pi_L)}{\pi_L}.$$

Note that $s(\pi_L) \equiv \pi_L \mod \pi_L^{i+1}$ since $s \in G_i$, and it follows that $s(\pi_L)/\pi_L \equiv 1 \mod \pi_L^i$, i.e., $s(\pi_L)/\pi_L \in U_L^i$.

Exercise 1.10.2. This map is a well-defined group homomorphism, and it is independent of the choice of π_L.

Now to check the injectivity of this map, we need to show that if $s \in G_i$ satisfies that $s\pi_L \equiv \pi_L \mod \pi_L^{i+2}$, then $sx \equiv x \mod \pi_L^{i+2}$ for all $x \in \mathcal{O}_L$. This follows from the fact that $\mathcal{O}_L = \mathcal{O}_{L^{G_0}}[\pi_L]$ as L/L^{G_0} is totally ramified.

For $i = 0$, $U_L/U_L^1 \cong l^\times$ by $x \mapsto (x \mod \mathfrak{m}_L)$. This is a cyclic group of order prime to p. For $i \geq 1$, the multiplicative group U_L^i/U_L^{i+1} is isomorphic to the additive group $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ by $x \mapsto x - 1$, and the latter is isomorphic to l, which is a product of $\mathbb{Z}/p\mathbb{Z}$. We conclude that:

- G_0/G_1 is a cyclic group of order prime to p.
- For $i \geq 1$, G_i/G_{i+1} is a product of $\mathbb{Z}/p\mathbb{Z}$.

This implies that G_1 is the unique p-Sylow subgroup of G_0. Note that $G/G_0 \cong \mathrm{Gal}(l/k)$ is also a cyclic group. Hence G is solvable.

We now introduce the *upper numbering* of ramification groups. For $u \in [-1, +\infty)$, define $G_u := G_{\min\{i \in \mathbb{Z} | i \geq u\}}$. For $u \in [0, +\infty)$, define

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

Also for $u \in [-1, 0)$ define

$$\phi(u) := u.$$

Then ϕ is a strictly increasing, continuous, piecewise linear, concave function on $[-1, +\infty)$. It is thus a bijection $[-1, +\infty) \to [-1, +\infty)$. Let $\psi = \psi_{L/K}$ be its inverse function. Then ψ is strictly increasing, continuous, piecewise linear, convex function on $[-1, +\infty)$.

Definition 1.10.3. The *upper numbering of ramification groups* is defined by

$$G^v := G_{\psi(v)}, \quad v \in [-1, +\infty),$$

i.e.,

$$G^{\phi(u)} := G_u, \quad u \in [-1, +\infty).$$

Now let $H \subset G$ be a normal subgroup, and $K' = L^H$. Then K'/K is a Galois extension of Galois group G/H, so we can define $(G/H)_u$ and $(G/H)^v$ with respect to L/K. Also we can define H_u and H^v with respect to L/L^H. It is clear from the definition that we have

$$H_u = H \cap G_u.$$

The following theorem is the main reason for considering the upper numbering.

Theorem 1.10.4. *For all $v \in [-1, +\infty)$, we have*

$$(G/H)^v = G^v H/H.$$

In the rest of this subsection we give a proof of Theorem 1.10.4. For any $s \in G - \{1\}$, define

$$i_G(s) := \max\{i \in \mathbb{Z} \mid i \geq -1, s \in G_i\} + 1.$$

The following result is the key.

Proposition 1.10.5. *For $\sigma \in G/H, \sigma \neq 1$, we have*

$$i_{G/H}(\sigma) = \frac{1}{e(L/K')} \sum_{s \in G, s \mapsto \sigma} i_G(s).$$

For the proof, we will use the following fact.

Fact 1.10.6 ([Ser79, III.6, Prop. 12], or [Neu99, Ch. II, (10.4)])**.** *For any finite extension E/K, there exists $x \in \mathcal{O}_E$ such that $\mathcal{O}_E = \mathcal{O}_K[x]$.*

Exercise 1.10.7. Suppose $\mathcal{O}_L = \mathcal{O}_K[x]$. Then for $s \in G$ we have

$$i_G(s) = \mathrm{ord}_L(sx - x).$$

Here ord_L is the normalized discrete valuation on L.

Proof of Proposition 1.10.5. (See [Ser79, III.1, Prop. 3].) Find $x \in \mathcal{O}_L$ and $y \in \mathcal{O}_{K'}$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$ and $\mathcal{O}_{K'} = \mathcal{O}_K[y]$, by Fact 1.10.6. Fix $s \in G$ lifting σ. Then the left hand side is equal to

$$\mathrm{ord}_{K'}(sy - y) = \frac{1}{e(L/K')} \mathrm{ord}_L(s(y) - y),$$

while the right hand side is equal to

$$\frac{1}{e(L/K')} \sum_{t \in H} \mathrm{ord}_L(st(x) - x).$$

Hence it suffices to show that the elements

$$a = s(y) - y, \quad b = \prod_{t \in H} (st(x) - x)$$

divide each other in $\mathcal{O}_L$. The minimal polynomial of x over K' is

$$f(X) = \prod_{t \in H} (X - tx) \in \mathcal{O}_{K'}[X].$$

Then $\pm b = (sf)(x)$. Since each coefficient c_i of f lies in $\mathcal{O}_{K'} = \mathcal{O}_K[y]$, we know that each coefficient of $s(f)-f$, namely $s(c_i)-c_i$, is divisible by a in $\mathcal{O}_L$ (e.g., $s(y^n)-y^n = (sy)^n - y^n = a((sy)^{n-1} + (sy)^{n-2}y + \cdots + y^{n-1})$). Hence a divides $(sf)(x) - f(x) = (sf)(x) = \pm b$. Conversely, let $g(X) \in \mathcal{O}_K[X]$ such that $y = g(x)$. Then $g(X) - y \in \mathcal{O}_{K'}[X]$ kills x, so it must be divisible by $f(X)$ in $\mathcal{O}_{K'}[X]$. Thus $\pm b = (sf)(x)$ divides $(s(g-y))(x)$ in $\mathcal{O}_L$. But $s(g) = g$ since $g \in \mathcal{O}_K[X]$. Hence $(s(g-y))(x) = g(x) - s(y) = y - s(y) = -a$. Thus b divides a in $\mathcal{O}_L$. □

We now write the right hand side of the formula in Proposition 1.10.5 in a better form. Let $j_G(\sigma) := \max\{i_G(s) \mid s \in G, s \mapsto \sigma\}$. Pick $s \in G, s \mapsto \sigma$ such that $i_G(s) = j_G(\sigma)$. Then $\sum_{s' \in G, s' \mapsto \sigma} i_G(s') = \sum_{t \in H} i_G(st)$, and it is easy to see (using that the G_i's are subgroups) that for each t we have

$$i_G(st) = \min(i_G(t), j_G(\sigma)).$$

Also note that $i_G(t) = i_H(t)$. Thus by Proposition 1.10.5, we have

$$i_{G/H}(\sigma) = \frac{1}{e(L/K')} \sum_{t \in H} \min(i_H(t), j_G(\sigma)).$$

It is elementary to check that for all $u \in [-1, +\infty]$, we have

$$\frac{1}{e(L/K')} \sum_{t \in H} \min(i_H(t), u) = \phi_{L/K'}(u-1) + 1$$

(e.g., by comparing the derivatives of the two sides). Hence we conclude that

$$i_{G/H}(\sigma) = \phi_{L/K'}(j(\sigma) - 1) + 1.$$

From this, the following result is immediate:

Theorem 1.10.8 (Herbrand's theorem)**.** *Let $u \in [-1, +\infty)$, and $v = \phi_{L/K'}(u)$. Then $G_u H/H = (G/H)_v$.*

Proof. Let $\sigma \in G/H, \sigma \neq 1$. We have $\sigma \in G_u H/H$ if and only if $j(\sigma) - 1 \geq u$, if and only if $\phi_{L/K'}(j(\sigma) - 1) \geq \phi_{L/K'}(u) = v$, if and only if $i_{G/H}(\sigma) - 1 \geq v$, if and only if $\sigma \in (G/H)_v$. □

By Herbrand's theorem, we have

$$\phi_{L/K} = \phi_{K'/K} \circ \phi_{L/K'}.$$

Indeed, it suffices to check that the two sides have the same derivative at arbitrary $u \in [0, +\infty), u \notin \mathbb{Z}$. The derivative of the left hand side is $|G_u|/e(L/K)$, while that of the right hand side is

$$\frac{|(G/H)_v|}{e(K'/K)} \frac{|H_u|}{e(L/K')}, \quad \text{where } v = \phi_{L/K'}(u).$$

That the two derivatives are equal follows from Herbrand's theorem.

Proof of Theorem 1.10.4. By definition, we have $(G/H)^v = (G/H)_x$, where $v = \phi_{K'/K}(x)$. By Herbrand's theorem, $(G/H)_x = G_w H/H$, where $x = \phi_{L/K'}(w)$. Then $v = \phi_{K'/K}(\phi_{L/K'}(w)) = \phi_{L/K}(w)$. □

2. Topological notions

2.1. **Inverse limits of topological spaces.** Recall that a *directed set*, or a *filtered set*, means a set I with a transitive binary relation $\leq$ such that for any $i, j \in I$, there exists $k \in I$ such that $i \leq k, j \leq k$. By an *inverse system* of sets (or groups, or topological spaces, or topological groups, etc.) indexed by $(I, \leq)$, we mean the following data:

- a set (or group, ...) X_i for each $i \in I$;
- for any $i, j \in I$ such that $i \leq j$, a transition map (or group homomorphism, ...) $p_{i,j} : X_j \to X_i$.

The transition maps $p_{i,j}$ should satisfy the following:

(1) For any $i \in I$, the map $p_{i,i} : X_i \to X_i$ is the identity.
(2) If $i \leq j \leq k$ in I, then $p_{ik} = p_{ij} \circ p_{jk}$.

We denote such an inverse system by $(X_i)_{i\in I}$, suppressing $\leq$ and p_{ij} from the notation.

For $(X_i)_{i\in I}$ an inverse system of sets, we define

$$X = \varprojlim_{i\in I} X_i := \{(x_i) \in \prod_i X_i \mid \forall i \leq j, p_{ij}(x_j) = x_i\}.$$

This is equipped with maps $p_i : X \to X_i$, by projection to the i-th coordinate. The set X together with the maps p_i is characterized by the following universal property: If Y is a set and $q_i : Y \to X_i$ are maps for all $i \in I$ which are compatible with the transition maps p_{ij}, then there is a unique map $q : Y \to X$ such that $q_i = p_i \circ q$ for all $i \in I$.

We now consider an inverse system $(X_i)_{i\in I}$ of topological spaces. We define $X = \varprojlim_{i\in I} X_i$ as a subset of $\prod_{i\in I} X_i$ in the same way, and equip it with the subspace topology inherited from the product topology on $\prod_{i\in I} X_i$. The latter is defined as the coarsest topology (i.e., topology with fewest open sets) such that each projection $\prod_{i\in I} X_i \to X_i$ is continuous. Thus every open set in $\prod_i X_i$ is a union of *fundamental open sets*, which are of the form

$$\prod_{i\in I_0} U_i \times \prod_{i\in I-I_0} X_i,$$

where I_0 is a *finite* subset of I, and U_i is an open set in X_i for $i \in I_0$.

The topology on $X = \varprojlim_{i\in I} X_i$ is called the *inverse limit topology.* The topological space X has a similar universal property (for continuous maps between topological spaces) as in the set case.

Exercise 2.1.1. If each X_i is Hausdorff, then so is $X = \varprojlim_{i\in I} X_i$. In this case, X is closed in $\prod_{i\in I} X_i$.

Theorem 2.1.2 (Tychonoff)**.** *If each X_i is compact, then $\prod_{i\in I} X_i$ is compact.*

By the above exercise and theorem, we see that if each X_i is Hausdorff compact, then X is compact.

Exercise 2.1.3. Assume that each X_i is Hausdorff compact non-empty. Then $\varprojlim_{i\in I} X_i \neq \emptyset$. (Hint: use Tychonoff's theorem, and use the characterization of compactness in terms of intersecting closed sets.)

Definition 2.1.4. A topological space X is called *connected*, if it cannot be written as the disjoint union of two open (equivalently, two closed) subsets.

Let X be a topological space. We define a relation $\sim$ on X by: $x \sim y$ if and only if there exists a connected subspace $Y \subset X$ containing both x and y.

Exercise 2.1.5. Show that $\sim$ is an equivalence relation. Moreover, each equivalence class is connected.

The equivalence classes are called *connected components of* X. Thus X is the disjoint union (in the set-theoretical sense) of its connected components, and each connected component is maximal connected.

Definition 2.1.6. A topological space is *totally disconnected*, if each connected component has only one element.

Definition 2.1.7. A topological space is *profinite*, if it is Hausdorff, compact, and totally disconnected.

Theorem 2.1.8. *A topological space is profinite if and only if it is homeomorphic to* $\varprojlim_{i\in I} X_i$ *for an inverse system* $(X_i)_{i\in I}$ *of finite sets, where each* X_i *is equipped with the discrete topology.*

Exercise 2.1.9. Prove the theorem. Hint: For the "only if" direction, you may construct $(I, \leq)$ and $(X_i)_i$ from the given profinite space X in the following way. Let I be the set of continuous maps $f : X \to \mathbb{Z}$ such that $\mathrm{im}(f)$ is finite. For $f, g \in I$, we define $f \leq g$ if there exists a (necessarily unique) map $r_{f,g} : \mathrm{im}(g) \to \mathrm{im}(f)$ such that $f = r_{f,g} \circ g$. For $f \in X$, let $X_f := \mathrm{im}(f)$, and let the transition maps be $r_{f,g}$. (The idea is that I is the "set of all continuous maps from X to finite sets", but we define it in this way to avoid set-theoretical issues.)

2.2. **Topological groups.** A topological group is a group G with a topology such that the multiplication map $G\times G \to G$ and the inversion map $G \to G, g \mapsto g^{-1}$ are both continuous. We write e for the identity element of a group.

Proposition 2.2.1. *Let* G *be a topological group.*

1. *For every open neighborhood* U *of* e*, there exists an open neighborhood* V *of* e *such that* $V^{-1} = V$ *and* $V \cdot V \subset U$.
2. *For every subgroup* H *of* G*, the closure* $\bar{H}$ *of* H *is still a subgroup. If* H *is normal, then* $\bar{H}$ *is normal.*
3. *Every open subgroup is closed. Every closed subgroup of finite index is open.*
4. *If* G *is compact, then every open subgroup is of finite index.*
5. *For* K, K' *compact sets in* G*, we have* $K \cdot K'$ *is compact.*
6. G *is Hausdorff if and only if* $\{e\}$ *is closed.* G *is discrete if and only if* $\{e\}$ *is open.*
7. *For any normal subgroup* H *in* G*, the group* G/H *with the quotient topology is a topological group. It is Hausdorff if and only if* H *is closed in* G*, and it is discrete if and only if* H *is open in* G.

Exercise 2.2.2. Prove the proposition.

If $(G_i)_{i\in I}$ is an inverse system of topological groups, then $G = \varprojlim_{i\in I} G_i$ equipped with the natural group structure and the inverse limit topology is a topological group. The maps $G \to G_i$ are continuous group homomorphisms, and we have a universal property in terms of continuous homomorphisms between topological groups.

Definition 2.2.3. A topological group is called *profinite*, if its underlying topological space is profinite.

Theorem 2.2.4. *A topological group G is profintie if and only if G is topologically isomorphic to $\varprojlim_{i\in I} G_i$ for an inverse system $(G_i)_{i\in I}$ of finite groups (equipped with discrete topology). In this case, the natural map*

$$G \to \varprojlim_{H \trianglelefteq G \text{ open}} G/H$$

is an isomorphism. Here each G/H is finite and discrete, so the inverse limit is an inverse limit of finite groups. (The set of H's is directed by: $H \leq H'$ if and only if $H \supset H'$.)

Exercise 2.2.5. Prove the theorem. Also prove that for a profinite group, the open normal subgroups form a neighborhood basis of e.

Remark 2.2.6. Let G be a profinite group. By a *cofinal system of open normal subgroups* of G, we mean a set S of open normal subgroups of G such that for every open normal subgroup V of G (or equivalently, every open neighborhood V of e), there is $H \in S$ contained in V. Then clearly S is a directed system where $H \leq H'$ if and only if $H \supset H'$. We have a natural map

$$G \to \varprojlim_{H\in S} G/H.$$

The same argument proving the last statement in the theorem also shows that this map is an isomorphism.

Now for an arbitrary topological group G, we define the *profinite completion*

$$\widehat{G} := \varprojlim_{\substack{H \trianglelefteq G \\ \text{open finite index}}} G/H.$$

This is profinite, with the inverse limit topology. We have a natural map $i : G \to \widehat{G}, g \mapsto (g \bmod H)_H$.

Exercise 2.2.7. Show that i is continuous, and that for any continuous homomorphism $f : G \to \Gamma$ where Γ is a profinite group, there exists a unique continuous homomorphism $\hat{f} : \widehat{G} \to \Gamma$ such that $f = \widehat{f} \circ i$. (Hint: for the uniqueness of $\hat{f}$, first show that i has dense image. For the existence of f, you can first treat the case where Γ is finite, and then in general use that Γ is an inverse limit of finite groups.)

Example 2.2.8. The ring of p-adic integers $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n$. Its "usual" topology is the sames as the inverse limit topology, hence profinite.

Example 2.2.9. The profinite completion of $\mathbb{Z}$ is $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. Here the transition maps are $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \bar{a} \mapsto \bar{a}$ for $n|m$.

Exercise 2.2.10. Using Chinese Remainder Theorem, show that there is a canonical isomorphism of topological groups $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, where the product is over all primes p. The natural map $\mathbb{Z} \to \widehat{\mathbb{Z}}$ is identified with the diagonal embedding $\mathbb{Z} \to \prod_p \mathbb{Z}_p, n \mapsto (n)_p$.

2.3. **Profinite groups arising from a local field.** Let K be a non-archimedean local field. Then the additive groups $\mathcal{O}_K \supset \mathfrak{m}_K \supset \mathfrak{m}_K^2 \supset \cdots$ and the multiplicative groups $U_K^0 \supset U_K^1 \supset U_K^2 \supset \cdots$ are all profinite, and $\{\mathfrak{m}_K^n\}_{n\geq i}$ (resp. $\{U_K^n\}_{n\geq i}$) is a cofinal system of open subgroups of $\mathfrak{m}_K^i$ (resp. U_K^i). (Recall that $U_K^0 = \mathcal{O}_K^\times$ and $U_K^i = 1 + \mathfrak{m}_K^i$ for $i \geq 1$.)

Exercise 2.3.1. Prove these claims.

By Remark 2.2.6, we have natural isomorphisms

$$\mathfrak{m}_K^i \xrightarrow{\sim} \varprojlim_{n\geq i} \mathfrak{m}_K^i/\mathfrak{m}_K^n, \quad U_K^i \xrightarrow{\sim} \varprojlim_{n\geq i} U_K^i/U_K^n \tag{2.1}$$

of topological groups.

Lemma 2.3.2. *Let A, B be (abstract) abelian groups, equipped with subgroups $A = A_0 \supset A_1 \supset A_2 \supset \cdots$ and $B = B_0 \supset B_1 \supset B_2 \supset \cdots$. Assume that the natural maps*

$$A \to \varprojlim_{n\geq 1} A/A_n, \quad B \to \varprojlim_{n\geq 1} B/B_n$$

are isomorphisms. Let $\phi : A \to B$ be a homomorphism such that $\phi(A_n) \subset B_n$ for each $n \geq 1$. If ϕ induces a surjection (resp. injection) $A_n/A_{n+1} \to B_n/B_{n+1}$ for each $n \geq 0$, then ϕ is a surjection (resp. injection).

Proof. Exercise. (See [Ser79, §V.1, Lem. 2]) □

These ideas can be applied to proving the following result.

Proposition 2.3.3. *Let L/K be a finite unramified extension, with residue extension l/k. Let N be the norm map $\mathrm{N}_{L/K} : L^\times \to K^\times$. For each $i \geq 0$, we have $N(U_L^i) = U_K^i$.*

Proof. Since l/k is Galois, so is L/K. Let G be the Galois group. We first show that $N(U_L^i) \subset U_K^i$. If $i = 0$, this follows from the fact that ord_L restricts to ord_K. If $i \geq 1$, let $x = 1 + y \in U_L^i$, with $y \in \mathfrak{m}_K^i$. Then

$$N(x) = \prod_{s\in G}(1 + sy) = 1 + \sum_{s\in G} sy + \sum_{s_1,s_2\in G}(s_1y)(s_2y) + \cdots \in 1 + \mathfrak{m}_L^i.$$

But $\mathfrak{m}_L^i \cap K = \mathfrak{m}_K^i$ since L/K is unramified. Hence $N(x) \in 1 + \mathfrak{m}_K^i = U_K^i$.

To finish the proof, by the isomorphisms (2.1) and Lemma 2.3.2, it suffices to check that N induces a surjection $U_L^i/U_L^{i+1} \to U_K^i/U_K^{i+1}$ for each $i \geq 0$. If $i = 0$, we have canonical identifications $U_L^0/U_L^1 \cong l^\times, U_K^0/U_K^1 \cong k^\times$, and the map $l^\times \to k^\times$ is the norm for l/k, which is surjective. Suppose $i \geq 1$. Then after choosing a uniformizer π_L of L we have an isomorphism $l = \mathcal{O}_L/\mathfrak{m}_L \xrightarrow{\sim} U_L^i/U_L^{i+1}$ sending $a + \mathfrak{m}_L$ (for $a \in \mathcal{O}_L$) to $(1 + \pi_L^i a)U_L^{i+1}$. Similarly, after choosing a uniformizer of K we have an isomorphism $k \xrightarrow{\sim} U_K^i/U_K^{i+1}$. Since L/K is unramified, we can choose the same uniformizer of K and L. Then the map $l \to k$ corresponding to $N : U_L^i/U_L^{i+1} \to U_K^i/U_K^{i+1}$ is the trace for l/k (since the "linear term" in the above formula for $N(x)$ is $\sum_{s\in G} sy$), which is surjective. □

2.4. Review of infinite Galois theory.

Recall that an (infinite degree) algebraic extension of fields L/K is called *Galois*, if it is separable (i.e., the minimal polynomial over K of any element of L is separable) and normal (i.e., the minimal polynomial over K of any element of L splits in L). Equivalently, L/K is the splitting field of a set of separable irreducible polynomials over K. Clearly an algebraic extension L/K is Galois if and only if L is the union of the finite Galois subextensions L'/K in L.

Let L/K be Galois, and let $G = \mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$. Let S be the set of finite Galois subextensions L'/K in L. Then S is a directed system with $L' \leq L''$ if and only if $L' \subset L''$. For $L' \leq L''$ in S, we have the restriction map $\mathrm{Gal}(L''/K) \to \mathrm{Gal}(L'/K)$, so we have an inverse system of finite groups $(\mathrm{Gal}(L'/K))_{L'\in S}$. Since $L = \bigcup_{L'\in S} L'$, we have a natural isomorphism (of groups)

$$\mathrm{Gal}(L/K) \cong \varprojlim_{L'\in S} \mathrm{Gal}(L'/K).$$

We equip $\mathrm{Gal}(L/K)$ with the inverse limit topology of the right hand side, which is profinite. This is called the *Krull topology* on $\mathrm{Gal}(L/K)$.

Theorem 2.4.1 (Main Theorem of Galois Theory)**.** *Let L/K be a Galois extension, and let $\mathcal{E}$ be the set of intermediate extensions $L/E/K$.*

(1) *We have a bijection*
$$\{\textit{closed subgroups of } \mathrm{Gal}(L/K)\} \xrightarrow{\sim} \mathcal{E},$$
sending H to L^H. The inverse map sends E to $\mathrm{Gal}(L/E)$.

(2) *Suppose H corresponds to E. Then H is of finite index in* $\mathrm{Gal}(L/K)$ *(i.e., open) if and only if E/K is finite.*

(3) *Suppose H corresponds to E. Then H is normal in* $\mathrm{Gal}(L/K)$ *if and only if E/K is Galois. In this case, we have a natural topological isomorphism* $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/H$*, where the right hand side has the quotient topology.*

Definition 2.4.2. Let G be a topological group. Let G_{der} be the commutator subgroup, i.e., the subgroup generated by $xyx^{-1}y^{-1}$ for $x, y \in G$. Let $\overline{G_{\mathrm{der}}}$ be its closure. Then $\overline{G_{\mathrm{der}}}$ is normal in G, and we define the *abelianization* $G^{\mathrm{ab}} := G/\overline{G_{\mathrm{der}}}$.

Clearly G^{ab} is Hausdorff and abelian, and every continuous homomorphism from G to a Hausdorff abelian topological group factors uniquely through $G \to G^{\mathrm{ab}}$.

Definition 2.4.3. By an *abelian extension*, we mean a Galois extension of fields whose Galois group is abelian.

Let L/K be a Galois extension. If $E_1/K, E_2/K$ are two abelian subextensions, then so is the compositum E_1E_2 (since E_1E_2/K is Galois, and $\mathrm{Gal}(E_1E_2/K) \hookrightarrow \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K)$). Thus inside L/K there is a unique maximal abelian extension E of K. Under the Galois correspondence, $\mathrm{Gal}(L/E) = \overline{\mathrm{Gal}(L/K)_{\mathrm{der}}}$, and $\mathrm{Gal}(E/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}}$.

Fix a separable closure K^s of K. Then the maximal abelian subextension of K in K^s is called an *absolute maximal abelian extension* of K, and we denote it by K^{ab}. We often write G_K for $\mathrm{Gal}(K^s/K)$, called the *absolute Galois group of* K. Then $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong G_K^{\mathrm{ab}}$.

Remark 2.4.4. If $K^s, K^{s\prime}$ are two separable closures of K. Then there exist K-isomorphisms $K^s \xrightarrow{\sim} K^{s\prime}$, and the set of all such isomorphisms is acted on simply transitively by $\mathrm{Gal}(K^s/K)$. If we choose such an isomorphism, then we obtain an isomorphism $\phi : \mathrm{Gal}(K^s/K) \xrightarrow{\sim} \mathrm{Gal}(K^{s\prime}/K)$, and different choices would result in different isomorphisms ϕ which are conjugate to each other. Note that all these isomorphisms $\phi : \mathrm{Gal}(K^s/K) \xrightarrow{\sim} \mathrm{Gal}(K^{s\prime}/K)$ induce the *same* isomorphism between the abelianizations, thus the same isomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}\prime}/K)$. Thus the invariant $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ of K is independent of the choice of K^s up to canonical isomorphism.

2.5. **Infinite decomposition groups.** Let K be a global field, and L/K a Galois extension, possibly of infinite degree. Fix $v \in V_K$, and let $S = \{w \in V_L \mid w|_K = v\}$. Here V_L denotes the set of places of L, and it is defined still as the set of equivalence classes of absolute values on L, despite that L may not be a global field. The group $\mathrm{Gal}(L/K)$ naturally acts on S, and for $w \in S$ we denote the stabilizer of w in $\mathrm{Gal}(L/K)$ by $D(w/v)$ or $D(w/K)$, called *the decomposition group.*

Exercise 2.5.1. $D(w/v)$ is a closed subgroup of $\mathrm{Gal}(L/K)$.

Fix a separable closure M of K_v. We have a map
$$\gamma : \mathrm{Hom}_K(L, M) \to S, \quad \phi \mapsto |\cdot|_v \circ \phi,$$

where $|\cdot|_v$ is the canonical absolute value on M (i.e., the unique one that extends the given one on K_v). Since M is separably closed and contains K, the set $\mathrm{Hom}_K(L, M)$ is non-empty, and is acted on simply transitively by $\mathrm{Gal}(L/K)$. It follows that $S \neq \emptyset$. Moreover, γ is $\mathrm{Gal}(L/K)$-equivariant.

Lemma 2.5.2. *The action of* $\mathrm{Gal}(L/K)$ *on* S *is transitive.*

Proof. Let $u, w \in S$. For each finite Galois extension L'/K in L, let $T_{L'} = \{g \in \mathrm{Gal}(L'/K) \mid g \cdot u|_{L'} = w|_{L'}\}$. Since $\mathrm{Gal}(L'/K)$ acts transitively on the set of places of L' over v, we have $T_{L'} \neq \emptyset$. Clearly $\{g \in \mathrm{Gal}(L/K) \mid gu = w\} \cong \varprojlim_{L'} T_{L'}$. Since this is an inverse limit of non-empty finite (hence compact) sets, this set is non-empty by Exercise 2.1.3. □

Corollary 2.5.3. *The map* γ *is a* $\mathrm{Gal}(L/K)$*-equivariant surjection.*

Now consider the case $L = K^s$, a separable closure of K. Fix $\phi \in \mathrm{Hom}_K(K^s, M)$, and let $w = \gamma(\phi)$, which is a place of K^s over v. We construct a homomorphism

$$h : D(w/v) \to \mathrm{Gal}(M/K_v) = G_{K_v}$$

as follows.

Lemma 2.5.4. *For any finite separable extension* E/K_v*, there exists* $\alpha \in E$ *which is algebraic and separable over* K *such that* $E = K_v(\alpha)$*.*

Proof. By the primitive element theorem, $E = K_v(\beta)$ for some $\beta \in E$. Let $f(X)$ be the minimal polynomial of β over K_v. By Krasner's lemma (see [Ser79, II.2, Exercise 2]), for every polynomial $f_1(X) \in K_v[X]$ whose coefficients are sufficiently close to those of f, f_1 is irreducible and E is generated over K_v by a root of f_1. Since K is dense in K_v, we can take $f_1 \in K[X]$. Thus $E = K_v(\alpha)$ for a root α of f_1. Since $\alpha \in E$, its minimal polynomial over K_v is separable. This polynomial is f_1, and it is also the minimal polynomial of α over K (since it is also irreducible over K). Hence α is separable over K. □

Lemma 2.5.5. *The image of* ϕ *is dense in* M*.*

Proof. Let $y \in M$. Then $K_v(y) = K_v(\alpha)$ for some $\alpha \in M$ which is algebraic and separable over K, by Lemma 2.5.4. Write $y = b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0$. Let $\epsilon > 0$ be arbitrary. Since K is dense in K_v, for each $0 \leq i \leq n$, we can find $c_i \in K$ such that $|c_i\alpha^i - b_i\alpha^i|_v \leq \epsilon$. (If $\alpha^i \neq 0$, choose $|c_i - b_i| \leq \epsilon/|\alpha^i|_v$; if $\alpha^i = 0$, choose any c_i.) Let $y' = c_n\alpha^n + \cdots + c_0$. Then $|y - y'| \leq \epsilon$. Note that α lies in the image of ϕ since the latter is the separable closure of K inside M. Hence y' lies in the image of ϕ. □

Since ϕ has dense image, it induces an isometric isomorphism from the completion $(K^s)_w$ of K^s with respect to w to the completion $\widehat{M}$ of M with respect to the canonical absolute value. For $\sigma \in D(w/v)$, we have a unique extension of σ to an isometric automorphism $\tilde{\sigma}$ of $(K^s)_w$. Using ϕ, we view $\tilde{\sigma}$ as an automorphism of $\widehat{M}$. This restricts to the identity on K_v, so it stabilizes M (as K_v^s is the separable closure of M *inside* $\widehat{M}$). The restriction $\tilde{\sigma}|_M$ is an element of $\mathrm{Gal}(M/K_v)$. We define h by

$$h(\sigma) = \tilde{\sigma}|_M.$$

We claim that h is an isomorphism. Indeed, the inverse is given as follows: Let $\tau \in \mathrm{Gal}(M/K_v)$. Then τ is automatically isometric, and so it extends uniquely to an isometric automorphism $\tilde{\tau}$ of $\widehat{M}$. Using ϕ, we view $\tilde{\tau}$ as an isometric automorphism of $(K^s)_w$. Since $\tilde{\tau}$ is the identity on K, it stabilizes K^s, and moreover $\tilde{\tau}|_{K^s}$ is an element of $D(w/v)$. The inverse of h sends τ to $\tilde{\tau}|_{K^s}$.

Lemma 2.5.6. *The isomorphism* $h : D(w/v) \xrightarrow{\sim} \mathrm{Gal}(M/K_v)$ *is a topological isomorphism.*

Proof. Since both sides are compact Hausdorff (see Exercise 2.5.1), it suffices to show that h is an open map. Since the open normal subgroups U of $\mathrm{Gal}(K^s/K)$ form a neighborhood basis of 1, it suffices to show that $h(D(w/v) \cap U)$ is open for such U. Write $U = \mathrm{Gal}(E/K)$ for a finite Galois extension E/K in K^s. Then $D(w/v) \cap U = D(w/E)$, and it is clear that $h(D(w/v) \cap U) = \mathrm{Gal}(M/E_{v'})$ where $v' = w|_E$. Since $E_{v'}/K_v$ is finite, $\mathrm{Gal}(M/E_{v'})$ is an open subgroup of $\mathrm{Gal}(M/K_v)$ as desired. □

In summary, if we choose any K-embedding ϕ of K^s into the separable closure $M = (K_v)^s$ of K_v, then we obtain via pull-back a place w of K^s, as well as a topological isomorphism $h : D(w/v) \xrightarrow{\sim} \mathrm{Gal}(M/K_v)$. Note that different choices of ϕ inducing the same w differ from each other by elements of $D(w/v)$, and so the resulting isomorphisms $h : D(w/v) \xrightarrow{\sim} \mathrm{Gal}(M/K_v)$ differ from each other by conjugation.

3. Adeles and ideles

3.1. **Restricted product.** Let V be a set, and $(X_v)_{v\in V}$ be a family of topological spaces. For almost all $v \in V$, we fix an open set U_v in X_v. The restricted product of $(X_v)_v$ with respect to $(U_v)_v$ is defined as

$$X = \prod_{v\in V}{}' X_v = \big\{(x_v)_v \in \prod_{v\in V} X_v \mid x_v \in U_v \text{ for almost all } v\big\}.$$

It is equipped with the topology generated by basic open sets of the form

$$\prod_{v\in S} Y_v \times \prod_{v\in V-S} U_v, \tag{3.1}$$

where $S \subset V$ is a finite subset, and for each $v \in S$, Y_v is an open set in X_v. Here are some immediate observations:

(1) If we change the choices of U_v for finitely many v, then the set X and its topology remain unchanged.
(2) If $U_v = X_v$ for almost all v, then $X = \prod_{v\in V} X_v$, and its topology is the usual product topology.
(3) On a basic open set as in (3.1), the subspace topology inherited from X is the same as the product topology coming from Y_v and U_v.

Lemma 3.1.1. *If each X_v is locally compact Hausdorff, and each U_v is compact, then X is locally compact Hausdorff.*

Proof. Any pair of points of X lie in a basic open of the form

$$U = \prod_{v\in S} X_v \times \prod_{v\in V-S} U_v,$$

where $S \subset V$ is finite. Since U has the product topology, it is Hausdorff, and it follows that X is Hausdorff. To show that X is locally compact, let $x \in X$. We need to find a compact set containing an open neighborhood of x in X. We may assume that x lies in U as above. Write $x = (x_v)$. For $v \in S$, since X_v is locally compact, there exists an open neighborhood V_v of x_v and a compact set K_v such that $V_v \subset K_v \subset X_v$. Then

$$\prod_{v\in S} K_v \times \prod_{v\in V-S} U_v$$

is a compact subset of U by Tychonoff. It contains the open neighborhood $\prod_{v\in S} V_v \times \prod_{v\in V-S} U_v$ of x. □

3.2. **Adeles.** Let K be a global field. The *ring of adeles* is defined as the restricted product of K_v over all $v \in V_K$, with respect to the open subsets $\mathcal{O}_{K_v} \subset K_v$ for non-archimedean v:

$$\mathbb{A}_K := \prod_{v\in V_K}{}' K_v.$$

Since each K_v is a topological ring and $\mathcal{O}_{K_v}$ is a subring, $\mathbb{A}_K$ is a topological (commutative) ring. Since each K_v is locally compact Hausdorff, and each $\mathcal{O}_{K_v}$ is compact (for non-archimedean v), $\mathbb{A}_K$ is locally compact Hausdorff.

As a variant, for a finite subset $S \subset V_K$, we define the adeles away from S to be

$$\mathbb{A}_K^S := \prod_{v\in V_K - S}{}' K_v,$$

where the restricted product is again with respect to $\mathcal{O}_{K_v}$ for non-archimedean v not in S. This is also a locally compact Hausdorff topological ring.

For any $x \in K$, we have $x \in \mathcal{O}_{K_v}$ for almost all v. Hence we have a diagonal embedding

$$K \hookrightarrow \mathbb{A}_K^S.$$

Example 3.2.1. As a ring, $\mathbb{A}_\mathbb{Q} \cong \mathbb{R} \times (\widehat{\mathbb{Z}} \otimes_\mathbb{Z} \mathbb{Q})$, and $\mathbb{A}_\mathbb{Q}^\infty \cong (\widehat{\mathbb{Z}} \otimes_\mathbb{Q} \mathbb{R})$. The first isomorphism follows from the second, and we sketch a proof of the second. By Exercise 2.2.10, we identify $\widehat{\mathbb{Z}}$ with $\prod_p \mathbb{Z}_p$. Define the map

$$f : (\prod_p \mathbb{Z}_p) \otimes_\mathbb{Z} \mathbb{Q} \to \mathbb{A}_\mathbb{Q}^\infty = \prod_p{}' \mathbb{Q}_p, \quad (x_p)_p \otimes r \mapsto (x_p r)_p.$$

This is well defined since for any $r \in \mathbb{Q}$, we have $r \in \mathbb{Z}_p$ for almost all primes p. Clearly f is a ring homomorphism, and it is injective since any element of the left hand side can be written as a pure tensor. To show surjectivity, let $(x_p)_p \in \prod_p' \mathbb{Q}_p$. Then there is a finite set S of primes such that for each prime $p \notin S$, $x_p \in \mathbb{Z}_p$. For $p \in S$, choose $e_p \in \mathbb{Z}_{\geq 0}$ such that $p^{e_p} x_p \in \mathbb{Z}_p$. Let $n = \prod_{p\in S} p^{e_p} \in \mathbb{Z}$. Clearly $nx_p \in \mathbb{Z}_p$ for all primes p. Hence $(x_p)_p$ is the image under f of $(nx_p)_p \otimes \frac{1}{n}$.

Now consider a finite extension L/K. Then for each $v \in V_K$, we have the diagonal embedding

$$\iota_v : K_v \hookrightarrow \prod_{w\in V_L, w|v} L_w.$$

Taking the product over all v, we obtain a map $\prod_{v\in V_K} K_v \to \prod_{w\in V_L} L_w$, which clearly restricts to an injective ring map

$$\iota : \mathbb{A}_K \hookrightarrow \mathbb{A}_L.$$

We shall always use this to view $\mathbb{A}_L$ as an $\mathbb{A}_K$-algebra. We now form the tensor product of ι with the diagonal embedding $L \hookrightarrow \mathbb{A}_L$, and get an $\mathbb{A}_K$-algebra map

$$\eta : L \otimes_K \mathbb{A}_K \to \mathbb{A}_L.$$

Proposition 3.2.2. *The map η is an isomorphism. Moreover, if we equip the left hand side with the product topology $L \otimes_K \mathbb{A}_K \cong \mathbb{A}_K^{[L:K]}$ (after choosing a K-basis of L), then η is a homeomorphism.*

Proof. We only give the proof assuming that L/K is separable. For the general case, see [Wei95, §VIII.6].

Let $\alpha_1, \dots, \alpha_n$ be a K-basis of L. Recall from Fact 1.4.3 that the tensor product of $\iota_v : K_v \to \prod_{w|v} L_w$ with the diagonal embedding $L \to \prod_{w|v} L_w$ gives rise to a K_v-algebra isomorphism

$$\eta_v : L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w.$$

We claim that for almost all $v \in V_K$, η_v maps the $\mathcal{O}_{K_v}$-lattice[3] $\mathcal{L}_v = \sum_i \mathcal{O}_{K_v} \cdot (\alpha_i \otimes 1)$ in the left hand side onto the $\mathcal{O}_{K_v}$-lattice $\mathcal{M}_v = \prod_{w|v} \mathcal{O}_{L_w}$ in the right hand side. To see this, let ψ be the K-bilinear form on L given by

$$L \times L \to K, \quad (s,t) \mapsto \mathrm{Tr}_{L/K}(st).$$

Since L/K is separable, ψ is non-degenerate. Write R for $L \otimes_K K_v$. Let ψ_v be the K_v-bilinear form on R obtained from ψ by extension of scalars. Then for $s, t \in R$, $\psi_v(s,t)$ is nothing but the trace of the K_v-linear endomorphism of R given by multiplication by st. This description of ψ_v uses only the ring structure and K_v-vector space structure on R. Hence if we use $\eta_v : R \xrightarrow{\sim} \prod_{w|v} L_w$ (which is a K_v-algebra isomorphism) to carry ψ_v to the right hand side, the resulting K_v-bilinear form on $\prod_{w|v} L_w$ is

$$\big((s_w)_w, (t_w)_w\big) \mapsto \sum_w \mathrm{Tr}_{L_w/K_v}(s_w t_w).$$

In particular, $\mathcal{M}_v$ is integral under this pairing, i.e., the pairing of any two elements of $\mathcal{M}_v$ lies in $\mathcal{O}_{K_v}$. For any $\mathcal{O}_{K_v}$-lattice $\mathcal{N}$ in R, define the dual lattice

$$\mathcal{N}^\vee := \{s \in R \mid \psi_v(s,t) \in \mathcal{O}_{K_v}, \ \forall t \in \mathcal{N}\}.$$

We conclude that $\mathcal{M}'_v := \eta_v^{-1}(\mathcal{M}_v)$ satisfies $\mathcal{M}'_v \subset \mathcal{M}'^\vee_v$.

On the other hand, for almost all v, as long as v is coprime to the discriminant

$$d(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) \in K^\times,$$

the lattice $\mathcal{L}_v$ is self-dual under ψ_v. Also, for almost all v, we have $\alpha_i \in \mathcal{O}_{L_w}$ for each i and each $w|v$. Hence for almost all v we have $\mathcal{L}_v \subset \mathcal{M}'_v \subset \mathcal{M}'^\vee_v \subset \mathcal{L}_v^\vee = \mathcal{L}_v$, and so $\mathcal{L}_v = \mathcal{M}'_v$.

We now prove that η is an isomorphism of $\mathbb{A}_K$-algebras. It suffices to prove that $\alpha_1, \dots \alpha_n \in \mathbb{A}_L$ form an $\mathbb{A}_K$-basis of $\mathbb{A}_L$. Let $x = (x_w)_w \in \mathbb{A}_L$. Then by the isomorphisms η_v, there exist unique $a_i = (a_{i,v})_v \in \prod_{v \in V_K} K_v$ for $1 \le i \le n$ such that $x = \sum_{i=1}^n a_i \alpha_i$. We only need to show that each a_i automatically lies in $\mathbb{A}_K$. For almost all v, the component $(x_w)_{w|v} \in \prod_{w|v} L_w$ lies in $\mathcal{M}_v$, and we have $\eta_v(\mathcal{L}_v) = \mathcal{M}_v$ by the claim. This means that $(x_w)_{w|v}$ must be an $\mathcal{O}_{K_v}$-linear combination of the images of $\alpha_i \in L$ in $\prod_{w|v} L_w$. In other words, $a_{i,v} \in \mathcal{O}_{K_v}$. This proves that $a_i \in \mathbb{A}_K$ as desired.

Note that the product topology on $L \otimes_K \mathbb{A}_K$ is independent of the choice of K-basis of L, since for every $g \in \mathrm{GL}_n(K)$, the map $g : \mathbb{A}_K^n \to \mathbb{A}_K^n$ is a homeomorphism. (This holds more generally for every $g \in \mathrm{GL}_n(\mathbb{A}_K)$, and only uses that $\mathbb{A}_K$ is a topological ring.) To check that η is a homeomorphism, first note that taking finite product commutes with taking restricted product. Thus the topology on $L \otimes_K \mathbb{A}_K$ is identified with the restricted product topology $\prod'_{v \in V_K}(L \otimes_K K_v)$, with respect to the open subsets $\mathcal{L}_v \subset L \otimes_K K_v$. By the claim, we see that η takes this topology to the following topology on $\mathbb{A}_L$: the restricted

[3] An $\mathcal{O}_{K_v}$*-lattice* in a finite dimensional K_v-vector space V is an $\mathcal{O}_{K_v}$-submodule of V containing a K_v-basis.

product topology $\prod'_{v\in V_K}(\prod_{w|v} L_w)$, with respect to the open subsets $\mathcal{M}_v \subset \prod_{w|v} L_w$. This topology clearly agrees with the original topology on $\mathbb{A}_L$. □

Proposition 3.2.3. *The image of $K \hookrightarrow \mathbb{A}_K$ is discrete. The quotient topology on $\mathbb{A}_K/K$ is compact.*

Proof. By Proposition 3.2.2, if K/K' is a finite separable extension of global fields, then to prove the proposition for K it suffices to prove it for K'. Thus we may assume $K = \mathbb{Q}$ or $K = \mathbb{F}_p(t)$ (see Exercise 1.2.1). For $K = \mathbb{Q}$, the set $U = (-1, 1) \times \prod_p \mathbb{Z}_p$ is an open neighborhood of 0 in $\mathbb{A}_\mathbb{Q}$. If $x \in \mathbb{Q} \cap U$, then the condition that $x \in \mathbb{Z}_p$ for all primes p implies that $x \in \mathbb{Z}$, and the condition that $-1 < x < 1$ implies that $x = 0$. This proves that $\mathbb{Q}$ is discrete in $\mathbb{A}_\mathbb{Q}$. To prove that $K = \mathbb{F}_p(t)$ is discrete in $\mathbb{A}_K$, let $U = \prod_{v\in V_K} \mathcal{O}_{K_v}$, which is a neighborhood of 0 in $\mathbb{A}_K$. Then $K \cap U$ consists of $f \in \mathbb{F}_p(t)$ satisfying $\deg f \le 0$, and for every irreducible polynomial $g \in \mathbb{F}_p[t]$, g does not divide the denominator of f, i.e., $\mathrm{ord}_g(f) \ge 0$. (All the discrete valuations on $\mathbb{F}_p(t)$ are given by $-\deg$ and ord_g.) Then f has to be a constant. Hence $K \cap U = \mathbb{F}_p$. Since $\mathbb{A}_K$ is Hausdorff, we can further shrink U to ensure that $K \cap U = \{0\}$.

To show that $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is compact, let $C = [-1/2, 1/2] \times \prod_p \mathbb{Z}_p$. Then C is a compact subset of $\mathbb{A}_\mathbb{Q}$. Let $x = (x_\infty, (x_p)_p) \in \mathbb{A}_\mathbb{Q}$. Let S be a finite set of primes such that for all primes $p \notin S$, we have $x_p \in \mathbb{Z}_p$. For each $p \in S$, there exists $r_p \in \mathbb{Q}$ such that $r_p + x_p \in \mathbb{Z}_p$, since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Moreover, we can arrange that the denominator of r_p is a p-power. This is because every rational number can be written as a sum of a rational number whose denominator is a p-power and another rational number which lies in $\mathbb{Z}_p$. (The proof of this assertion uses the Bézout property of $\mathbb{Z}$: Let $q = \frac{n}{p^a b} \in \mathbb{Q}$, where b is coprime to p. Let $x, y \in \mathbb{Z}$ be such that $xp^a + yb = 1$. Then $\frac{yn}{p^a} + \frac{xn}{b} = q$.) Thus $r_p \in \mathbb{Z}_l$ for every prime $l \neq p$. Let $n \in \mathbb{Z}$ be such that $n + (\sum_{p\in S} r_p) + x_\infty \in [-1/2, 1/2]$. Then the rational number $n + \sum_{p\in S} r_p$ satisfies that $n + \sum_{p\in S} r_p + x \in C$. Hence C surjects onto $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$, which implies that $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is compact.

We now show that $\mathbb{A}_K/K$ is compact for $K = \mathbb{F}_p(t)$. Let $C = \prod_{v\in V_K} \mathcal{O}_{K_v}$, which is compact. Let $x = (x_v) \in \mathbb{A}_K$. Write ∞ for the place corresponding to the discrete valuation $-\deg$. Thus all the other places correspond to discrete valuations ord_g, for g monic irreducible polynomials in $\mathbb{F}_p[t]$. Let S be a finite subset of $V_K - \{\infty\}$ such that for all $v \in V_K - (S \cup \{\infty\})$, we have $x_v \in \mathcal{O}_{K_v}$. For each $v \in S$, let $r_v \in K$ be such that $r_v + x_v \in \mathcal{O}_{K_v}$. Suppose v corresponds to the irreducible polynomial $g \in \mathbb{F}_p[t]$. The same argument as in the case of $\mathbb{Q}$ shows that we can arrange that the denominator of r_v is a power of g. (This uses the Bézout property of $\mathbb{F}_p[t]$, which is a PID.) Then $r_v \in \mathcal{O}_{K_w}$ for every $w \in V_K - \{\infty, v\}$. Let $u \in \mathbb{F}_p[t]$ be such that $u + (\sum_{v\in S} r_v) + x_\infty \in \mathcal{O}_{K_\infty}$. Here, note that $K_\infty = \mathbb{F}(\!(t^{-1})\!)$ and $\mathcal{O}_{K_\infty} = \mathbb{F}[\![t^{-1}]\!]$ (because under the automorphism $K \to K, t \mapsto t^{-1}$, the place ∞ gets sent to the place corresponding to the irreducible polynomial t). Thus every element of K_∞ is the sum of a finite linear combination of negative powers of t^{-1} and an element of $\mathcal{O}_{K_\infty}$. Hence u exists. Then we have $(u + \sum_{v\in S} r_v) + x \in C$, which implies that C surjects onto $\mathbb{A}_K/K$. □

3.3. **Ideles.** Let K be a global field. The group of *ideles* is defined to be the restricted product

$$\mathbb{I}_K := \prod_{v\in V_K}{}' K_v^\times,$$

with respect to the compact open subgroups $\mathcal{O}_{K_v}^\times \subset K_v^\times$ for almost all v. Then $\mathbb{I}_K$ is a Hausdorff locally compact topological group (under multiplication).

We have $K_v^\times \subset K_v$ for each v and $\mathcal{O}_{K_v}^\times \subset \mathcal{O}_{K_v}$ for each non-archimedean v. Hence $\mathbb{I}_K$ is a subset of $\mathbb{A}_K$.

Exercise 3.3.1. The subset $\mathbb{I}_K$ consists precisely of the invertible elements of the ring $\mathbb{A}_K$. The inclusion map $\mathbb{I}_K \hookrightarrow \mathbb{A}_K$ is continuous, but not a homeomorphism onto the image. The map $\mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K, g \mapsto (g, g^{-1})$ is a homeomorphism onto the image.

More generally, if R is a topological ring, then we equip $R^\times$, the group of invertible elements, the subspace topology via $R^\times \hookrightarrow R \times R,\ g \mapsto (g, g^{-1})$. This will be the "standard" topology on $R^\times$, *not* the subspace topology via $R^\times \subset R$. Under this standard topology, $R^\times$ is a topological group. With this comment and the above exercise in mind, we will also denote $\mathbb{I}_K$ by $\mathbb{A}_K^\times$.

Definition 3.3.2. The *idele norm* is the homomorphism

$$\|\cdot\| : \mathbb{I}_K \to \mathbb{R}_{>0}, \quad x = (x_v)_v \mapsto \prod_v \|x_v\|_v.$$

Here $\|\cdot\|_v$ denotes the normalized absolute value at v, and we have $\|x_v\|_v = 1$ for almost all v. The kernel of the idele norm is denoted by $\mathbb{I}_K^1 = (\mathbb{A}_K^\times)^1$, called the group of *unit ideles.*

Exercise 3.3.3. The idele norm is continuous. Hence $\mathbb{I}_K^1$ is a closed subgroup of $\mathbb{I}_K$.

We have a diagonal embedding $K^\times \to \mathbb{I}_K$ (which is a group homomorphism). By the product formula, it factors through $\mathbb{I}_K^1$.

Example 3.3.4. Let $K = \mathbb{Q}$. We have $\mathbb{I}_\mathbb{Q} = \mathbb{R}^\times \times \prod_p' \mathbb{Q}_p^\times$. The idele norm $\|\cdot\| : \mathbb{I}_\mathbb{Q} \to \mathbb{R}_{>0}$ has a canonical section $\mathbb{R}_{>0} \to \mathbb{I}_\mathbb{Q}, x \mapsto (x, 1, 1, \cdots)$. Hence we have a canonical isomorphism

$$\mathbb{I}_\mathbb{Q} \cong \mathbb{R}_{>0} \times \mathbb{I}_\mathbb{Q}^1.$$

Next we study $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$. Let $x = (x_v)_v \in \mathbb{I}_\mathbb{Q}$. Let

$$y = \prod_{p \text{ primes}} p^{\operatorname{ord}_p(x_p)} \in \mathbb{Q}^\times.$$

This is a finite product because $\operatorname{ord}_p(x_p) = 0$ for almost all p. Then

$$1 = \|x\| = \|x_\infty\|_\infty \prod_p p^{-\operatorname{ord}_p(x_p)} = \|x_\infty\|_\infty y^{-1}.$$

Thus $x_\infty = \pm y$ lies in $\mathbb{Q}^\times$. Hence modulo $\mathbb{Q}^\times$ we have $x \equiv (x_\infty/x_\infty, (x_p/x_\infty)_p) = (1, (x_p/x_\infty)_p)$. Also note that for each prime p,

$$x_p/x_\infty = \pm x_p/y = \pm \frac{x_p}{p^{\operatorname{ord}_p(x_p)}} \prod_{q, q \neq p} q^{-\operatorname{ord}_q(x_q)} \in \mathbb{Z}_p^\times.$$

We conclude that the subgroup $\prod_p \mathbb{Z}_p^\times \subset \mathbb{I}_\mathbb{Q}^1$ (with trivial archimedean component) surjects onto $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$. Clearly $(\prod_p \mathbb{Z}_p^\times) \cap \mathbb{Q}^\times = 1$ (intersection inside $\mathbb{I}_\mathbb{Q}$) since every element of $\prod_p \mathbb{Z}_p^\times$ has trivial archimedean component. Thus we have $\prod_p \mathbb{Z}_p^\times \cong \mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$. This is actually an isomorphism of topological groups. In particular, $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$ is compact.

Note that in the above argument, the crucial step was the construction of y, which depends on the surjectivity of

$$\mathbb{Q}^\times \to \bigoplus_p \mathbb{Z}, \quad y \mapsto (\operatorname{ord}_p(y))_p.$$

In general, for a number field K, the map

$$K^\times \to \bigoplus_{v\in V_{K,f}} \mathbb{Z}, \quad y \mapsto (\mathrm{ord}_v(y))_v$$

is not necessarily surjective, but it always has finite cokernel, which is nothing but the class group of K. On the other hand, $\mathbb{I}_K^1/K^\times$ is always compact. We shall see that the finiteness of class group is closely related to the compactness of $\mathbb{I}_K^1/K^\times$.

3.4. **Haar measures on local fields.** Let G be a locally compact Hausdorff topological group. Recall that on any topological space, the class of *Borel measurable sets* or simply *Borel sets* is the σ-algebra generated by open sets. Thus this class is the minimal class of subsets which contains all open sets and is closed under taking complement and taking countable union.

Definition 3.4.1. A *Radon measure* on G is a function $\mu : \{\text{Borel sets in } G\} \to \mathbb{R}_{\geq 0}\cup\{+\infty\}$ satisfying the following conditions:

(1) $\mu(\emptyset) = 0$.
(2) If $(B_n)_{n\in\mathbb{N}}$ is a countable family of mutually disjoint Borel sets, then $\mu(\bigcup_n B_n) = \sum_n \mu(B_n)$.
(3) For any compact (hence closed) set C, we have $\mu(C) < +\infty$.
(4) For any open set U, we have $\mu(U) = \sup\{\mu(C) \mid C \subset U,\ C \text{ is compact}\}$.
(5) For any Borel set B, we have $\mu(B) = \inf\{\mu(U) \mid B \subset U,\ U \text{ is open}\}$.

Definition 3.4.2. A *left Haar measure* on G is a non-zero Radon measure μ satisfying $\mu(gB) = \mu(B)$ for all $g \in G$ and all Borel set B. Similarly, we define right Haar measure.

Theorem 3.4.3. *There exists a left Haar measure. Any two left Haar measures differ by multiplication by a constant in $\mathbb{R}_{>0}$. Similarly for right Haar measures.*

For a systematic discussion of Haar measures, see [Wei40].

If G is abelian, there is no difference between left and right Haar measures, and we simply say “Haar measure”.

Example 3.4.4. On the additive group $\mathbb{R}^n$, a Haar measure is given by the Lebesgue measure (restricted to Borel sets).

Exercise 3.4.5. Let G be a locally compact Hausdorff topological group. Assume that there is an open subgroup of G which is profinite. Such G is called *locally profinite*. For instance, any open subgroup of $(F, +)$ or $(F^\times, \times)$, where F is a non-archimedean local field, is locally profinite.

(1) Show that $1 \in G$ has a basis of neighborhoods consisting of compact open subgroups.
(2) Suppose μ is a Radon measure on G. Show that for any open U we have

$$\mu(U) = \sup\{\mu(U') \mid U' \subset U,\ U' \text{ is compact open}\}.$$

(3) Show that a left Haar measure on G is uniquely determined by its values on compact open subgroups (without using the uniqueness in Theorem 3.4.3).
(4) For such G, prove the uniqueness of left Haar measures up to scaling.

Given a left Haar measure μ on G, we have the corresponding theory of integration. For any non-negative Borel measurable function $f : G \to \mathbb{R}_{\geq 0}$ (where “Borel measurable” means that the inverse image of any Borel set is Borel), the integral

$$\int_G f(x)d\mu(x) := \sup_{n\geq 1, a_1,\dots,a_n\in[0,+\infty)} \sum_{i=1}^n a_i\mu(f^{-1}(a_i)) \in [0, +\infty]$$

is defined. For a general Borel measurable function $f : G \to \mathbb{R}$, we say that f is *integrable*, or L^1, if

$$\int_G |f(x)|d\mu(x) < +\infty.$$

In this case, we define

$$\int_G f(x)d\mu(x) = \int_G f_+(x)d\mu(x) - \int_G f_-(x)d\mu(x) \in \mathbb{R}$$

where $f = f_+ - f_-$ and $f_+, f_- \geq 0$. The fact that μ is left invariant under G is expressed by the following identity:

$$\int_G f(gx)d\mu(x) = \int_G f(x)d\mu(x), \quad \forall g \in G.$$

Formally, we can "change variable of integration" and have

$$\int_G f(x)d\mu(x) = \int_G f(gx)d\mu(gx).$$

So the left invariance can be expressed by the formal rule

$$d\mu(gx) = d\mu(x). \tag{3.2}$$

Now let F be a local field. Fix a Haar measure μ on $(F, +)$. For any $x \in F^\times$, multiplication by x is a topological automorphism of $(F, +)$, so we can pull back μ along this automorphism to obtain a new Haar measure, which must differ from μ by a multiplicative constant $s(x) \in \mathbb{R}_{>0}$. Concretely, we have

$$\mu(xB) = s(x)\mu(B)$$

for any Borel set B. Clearly $s(x)$ is independent of the choice of μ since another choice differs just by scaling.

Lemma 3.4.6. *For any $x \in F$, $s(x) = \|x\|$, where $\|\cdot\|$ is the normalized absolute value.*

Proof. If $F = \mathbb{R}$ or $\mathbb{C}$, take B to be the closed unit disk centered at 0 in F. We may assume that μ is the Lebesgue measure. Then $\mu(B) = 2$ or π for $F = \mathbb{R}$ or $\mathbb{C}$. Note that xB is the closed disk of radius $|x|$ centered at 0, where $|\cdot|$ is the usual real or complex absolute value. So $\mu(xB) = 2|x|$ or $\pi|x|^2$ for $F = \mathbb{R}$ or $\mathbb{C}$, and it follows that $s(x) = |x|$ or $|x|^2$ respectively.

Now assume that F is non-archimedean. Note that both $s(\cdot)$ and $\|\cdot\|$ are homomorphisms $F^\times \to \mathbb{R}_{>0}$. Since the group $F^\times$ is generated by all uniformizers in F, it suffices to show that for any uniformizer π we have $s(\pi) = q^{-1}$ where $q = |\mathcal{O}_F/\mathfrak{m}_F|$. Since $\mathcal{O}_F$ is compact, its volume is finite. If $\mu(\mathcal{O}_F) = 0$, then we have $\mu(\pi^n\mathcal{O}_F) = s(\pi^n)\mu(\mathcal{O}_F) = 0$ for all $n \in \mathbb{Z}$, and it follows that $\mu(F) = 0$ since F is an increasing union of the open sets $\pi^n\mathcal{O}_F$. This contradicts with μ being non-zero. Hence $\mu(\mathcal{O}_F) \in (0, \infty)$. Now $\mathcal{O}_F$ is the disjoint union of q cosets $x_i + \pi\mathcal{O}_F$, and each coset has volume equal to that of $\pi\mathcal{O}_F$ since μ is invariant. Hence $\mu(\mathcal{O}_F) = q\mu(\pi\mathcal{O}_F)$, from which $s(\pi) = q^{-1}$. □

The lemma can be expressed by the following identity:

$$\int_F f(g^{-1}x)d\mu(x) = \|g\| \int_F f(x)d\mu(x), \quad \forall g \in F^\times. \tag{3.3}$$

Again, we can compare the above with the formal change of variable:

$$\int_F f(g^{-1}x)d\mu(x) = \int_F f(x)d\mu(gx).$$

Thus we have the formal rule

$$d\mu(gx) = \|g\| d\mu(x).$$

Note that this does not contradict with (3.2) as here μ is Haar measure with respect to the *additive* group.

Corollary 3.4.7. *Let μ be a Haar measure on $(F, +)$. Then a Haar measure $\mu^\times$ on $(F^\times, \times)$ is given by*

$$\mu^\times(B) = \int_F 1_B(x)\|x\|^{-1} d\mu(x).$$

for any Borel set B in $F^\times$. For any integrable function f on $F^\times$ (with respect to $\mu^\times$), the function $f(x)\|x\|^{-1}$ is integrable on F (with respect to μ), and we have

$$\int_{F^\times} f(x) d\mu^\times(x) = \int_F f(x)\|x\|^{-1} d\mu(x).$$

Proof. The second assertion is a formal consequence of the first. For the proof of the first assertion, we admit that the formula defining $\mu^\times$ gives a Radon measure. We only check that it is invariant under multiplication by $F^\times$. Let $g \in F^\times$. Then

$$\mu^\times(gB) = \int_F 1_{gB}(x)\|x\|^{-1} d\mu(x) = \|g\| \int_F 1_{gB}(gx)\|gx\|^{-1} d\mu(x)$$
$$= \int_F 1_B(x)\|x\|^{-1} d\mu(x) = \mu^\times(B),$$

where the second equality uses (3.3). □

Remark 3.4.8. The corollary can be expressed by the formal rule

$$d\mu^\times(x) = \|x\|^{-1} d\mu(x).$$

3.5. **Haar measures on adeles and related spaces.** Now let K be a global field. For each $v \in V_K$, fix a Haar measure μ_v on K_v. We assume that for almost all non-archimedean v, μ_v is normalized such that $\mu_v(\mathcal{O}_{K_v}) = 1$. (In the proof of Lemma 3.4.6 we saw that $\mu_v(\mathcal{O}_{K_v}) \in (0, +\infty)$.) Let $\mu_v^\times$ be the Haar measure on $K_v^\times$ normalized by $\mu_v^\times(\mathcal{O}_{K_v}^\times) = 1$. Note that $\mu_v^\times$ differs by a normalization factor from the one induced by μ_v as in Corollary 3.4.7, since the latter would give volume $1 - |k_v|^{-1}$ to $\mathcal{O}_{K_v}^\times$ (because $[\mathcal{O}_{K_v} : \mathfrak{m}_{K_v}] = |k_v|$ and $\mathcal{O}_{K_v}^\times = \mathcal{O}_{K_v} - \mathfrak{m}_{K_v}$).

Proposition 3.5.1. *There is a unique Haar measure μ on $(\mathbb{A}_K, +)$ satisfying the following condition. For any finite set $S \subset V_K$ containing $V_{K,\infty}$, and for any family of compact sets $(C_v \subset K_v)_{v \in S}$, we have*

$$\mu(\prod_{v\in S} C_v \times \prod_{v\notin S} \mathcal{O}_{K_v}) = \prod_{v\in S} \mu_v(C_v) \times \prod_{v\notin S} \mu_v(\mathcal{O}_{K_v}).$$

Similarly, there is a unique Haar measure $\mu^\times$ on $(\mathbb{A}_K^\times, \times)$ satisfying the following condition. For any finite set $S \subset V_K$ containing $V_{K,\infty}$, and for any family of compact sets $(C_v \subset K_v^\times)_{v\in S}$, we have

$$\mu^\times(\prod_{v\in S} C_v \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times) = \prod_{v\in S} \mu_v^\times(C_v) \times \prod_{v\notin S} \mu_v^\times(\mathcal{O}_{K_v}^\times).$$

For any Borel set $B \subset \mathbb{A}_K$ and any $g \in \mathbb{A}_K^\times$, we have

$$\mu(gB) = \|g\|\mu(B),$$

where $\|\cdot\|$ is the idele norm.

Proof. The first two assertions follow from the general theory of obtaining a Haar measure on a restricted product from Haar measures on the factors. For the third assertion, we know that there is a constant $s(g)$ such that $\mu(gB) = s(g)\mu(B)$, so in order to show $s(g) = \|g\|$ we may take $B = \prod_{v\in S} C_v \times \prod_{v\notin S} \mathcal{O}_{K_v}$ as in the first part. We may also assume that S is sufficiently large such that $g_v \in \mathcal{O}_{K_v}^\times$ for all $v \notin S$, and assume that $\mu_v(C_v) \neq 0$ for all $v \in S$. Then by the first part and by Lemma 3.4.6, we have

$$\begin{aligned} s(g)\mu(B) = \mu(gB) = \mu(\prod_{v\in S} g_v C_v \times \prod_{v\notin S} \mathcal{O}_{K_v}) = \prod_{v\in S} \mu_v(g_v C_v) \times \prod_{v\notin S} \mu_v(\mathcal{O}_{K_v}) \\ = \prod_{v\in S} \|g_v\|_v \times \prod_{v\in S} \mu_v(C_v) \times \prod_{v\notin S} \mu_v(\mathcal{O}_{K_v}) = \|g\|\mu(B) \neq 0. \end{aligned}$$

Hence $s(g) = \|g\|$. □

Remark 3.5.2. By a *factorizable integrable function* on $\mathbb{A}_K$, we mean a function $f : \mathbb{A}_K \to \mathbb{R}$ of the form $f(x) = \prod_v f_v(x_v)$, where f_v is an integrable function $K_v \to \mathbb{R}$ and for almost all v we have $f_v = 1_{\mathcal{O}_{K_v}}$. (Thus the product $\prod_v f_v(x_v)$ is always a finite product.) We write $f = \bigotimes_v f_v$. For such a function, generalizing the first assertion in Proposition 3.5.1 we have

$$\int_{\mathbb{A}_K} f(x)d\mu(x) = \prod_v \int_{K_v} f_v(x_v)d\mu_v(x_v).$$

Note that for almost all v, the factor is $\int_{K_v} f_v(x_v)d\mu_v(x_v) = \mu_v(\mathcal{O}_{K_v}) = 1$, so the product is finite. There is a similar discussion for factorizable integrable functions on $\mathbb{A}_K^\times$ and their integrals.

Recall that the diagonally embedded K in $\mathbb{A}_K$ is a discrete subgroup, and $\mathbb{A}_K/K$ is compact. Since every discrete subgroup is closed, $\mathbb{A}_K/K$ is also Hausdorff. Hence $\mathbb{A}_K/K$ also has Haar measures. We now describe how they are related to Haar measures on $\mathbb{A}_K$. Write π for the projection $\mathbb{A}_K \to \mathbb{A}_K/K$. For any continuous compactly supported function $f : \mathbb{A}_K \to \mathbb{R}_{\geq 0}$, define

$$\pi_!(f) : \mathbb{A}_K/K \to \mathbb{R}_{\geq 0}, \quad x + K \mapsto \sum_{y\in x+K} f(y).$$

The sum is finite since the compact support of f intersects with the discrete set $x + K$ at only finitely many points. Abstractly, this function is the result of integrating f along fibers of π, where we equip each fiber with the counting measure.

Exercise 3.5.3. The function $\pi_!(f)$ is continuous.

Proposition 3.5.4. *We can choose a Haar measure μ on $\mathbb{A}_K$ and a Haar measure $\bar{\mu}$ on $\mathbb{A}_K/K$ such that for any continuous compactly supported function $f : \mathbb{A}_K \to \mathbb{R}_{\geq 0}$, we have*

$$\int_{\mathbb{A}_K} f(x)d\mu(x) = \int_{\mathbb{A}_K/K} (\pi_! f)(x)d\bar{\mu}(x).$$

When this holds, we say that $\bar{\mu}$ is induced by μ.

Proof. This is a consequence of the general theory of quotient Haar measures on homogeneous spaces. □

The following corollary is the main motivation for us to consider the Haar integration theory.

Corollary 3.5.5. *Let μ be a Haar measure on $\mathbb{A}_K$ and let $\bar{\mu}$ be the induced Haar measure on $\mathbb{A}_K/K$. Let $S \subset V_K$ be a finite subset, and for each $v \in S$ let C_v be a closed disk in K_v (of some radius). Let $C = \prod_{v\in S} C_v \times \prod_{v\notin S} \mathcal{O}_{K_v} \subset \mathbb{A}_K$. If $\mu(C) > \bar{\mu}(\mathbb{A}_K/K)$, then the projection $C \to \mathbb{A}_K/K$ is not injective. (Since $\mathbb{A}_K/K$ is compact, $\bar{\mu}(\mathbb{A}_K/K) \in (0, +\infty)$)*

Proof. By Proposition 3.5.1, $\mu(C)$ is finite. (This also follows directly from the compactness of C.) We may assume that μ is related to local Haar measures μ_v on K_v as in that proposition. Let

$$\lambda = \mu(C)/\bar{\mu}(\mathbb{A}_K/K) > 1.$$

For each $v \in S$, find a continuous function $f_v : K_v \to [0,1]$ supported inside C_v that is "sufficiently close" to the indicator function of C_v in the sense that

$$\int_{K_v} f_v(z) d\mu_v(z) > \frac{\mu_v(C_v)}{\lambda^{\frac{1}{\#S}}}.$$

(For v archimedean, take f_v to be a "bump function"; for v non-archimedean, take f_v to be the indicator function of C_v itself, which is continuous.) Let

$$f = \bigotimes_{v\in S} f_v \otimes \bigotimes_{v\notin S} 1_{\mathcal{O}_{K_v}}$$

as in Remark 3.5.2. Then as in that remark, we have

$$\begin{aligned}&\int_{\mathbb{A}_K} f(x) d\mu(x)\\ &\qquad = \prod_{v\in S} \int_{K_v} f_v(z) d\mu_v(z) \times \prod_{v\notin S} \mu_v(\mathcal{O}_{K_v}) > \frac{\prod_{v\in S} \mu_v(C_v) \times \prod_{v\notin S} \mu_v(\mathcal{O}_{K_v})}{\lambda}.\end{aligned}$$

By Proposition 3.5.1, the last term is $\mu(C)/\lambda = \bar{\mu}(\mathbb{A}_K/K)$. On the other hand, f is continuous, compactly supported, and takes values in $[0,1]$. If $C \to \mathbb{A}_K/K$ is injective then $\pi_! f$ as in Proposition 3.5.4 takes values in $[0,1]$, and by that proposition we have

$$\int_{\mathbb{A}_K} f(x) d\mu(x) = \int_{\mathbb{A}_K/K} (\pi_! f)(x) d\bar{\mu}(x) \leq \bar{\mu}(\mathbb{A}_K/K),$$

a contradiction. □

3.6. **The adelic Minkowski theorem.** Recall that the classical Minkowski lemma asserts that for any complete lattice Λ in a Euclidean space $\mathbb{R}^n$ (i.e., Λ is a $\mathbb{Z}$-submodule generated by an $\mathbb{R}$-basis) and any compact, convex, centrally symmetric (i.e. $x \in S$ iff $-x \in S$) subset $S \subset \mathbb{R}^n$, we have

$$\mathrm{vol}(S) \geq 2^n \,\mathrm{vol}(\Lambda) \Rightarrow S \cap \Lambda \supsetneq \{0\}.$$

Here $\mathrm{vol}(\Lambda)$ denotes the volume of $\mathbb{R}^n/\Lambda$, or equivalently the volume of a fundamental parallelepiped for Λ, or equivalently $|\det g|$ for $g \in \mathrm{GL}_n(\mathbb{R})$ such that $g(\mathbb{Z}^n) = \Lambda$. In classical applications, one typically starts with a number field K with r_1 real embeddings and r_2 pairs of complex conjugate complex embeddings. In each of the r_2 pairs choose a complex embedding. Then one obtains a diagonal embedding $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2}$. For any ideal $\mathfrak{a}$ in $\mathcal{O}_K$, its image in $\mathbb{R}^{r_1+2r_2}$ is a lattice, and one would apply Minkowski's lemma to this situation in order to prove finiteness results, e.g., finiteness of the class group.

We shall develop an adelic analogue of the Minkowski theory, and this will be used in the proof of some fundamental theorems about adeles and ideles. From the latter we can eventually deduce the classical finiteness results concerning class groups and the groups of units.

The main point of adelic Minkowski theory is that the embedding $\mathfrak{a} \subset K \hookrightarrow \mathbb{R}^{r_1+2r_2}$ is replaced by the embedding $K \hookrightarrow \mathbb{A}_K$. Thus we need a criterion for certain subsets $S \subset \mathbb{A}_K$ of "nice shape" to satisfy $S \cap K \supsetneq \{0\}$. We first define these subsets of nice shape. In the following, let K be a global field.

Definition 3.6.1. For each $x = (x_v)_v \in \mathbb{A}_K^\times$, define $S_x = \{y \in \mathbb{A}_K \mid \forall v, \|y_v\|_v \leq \|x_v\|_v\}$.

Of course S_x depends on x only via the numbers $\|x_v\|_v$, and almost all of these numbers are equal to 1. Also, observe that S_x is of the form

$$\prod_{v \in S} C_v \times \prod_{v \notin S} \mathcal{O}_{K_v},$$

where S is a finite subset of V_K containing $V_{K,\infty}$, and each C_v is a closed disk in K_v centered at 0, which is compact. Since the subset $\prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_{K_v} \subset \mathbb{A}_K$ has the product topology, we see that S_x is compact by Tychonoff.

Theorem 3.6.2 (Adelic Minkowski)**.** *There is a constant $c = c_K > 0$ depending only on K such that for any $x \in \mathbb{A}_K^\times$, if $\|x\| > c$ (where $\|\cdot\|$ is the idele norm), then $S_x \cap K \supsetneq \{0\}$.*

Proof. Let μ be a Haar measure on $\mathbb{A}_K$, and let $\bar{\mu}$ be the induced Haar measure on $\mathbb{A}_K/K$. Since $\mathbb{A}_K/K$ is compact, $\bar{\mu}(\mathbb{A}_K/K) \in (0, +\infty)$. Let

$$Z = \{z \in \mathbb{A}_K \mid \forall v \in V_{K,\infty}, |z_v|_v \leq \frac{1}{2};\ \forall v \in V_{K,f}, \|z_v\|_v \leq 1\}.$$

Here $|\cdot|_v$ denotes the *usual* absolute value on $K_v = \mathbb{R}$ or $\mathbb{C}$, not the normalized one. By the first part of Proposition 3.5.1, we have $\mu(Z) \in (0, +\infty)$. Let

$$c = c_K = \bar{\mu}(\mathbb{A}_K/K)/\mu(Z).$$

We now show that for any $x \in \mathbb{A}_K^\times$ such that $\|x\| > c$, we have $S_x \cap K \supsetneq \{0\}$.

By the last assertion in Proposition 3.5.1, we have $\mu(xZ) = \|x\|\mu(Z) > \bar{\mu}(\mathbb{A}_K/K)$. We then apply Corollary 3.5.5 to the set xZ to conclude that the projection $xZ \to \mathbb{A}_K/K$ is not injective. Hence there exist unequal $y, y' \in xZ$ such that $a = y - y' \in K^\times$. Write $y = xz, y' = xz'$ for $z, z' \in Z$. For every $v \in V_K$, note that $\|z_v - z'_v\|_v \leq 1$ since $z, z' \in Z$. Hence $\|a\|_v = \|x_v(z_v - z'_v)\|_v \leq \|x_v\|_v$, and $a \in K^\times \cap S_x$. □

Exercise 3.6.3. Show that $c_{\mathbb{Q}} = 1$ and $c_{\mathbb{F}_p(t)} = 1/p$.

Exercise 3.6.4. For K a number field, express c_K in terms of the discriminant of K and the numbers of real and complex places of K. Hint: For $\mathbb{Q}$, take the Haar measure $\mu_{\mathbb{Q}}$ on $\mathbb{A}_{\mathbb{Q}}$ coming from the Lebesgue measure on $\mathbb{R}$ and the Haar measures μ_p on $\mathbb{Q}_p$ normalized by $\mu_p(\mathbb{Z}_p) = 1$. Then $\bar{\mu}(\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}) = 1$. Use a $\mathbb{Z}$-basis for $\mathcal{O}_K$ to identify $\mathbb{A}_K \cong \mathbb{A}_{\mathbb{Q}}^d$ and $K \cong \mathbb{Q}^d$. If we equip $\mathbb{A}_K \cong \mathbb{A}_{\mathbb{Q}}^d$ with the product Haar measure $\mu_{\mathbb{Q}}^{\otimes d}$ coming from $\mu_{\mathbb{Q}}$, then $\bar{\mu}(\mathbb{A}_K/K) = 1$. It remains to compute the volume of $Z \subset \mathbb{A}_K$ under this Haar measure. For this, study how this Haar measure comes from local Haar measures μ_v on K_v for each v. Show that for each prime p, the local isomorphism $\prod_{v|p} K_v \cong \mathbb{Q}_p^d$ takes $\prod_{v|p} \mathcal{O}_{K_v}$ to $\mathbb{Z}_p^d$. Thus the product Haar measure on $\mathbb{Q}_p^d$ coming from μ_p on $\mathbb{Q}_p$ is compatible with the product Haar measure on $\prod_{v|p} K_v$ coming from μ_v on K_v normalized by $\mu_v(\mathcal{O}_{K_v}) = 1$. It only remains to compare Haar measures on the two sides of $\prod_{v|\infty} K_v \cong \mathbb{R}^d$.

3.7. **Two fundamental theorems.** Let K be a global field.

Theorem 3.7.1 (Strong approximation). *Let $v_0 \in V_K$, and define $\mathbb{A}_K^{v_0} = \prod'_{v \in V_K - \{v_0\}} K_v$, where the restricted product is with respect to $\mathcal{O}_{K_v} \subset K_v$ for all non-archimedean $v \neq v_0$. Then the image of the diagonal embedding $K \hookrightarrow \mathbb{A}_K^{v_0}$ is dense. Equivalently, for any $x \in \mathbb{A}_K^{v_0}$, any finite subset $S \subset V_K - \{v_0\}$, and any $\epsilon > 0$, there exists $y \in K$ such that $\|y - x_v\|_v \leq 1$ for all $v \neq v_0$ and $\|y - x_v\|_v < \epsilon$ for all $v \in S$.*

Proof. The two forms are equivalent by considering a suitable neighborhood basis of x in $\mathbb{A}_K^{v_0}$. We prove the second form. We may enlarge S such that $S \cup \{v_0\}$ contains all archimedean places and such that for all $v \in V_K - (S \cup \{v_0\})$, we have $\|x_v\|_v \leq 1$. We may also assume that $\epsilon < 1$. Then we need to find $y \in K$ such that $\|y - x_v\|_v < \epsilon$ for all $v \in S$ and $\|y\|_v \leq 1$ for all $v \in V_K - (S \cup \{v_0\})$.

For each $w \in \mathbb{A}_K^\times$, let

$$S_w^0 = \{z \in \mathbb{A}_K \mid \forall v \in V_{K,\infty}, \|z_v\|_v < \|x_v\|_v;\ \forall v \in V_{K,f}, \|z_v\|_v \leq \|x_v\|_v\}.$$

Then S_w^0 is open in $\mathbb{A}_K$ and is contained in S_w. Clearly $\mathbb{A}_K$ can be written as an increasing union of sets of the form S_w^0. Since $\mathbb{A}_K/K$ is compact, there exists $w \in \mathbb{A}_K^\times$ such that S_w maps surjectively onto $\mathbb{A}_K/K$. We fix such a w.

Let c be the constant as in Theorem 3.6.2. We shall choose a $w' \in \mathbb{A}_K^\times$ such that $\|w'\| > c$. Then there exists $u \in K^\times \cap S_{w'}$. Consider $xu^{-1} \in \mathbb{A}_K$. Here $u^{-1} \in \mathbb{A}_K$ since $u \in K^\times$. By the definition of w, there exist $\alpha \in K$ and $\beta \in S_w$ such that $xu^{-1} = \alpha + \beta$, and so $x = \alpha u + \beta u$ with $\alpha u \in K$. We would like to conclude that αu is the desired y. Thus we need to ensure that

$$\|\beta_v u_v\|_v \begin{cases} < \epsilon, & v \in S, \\ \leq 1, & v \notin S \cup \{v_0\}. \end{cases}$$

Since $\beta \in S_w$ and $u \in S_{w'}$, the above can be ensured if we choose w' to satisfy:

$$\|w'_v w_v\|_v \begin{cases} < \epsilon, & v \in S, \\ \leq 1, & v \notin S \cup \{v_0\}. \end{cases}$$

Since $w \in \mathbb{A}_K^\times$, the above inequalities can be achieved if we choose $\|w'_v\|_v$ to be small for finitely many $v \neq v_0$, and to be 1 for all the remaining $v \neq v_0$. Finally we can choose $\|w'_{v_0}\|_{v_0}$ to be sufficiently large to arrange that w' is an element of $\mathbb{A}_K^\times$ satisfying $\|w'\| > c$. □

Recall that the diagonal embedding $K^\times \hookrightarrow \mathbb{A}_K^\times$ factors through the unit ideles $(\mathbb{A}_K^\times)^1$ by the product formula. Since the inclusion map $\mathbb{A}_K^\times \to \mathbb{A}_K$ is continuous (although not a homeomorphism onto the image) and the image of K in $\mathbb{A}_K$ is already discrete, the image of $K^\times$ in $(\mathbb{A}_K^\times)^1$ is discrete.

Theorem 3.7.2. *The group $(\mathbb{A}_K^\times)^1/K^\times$ is compact.*

The case for $\mathbb{Q}$ was already discussed in Example 3.3.4. For the proof we first need a technical lemma.

Lemma 3.7.3. *The following statements hold.*

1. *The subset $(\mathbb{A}_K^\times)^1 \subset \mathbb{A}_K$ is closed.*
2. *The natural topology on $(\mathbb{A}_K^\times)^1$ (i.e., subspace topology inherited from $\mathbb{A}_K^\times$) agrees with the subspace topology inherited from $\mathbb{A}_K$.*

Proof. The proofs of both parts are based on the following observation: For a non-archimedean place v, the normalized absolute value $\|\cdot\|_v : K_v \to \mathbb{R}$ takes values in $|k_v|^{\mathbb{Z}} \cup \{0\}$. Hence any $x \in K_v$ satisfying $\|x\|_v < 1$ actually satisfies $\|x\|_v \leq 1/|k_v|$. Apart from finitely many v, the cardinality $|k_v|$ is very large, and so the upper bound $1/|k_v|$ is significantly smaller than 1.

(1) Let $x \in \mathbb{A}_K - (\mathbb{A}_K^\times)^1$. We need to find an open neighborhood of x in $\mathbb{A}_K$ disjoint from $(\mathbb{A}_K^\times)^1$.

Case 1: $x \notin \mathbb{A}_K^\times$. Then there are infinitely many places v such that $\|x_v\|_v < 1$. Note that for any non-archimedean v, $\|x_v\|_v < 1$ is equivalent to $\|x_v\|_v \leq 1/2$. Hence there exists a finite subset $S \subset V_K$ such that $\|x_v\|_v \leq 1$ for all $v \notin S$, and $\prod_{v\in S} \|x_v\|_v < 1$. Indeed, let $S_0 = \{v \mid \|x_v\|_v > 1\}$, which is finite. Let $n \in \mathbb{Z}_{\geq 1}$ be such that $\prod_{v \in S_0} \|x_v\|_v < 2^n$, and find $v_1, \ldots, v_n$ such that $\|x_{v_i}\|_{v_i} \leq 1/2$ for all $1 \leq i \leq n$. Then let $S = S_0 \cup \{v_1, \ldots, v_n\}$.

Given S, we pick a neighborhood U_v of x_v in K_v for each $v \in S$ such that for all $(y_v)_{v\in S} \in \prod_{v \in S} U_v$, we have $\prod_{v\in S} \|y_v\|_v < 1$. Then $\prod_{v\in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v}$ is the desired neighborhood of x.

Case 2: $x \in \mathbb{A}_K^\times$ and $\|x\| < 1$. In this case, there exists a finite set S with the same property as in case 1, and the rest of the proof is the same.

Case 3: $x \in \mathbb{A}_K^\times$ and $\|x\| > 1$. Write $P = \|x\|$. Let S be a finite subset of V_K containing $V_{K,\infty}$ such that for all $v \notin S$ we have $\|x_v\|_v = 1$. We now enlarge S such that for all $v \notin S$, $|k_v| > 2P$. Indeed, if K is a number field, then we can enlarge S such that for all $v \notin S$, v divides a rational prime $p > 2P$. Then $k_v \supset \mathbb{F}_p$. If K is a function field, say a finite extension of $\mathbb{F}_p(t)$, then we can enlarge S such that for all $v \notin S$, v divides a place of $\mathbb{F}_p(t)$ corresponding to a monic irreducible polynomial g in $\mathbb{F}_p[t]$ whose degree d satisfies $p^d > 2P$ (as there are only finitely many polynomials of bounded degree). Then $k_v \supset \mathbb{F}_p[t]/(g)$ whose cardinality is p^d.

Now we have $\prod_{v\in S} \|x_v\|_v = P > 1$. For each $v \in S$, pick a neighborhood U_v of x_v in K_v such that for all $(y_v)_{v\in S} \in \prod_{v\in S} U_v$, we have $\prod_{v\in S} \|y_v\|_v \in (1, 2P)$. We now show that the neighborhood $\prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_{K_v}$ of x in $\mathbb{A}_K$ is disjoint from $(\mathbb{A}_K^\times)^1$. Suppose y is an element of this neighborhood, and also lies in $(\mathbb{A}_K^\times)^1$. If there exists $v_0 \notin S$ such that $\|y_{v_0}\|_{v_0} < 1$, then $\|y_{v_0}\|_{v_0} \leq |k_{v_0}|^{-1} < (2P)^{-1}$. Since $\prod_{v\in S} \|y_v\|_v < 2P$, we must have $\|y\| < 1$, a contradiction. Thus for all $v \notin S$ we have $\|y_v\|_v = 1$. Then

$$\|y\| = \prod_{v\in S} \|y_v\|_v \in (1, 2P),$$

again contradicting with $\|y\| = 1$.

(2) It suffices to show that for each $x \in (\mathbb{A}_K^\times)^1$, there is a family of subsets of $(\mathbb{A}_K^\times)^1$ containing x which is a neighborhood basis in both topologies. Fix x. Consider a finite subset $S \subset V_K$ containing $V_{K,\infty}$ such that for all $v \notin S$, $\|x_v\|_v = 1$. For each $v \in S$, consider an open neighborhood U_v of x_v in $K_v^\times$ such that for all $(y_v)_{v\in S} \in \prod_{v\in S} U_v$, we have $\prod_v \|y_v\|_v \in [2/3, 4/3]$. This can always be arranged by shrinking U_v, since we have $\prod_{v\in S} \|x_v\|_v = 1$. Clearly if we let S and $(U_v)_{v\in S}$ vary, then the resulting sets

$$U = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_{K_v}, \quad V = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times$$

form a neighborhood basis of x in $\mathbb{A}_K$ and a neighborhood basis of x in $\mathbb{A}_K^\times$ respectively. It remains to show that

$$U \cap (\mathbb{A}_K^\times)^1 = V \cap (\mathbb{A}_K^\times)^1.$$

Clearly the right hand side is contained in the left hand side. Let $y \in U \cap (\mathbb{A}_K^\times)^1$. If there exists $v_0 \notin S$ such that $\|y_{v_0}\|_{v_0} < 1$, then $\|y_{v_0}\|_{v_0} \le 1/2$. Since $\prod_{v\in S} \|y_v\|_v \le 4/3$, we have $\|y\| \le 2/3$, a contradiction. Hence such v_0 does not exist, and so $y \in V$. □

Proof of Theorem 3.7.2. By Lemma 3.7.3, we only need to find a compact subset $E \subset \mathbb{A}_K$ such that $E \cap (\mathbb{A}_K^\times)^1$ maps onto $(\mathbb{A}_K^\times)^1/K^\times$ under the projection. Let c be the constant in Theorem 3.6.2, and let $x \in \mathbb{A}_K^\times$ be such that $\|x\| > c$. We take E to be S_x, which is compact. We need to show that $(\mathbb{A}_K^\times)^1 = ((\mathbb{A}_K^\times)^1 \cap S_x) \cdot K^\times$. Let $y \in (\mathbb{A}_K^\times)^1$ be arbitrary. Then $\|x/y\| = \|x\| > c$, and so there exists $r \in S_{x/y} \cap K^\times$. We have $ry \in (\mathbb{A}_K^\times)^1 \cap S_x$. □

3.8. **Classical finiteness results.** Let K be a global field, and let S be a subset of V_K. In the number field case, assume that S contains all the archimedean places. In the function field case, assume that S is non-empty. Recall that we have the ring of S-integers

$$\mathcal{O}_{K,S} = \{x \in K \mid \|x\|_v \le 1,\ \forall v \notin S\}.$$

This is a Dedekind domain with fraction field K. Its prime ideals are in bijection with the set $V_K - S$. As usual, we define the class group $\mathrm{Cl}(\mathcal{O}_{K,S})$ of $\mathcal{O}_{K,S}$ to be the group of fractional ideals (i.e., $\mathcal{O}_{K,S}$-submodules $\mathfrak{a}$ of K such that there exists $x \in K^\times$ with $x\mathfrak{a} \subset \mathcal{O}_{K,S}$) modulo the group of principal fractional ideals (i.e., $\mathcal{O}_{K,S}$-submodules of K generated by a single element). It is identified with the cokernel of the map

$$\Phi : K^\times \to \mathbb{Z}[V_K - S] = \bigoplus_{v\notin S} \mathbb{Z}, \quad x \mapsto \sum_{v\notin S} \mathrm{ord}_v(x)[v].$$

Also note that the kernel of Φ is exactly the group of units in $\mathcal{O}_{K,S}$:

$$\mathcal{O}_{K,S}^\times = \{x \in K^\times \mid \|x\|_v = 1,\ \forall v \notin S\}.$$

In order to relate the groups $\mathrm{cok}(\Phi) = \mathrm{Cl}(\mathcal{O}_{K,S})$ and $\ker(\Phi) = \mathcal{O}_{K,S}^\times$ to ideles, we define

$$\mathbb{A}_{K,S} := \{(x_v)_v \in \mathbb{A}_K \mid \forall v \notin S,\ \|x_v\|_v \le 1\} = \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v}.$$

This is a basic open set in $\mathbb{A}_K$, and as such its subspace topology agrees with the product topology. It is a subring of $\mathbb{A}_K$, and its group of invertible elements is

$$\mathbb{A}_{K,S}^\times = \{(x_v)_v \in \mathbb{A}_K^\times \mid \forall v \notin S,\ \|x_v\|_v = 1\} = \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times.$$

This is an open subgroup of $\mathbb{A}_K^\times$, and we endow it with the subspace topology, which agrees with the product topology.

Clearly, by definition, $\mathbb{A}_K$ (resp. $\mathbb{A}_K^\times$) is the union of $\mathbb{A}_{K,S}$ (resp. $\mathbb{A}_{K,S}^\times$) over all choices of S as above.

Now we have the following simple observations:

$$\mathcal{O}_{K,S} = K \cap \mathbb{A}_{K,S}, \quad \mathcal{O}_{K,S}^\times = K^\times \cap \mathbb{A}_{K,S}^\times.$$

Moreover, the map $\Phi : K^\times \to \mathbb{Z}[V_K - S]$ extends to a homomorphism

$$\Phi : \mathbb{A}_K^\times \to \mathbb{Z}[V_K - S], \quad (x_v)_{v\in V_K} \mapsto \sum_{v\notin S} \mathrm{ord}_v(x_v)[v].$$

The following is a key observation:

Lemma 3.8.1. *The map Φ induces an isomorphism $\mathbb{A}_K^\times/(K^\times \mathbb{A}_{K,S}^\times) \xrightarrow{\sim} \mathrm{Cl}(\mathcal{O}_{K,S})$.*

Proof. Clearly $\Phi : \mathbb{A}_K^\times \to \mathbb{Z}[V_K - S]$ is surjective, and its kernel is $\mathbb{A}_{K,S}^\times$. □

In the following, we denote by $\mathscr{M}_K$ the image of $\|\cdot\| : \mathbb{A}_K^\times \to \mathbb{R}_{>0}$. If K is a number field, then $\mathscr{M}_K = \mathbb{R}_{>0}$. If K is a function field of characteristic p, then $\mathscr{M}_K = q^{\mathbb{Z}}$ for some p-power q. As a fact, q is such that $\mathbb{F}_q$ is the algebraic closure of $\mathbb{F}_p$ in K, and K is the function field of a projective, smooth, geometrically connected curve over $\mathbb{F}_q$. We will not use this fact.

Theorem 3.8.2. *The group* $\mathrm{Cl}(\mathcal{O}_{K,S})$ *is finite.*

Proof. By Lemma 3.8.1, we need to show that $\mathbb{A}_K^\times/(K^\times \mathbb{A}_{K,S}^\times)$ is finite. To simplify notation, write $\mathbb{A}^1$ for $(\mathbb{A}_K^\times)^1$, and write $\mathbb{A}_S^1$ for $(\mathbb{A}_K^\times)^1 \cap \mathbb{A}_{K,S}^\times$. We have a short exact sequence

$$1 \to \mathbb{A}^1/\mathbb{A}_S^1 \to \mathbb{A}_K^\times/\mathbb{A}_{K,S}^\times \xrightarrow{\|\cdot\|} \mathscr{M}_K/\|\mathbb{A}_{K,S}^\times\| \to 1.$$

Clearly $\mathscr{M}_K/\|\mathbb{A}_{K,S}^\times\|$ is finite, so $\mathbb{A}^1/\mathbb{A}_S^1$ is a subgroup of finite index in $\mathbb{A}_K^\times/\mathbb{A}_{K,S}^\times$. Now the image of $K^\times \to \mathbb{A}_K^\times/\mathbb{A}_{K,S}^\times$ is contained in $\mathbb{A}^1/\mathbb{A}_S^1$, so it suffices to prove the finiteness of

$$\mathbb{A}^1/(\mathbb{A}_S^1 \cdot K^\times).$$

This follows from the compactness of $\mathbb{A}^1/K^\times$, and the fact that $\mathbb{A}_S^1$ is an open subgroup of $\mathbb{A}^1$. □

Theorem 3.8.3. *The group* $\mathcal{O}_{K,S}^\times$ *is a finitely generated abelian group of rank* $\#S-1$.

For the proof we need two lemmas.

Lemma 3.8.4. *For any finite closed interval* $[a,b] \subset \mathbb{R}$*, the set*

$$\{x \in \mathcal{O}_{K,S}^\times \mid \forall v \in S,\ \|x\|_v \in [a,b]\}$$

is finite.

Proof. The set in question is the intersection of $K^\times$ with the set

$$\{(x_v)_v \in \mathbb{A}_K^\times \mid \forall v \in S,\ \|x_v\|_v \in [a,b];\ \forall v \notin S,\ \|x_v\|_v = 1\}$$

in $\mathbb{A}_K^\times$. The latter set is compact in $\mathbb{A}_K^\times$, and $K^\times$ is discrete in $\mathbb{A}_K^\times$, so the intersection is finite. □

The following lemma is also of independent interest.

Lemma 3.8.5. *We have* $\{x \in K^\times \mid \forall v \in V_K,\ \|x\|_v = 1\} = \{$*roots of unity in* $K^\times\}$. *This group is finite.*

Proof. Clearly the right hand side is contained in the left hand side. To prove the reverse containment, it suffices to show that the left hand side is a finite group. This is a special case of Lemma 3.8.4. □

Proof of Theorem 3.8.3. Let $B = \prod_{v\in S} K_v^\times$, and let $B^1 = \{(x_v)_{v\in S} \in B \mid \prod_{v\in S}\|x_v\|_v = 1\}$. Then B^1 is a subgroup of B under coordinate-wise multiplication. We view $\mathcal{O}_{K,S}^\times$ as a subgroup of B via the diagonal embedding. Then it is a subgroup of B^1.

Let $L : B \to \mathbb{R}^S$ be the map $(x_v)_{v\in S} \mapsto (\log\|x_v\|_v)_{v\in S}$. Let H be the hyperplane in $\mathbb{R}^S$ defined by the condition that the sum of all the coordinates is zero. Thus $B^1 = L^{-1}(H)$. By lemma 3.8.4, the intersection of any compact neighborhood of 0 in $\mathbb{R}^S$ with $L(\mathcal{O}_{K,S}^\times)$ is finite, so $L(\mathcal{O}_{K,S}^\times) \subset H \subset \mathbb{R}^S$ is a discrete subgroup. By Lemma 3.8.5, $\ker L|_{\mathcal{O}_{K,S}^\times}$ is finite. Hence $\mathcal{O}_{K,S}^\times$ is finitely generated of rank at most $\dim_{\mathbb{R}} H = \#S-1$.

To prove that the rank is exactly $\#S-1$, we need to prove that $L(\mathcal{O}_{K,S}^\times)$ is a complete lattice in H. We divide the proof into the number field case and the function field case.

In the number field case, pick an archimedean place v_0. Then the projection $\mathbb{R}^S \to \mathbb{R}^{S-\{v_0\}}$ induces an isomorphism $\phi : H \xrightarrow{\sim} \mathbb{R}^{S-\{v_0\}}$. We have

$$\phi(L(B^1)) = \prod_{v\in S-\{v_0\}} \log \|K_v^\times\|_v,$$

since $\log\|\cdot\|_{v_0} : K_{v_0}^\times \to \mathbb{R}$ is surjective. Now the above is equal to

$$\prod_{v\in V_{K,\infty}-\{v_0\}} \mathbb{R} \times \prod_{v\in S\cap V_{K,f}} \mathbb{Z}\cdot \log \#k_v.$$

Hence in order to prove that $L(\mathcal{O}_{K,S}^\times)$ is a complete lattice in H it suffices to prove that $\phi(L(B^1))/\phi(L(\mathcal{O}_{K,S}^\times))$ is compact, and for this it suffices to show that $B^1/\mathcal{O}_{K,S}^\times$ is compact. We have a projection $\mathbb{A}_{K,S}^\times \cap (\mathbb{A}_K^\times)^1 \to B^1$, mapping $(x_v)_{v\in V_K}$ to $(x_v)_{v\in S}$. This is a continuous surjective homomorphism. Thus it suffices to show that $(\mathbb{A}_{K,S}^\times \cap (\mathbb{A}_K^\times)^1)/\mathcal{O}_{K,S}^\times$ is compact, where $\mathcal{O}_{K,S}^\times$ maps into $\mathbb{A}_{K,S}^\times$ diagonally (across all places). But this group is an open, and hence closed, subgroup of the compact group $(\mathbb{A}_K^\times)^1/K^\times$. Hence this group is compact as desired.

In the function field case, we first note that $L(B^1)$ is a complete lattice in H. Indeed, it is clearly a discrete subgroup of H as every $\|\cdot\|_v : K_v^\times \to \mathbb{R}_{>0}$ has discrete image. We now show that it is a complete lattice. If S has only one element, then there is nothing to prove, so suppose that S has at least two elements. Pick an arbitrary $v_0\in S$. Again the projection $\mathbb{R}^S \to \mathbb{R}^{S-\{v_0\}}$ induces an isomorphism $\phi : H \xrightarrow{\sim} \mathbb{R}^{S-\{v_0\}}$. Note that $\{\prod_{v\in S-\{v_0\}} \|x_v\|_v \mid (x_v)\in \prod_{v\in S-\{v_0\}} K_v^\times\}$ and $\|K_{v_0}^\times\|_{v_0}$ are both infinite subgroups of the infinite cyclic group $\mathscr{M}_K$. Hence $\phi(L(B^1))$ is of finite index in $\prod_{v\in S-\{v_0\}} \log\|K_v^\times\|_v$. Since the latter is a complete lattice in $\mathbb{R}^{S-\{v_0\}}$, we conclude that $L(B^1)$ is a complete lattice in H. Now in order to show that $L(\mathcal{O}_{K,S}^\times)$ is a complete lattice in H, it again suffices to show that $B^1/\mathcal{O}_{K,S}^\times$ is compact. This is proved in the same way as in the number field case. □

3.9. The idele class group.

Let K be a global field.

Definition 3.9.1. The *idele class group* of K is $C_K = \mathbb{A}_K^\times/K^\times$.

The idele norm $\|\cdot\| : \mathbb{A}_K^\times \to \|\cdot\|$ descends to C_K by the product formula for K. We shall view $\|\cdot\|$ as a homomorphism $C_K \to \mathbb{R}_{>0}$, and denote its kernel by C_K^1. Of course $C_K^1 = (\mathbb{A}_K^\times)^1/K^\times$, which we have seen is compact.

Again, let $\mathscr{M}_K$ be the image of $\|\cdot\| : \mathbb{A}_K^\times \to \mathbb{R}_{>0}$. Clearly there exists a continuous homomorphism $s : \mathscr{M}_K \to \mathbb{A}_K^\times$ which is a section of $\|\cdot\|$. (In the number field case, pick an archimedean place v_0 of K, and let $\tilde{s} : \mathbb{R}_{>0} \to K_{v_0}^\times$ be a continuous homomorphism that is a section of $\|\cdot\|_{v_0} : K_{v_0}^\times \to \mathbb{R}_{>0}$. For instance, if $K_{v_0} = \mathbb{R}$ then we can take $\tilde{s}(t) = t$, and if $K_{v_0} = \mathbb{C}$ we can take $\tilde{s}(t) = \sqrt{t}$. Then define $s : \mathscr{M}_K = \mathbb{R}_{>0} \to \mathbb{A}_K^\times, t \mapsto (\tilde{s}(t), 1, 1, \cdots) \in \mathbb{A}_K^\times$ where $\tilde{s}(t)$ appears at the place v_0. In the function field case, write $\mathscr{M}_K = q^{\mathbb{Z}}$. Pick any $x \in \mathbb{A}_K^\times$ with $\|x\| = q$, and define $s(q^n) = x^n$.) Once such a section is chosen, we obtain isomorphisms of topological groups

$$\mathbb{A}_K^\times \cong \mathscr{M}_K \times (\mathbb{A}_K^\times)^1, \quad C_K \cong \mathscr{M}_K \times C_K^1.$$

Now let L be a finite separable extension of K. Then we obtain natural maps $\mathbb{A}_K \hookrightarrow \mathbb{A}_L, \mathbb{A}_K^\times \hookrightarrow \mathbb{A}_L^\times$, which are compatible with the inclusions $K \hookrightarrow L, K^\times \hookrightarrow L^\times$. Thus we obtain a natural map $C_K \to C_L$.

Lemma 3.9.2. *The map $C_K \to C_L$ is injective.*

Proof. We need to show that the intersection of $L^\times$ and $\mathbb{A}_K^\times$ inside $\mathbb{A}_L^\times$ is $K^\times$. For this, it suffices to show that the intersection of L and $\mathbb{A}_K$ inside $\mathbb{A}_L$ is K. This immediately follows from the canonical isomorphism $L \otimes_K \mathbb{A}_K \cong \mathbb{A}_L$. □

Write $\|\cdot\|_K : \mathbb{A}_K^\times \to \mathbb{R}_{>0}, \|\cdot\|_L : \mathbb{A}_L^\times \to \mathbb{R}_{>0}$ for the idele norms respectively.

Exercise 3.9.3. Write i for the map $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$. Show that for any $x \in \mathbb{A}_K^\times$, we have $\|i(x)\|_L = \|x\|_K^{[L:K]}$.

Proposition 3.9.4. *The map $C_K \to C_L$ is a closed embedding.*

Proof. By Exercise 3.9.3, we have a commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & C_K^1 \arrow[r] \arrow[d, "i"] & C_K \arrow[r] \arrow[d, "i"] & \mathscr{M}_K \arrow[r] \arrow[d, "(\cdot)^{[L:K]}"] & 1 \\
1 \arrow[r] & C_L^1 \arrow[r] & C_L \arrow[r] & \mathscr{M}_L \arrow[r] & 1
\end{tikzcd}$$

The map $i : C_K^1 \to C_L^1$ is an injective continuous homomorphism between compact Hausdorff groups, so it is a closed embedding.

First assume that K, L are function fields, so $\mathscr{M}_K, \mathscr{M}_L$ are infinite cyclic groups in $\mathbb{R}_{>0}$. Then as a topological space, C_K is the disjoint union of $\mathscr{M}_K$-copies of C_K^1. More precisely, each coset of C_K^1 in C_K is open and closed, and homeomorphic to C_K^1. Similarly for C_L. Since $i : C_K \to C_L$ is injective, it suffices to show that it is a closed map. Let B be a closed subset of C_K. Then B is of the form $\coprod_{t \in \mathscr{M}_K} B_t$, where B_t is a closed subset of the coset of C_K^1 in C_K corresponding to t. Now different cosets of C_K^1 in C_K are mapped into different cosets of C_L^1 in C_L since $(\cdot)^{[L:K]} : \mathscr{M}_K \to \mathscr{M}_L$ is injective. In C_L, if in each coset of C_L^1 we take a closed subset, then the union of them is closed. Hence it suffices to show that each B_t has closed image in C_L. This easily follows from the fact that $C_K^1 \to C_L^1$ is a closed embedding.

Now assume that K, L are number fields. Pick a continuous homomorphism $s : \mathscr{M}_K \to \mathbb{A}_K^\times$ that is a section of $\|\cdot\|_K$. By Exercise 3.9.3, the composite map

$$s' : \mathscr{M}_L = \mathbb{R}_{>0} \xrightarrow{(\cdot)^{1/[L:K]}} \mathbb{R}_{>0} = \mathscr{M}_K \overset{s}{\to} \mathbb{A}_K^\times \overset{i}{\to} \mathbb{A}_L^\times$$

is a continuous homomorphism which is a section of $\|\cdot\|_L$. Using the sections s and s' to make identifications $C_K \cong C_K^1 \times \mathbb{R}_{>0}, C_L \cong C_L^1 \times \mathbb{R}_{>0}$, the map $i : C_K \to C_L$ becomes $(x, t) \mapsto (i(x), t^{[L:K]})$ for $x \in C_K^1, t \in \mathbb{R}_{>0}$. This is clearly a closed embedding since $i : C_K^1 \to C_L^1$ is a closed embedding. □

We have seen that the $\mathbb{A}_K$-module $\mathbb{A}_L$ is isomorphic to $L \otimes_K \mathbb{A}_K$, so it is free of rank $[L : K]$. For any $x \in \mathbb{A}_L$, the multiplication map $x : \mathbb{A}_L \to \mathbb{A}_L, y \mapsto xy$ is $\mathbb{A}_K$-linear, so we can consider its determinant, which is an element of $\mathbb{A}_K$. This determinant is called the *norm* of x to $\mathbb{A}_K$, denoted by $\mathrm{N}_{L/K}(x)$.

Lemma 3.9.5. *The following statements hold.*

(1) *For any $x \in \mathbb{A}_L$, we have $x \in \mathbb{A}_L^\times$ if and only if $\mathrm{N}_{L/K}(x) \in \mathbb{A}_K^\times$. In particular, we have a group homomorphism $\mathrm{N}_{L/K} : \mathbb{A}_L^\times \to \mathbb{A}_K^\times$.*

(2) *We have a commutative diagram*

$$\begin{tikzcd} L \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"'] & \mathbb{A}_L \arrow[d, "\mathrm{N}_{L/K}"] \\ K \arrow[r] & \mathbb{A}_K \end{tikzcd},$$

where $\mathrm{N}_{L/K} : L \to K$ is the usual norm for a field extension.

(3) *For $x = (x_w)_w \in \mathbb{A}_L$, we have $\mathrm{N}_{L/K}(x) = (y_v)_v$, with $y_v = \prod_{w \in V_L, w|v} \mathrm{N}_{L_w/K_v}(x_w)$.*

(4) *For $x \in \mathbb{A}_L^\times$, we have $\|\mathrm{N}_{L/K}(x)\|_K = \|x\|_L$.*

(5) *For $x \in \mathbb{A}_K \subset \mathbb{A}_L$, we have $\mathrm{N}_{L/K}(x) = x^{[L:K]}$.*

Proof. Exercise. □

By the lemma, we have a homomorphism $\mathrm{N}_{L/K} : C_L \to C_K$ that is compatible with $\|\cdot\|_L$ and $\|\cdot\|_K$. In particular it restricts to a homomorphism $C_L^1 \to C_K^1$.

3.10. **The identity connected component.** Next we study the identity connected component of C_K. For any topological group G, we denote by G^0 the identity connected component, i.e., the connected component of the identity element.

Lemma 3.10.1. *The subset G^0 is a closed normal subgroup of G. If H is a connected subgroup of G such that the homogeneous space G/H with the quotient topology is totally disconnected, then $H = G^0$.*

Proof. The closure of any connected subset is connected, so G^0 is closed. For any $g \in G$, the map $G \to G, x \mapsto gxg^{-1}$ is a homeomorphism sending e to e, so it stabilizes G^0. Hence G^0 is normal. If H is as in the lemma, then clearly $H \subset G^0$. The image of G^0 in G/H, being connected and containing e, must be $\{e\}$. Hence $G^0 = H$. □

Remark 3.10.2. It is not always true that G/G^0 is totally disconnected.

Definition 3.10.3. An element g of a group G is called *divisible*, if for every $n \in \mathbb{Z}_{\geq 1}$ there exists $h \in G$ such that $h^n = g$.

Let K be a number field. Let D'_K denote the image of $(\prod_{v \in V_{K,\infty}} K_v^\times)^0$ under the composite map $\prod_{v \in V_{K,\infty}} K_v^\times \hookrightarrow \mathbb{A}_K^\times \to C_K$. Let D_K be the closure of D'_K. Since D'_K is a subgroup, so is D_K.

Proposition 3.10.4. *Let K be a number field. We have*

$$D_K = C_K^0 = \{\textit{divisible elements of } C_K\}.$$

The quotient group C_K/D_K is profinite.

For the proof we need some preparations.

Definition 3.10.5. A topological group is called *locally profinite*, if it has an open subgroup which is profinite.

Lemma 3.10.6. *Any locally profinite group is totally disconnected.*

Proof. Suppose G has an open subgroup H which is locally profinite. Since H is an open subgroup, it is closed. Hence $G^0 \cap H$ is open and closed in G^0. Since G^0 is connected, we must have $G^0 \cap H = G_0$, i.e., $G^0 \subset H$. Then since H is totally disconnected, we have $G^0 = \{e\}$. This implies that G is totally disconnected. □

Lemma 3.10.7. *Let $\phi : G \to H$ be a surjective continuous homomorphism from a profinite group G to a Hausdorff topological group H. Then ϕ is a quotient map, and H is profinite.*

Proof. Since G is compact and H is Hausdorff, ϕ is a closed map, and hence a quotient map. (If U is a subset of H such that $\phi^{-1}(U)$ is open, then U is open since $H-U = \phi(G-\phi^{-1}(U))$ is closed.) Let $N = \ker \phi$, which is a closed normal subgroup of G. Since ϕ is a quotient map, we have a topological isomorphism $G/N \cong H$. Since G is compact, so is H. It remains to show that $G/N \cong H$ is totally disconnected. For this, it suffices to show that any non-trivial element of G/N has an open and closed neighborhood disjoint from the trivial element. (As it then follows that the connected component of the trivial element is singleton.) The quotient map $G \to G/N$ is open (as for any quotient map between topological groups) and closed (as G is compact and G/N is Hausdorff). Hence it suffices to show that any non-trivial N-coset gN in G has an open and closed neighborhood which is disjoint from N. For any $y \in gN$, the set $G - N$ is an open neighborhood of y. Since G is a profinite group, y has a neighborhood basis consisting of compact open sets (by Exercise 2.2.5). Hence y has a compact open neighborhood U_y contained in $G - N$. Since gN is compact, there exist finitely many $y_1, \cdots, y_n \in gN$ such that $gN \subset \bigcup_{i=1}^n U_{y_i}$. Then $\bigcup_{i=1}^n U_{y_i}$ is the desired open and closed (since it is compact) neighborhood of gN. □

Lemma 3.10.8. *In a profinite group, the only divisible elements is e.*

Proof. The profinite group is an inverse limit of finite groups. In each finite group, the only divisible element is the trivial element. □

Proof. Let $U = \prod_{v \in V_{K,\infty}} K_v^\times \times \prod_{v \in V_{K,f}} \mathcal{O}_{K_v}^\times$. This is an open subgroup of $\mathbb{A}_K^\times$, and its subspace topology agrees with the product topology. By the definition of D_K, the map $U \to C_K/D_K$ factors through the following quotient of U (equipped with product topology):

$$U' = \prod_{v \text{ complex}} \{1\} \times \prod_{v \text{ real}} \{\pm 1\} \times \prod_{v \in V_{K,f}} \mathcal{O}_{K_v}^\times.$$

Here, for v real, the quotient map $K_v^\times \to \{\pm 1\}$ is the sign map. Clearly U' is profinite. Since C_K/D_K is Hausdorff (as D_K is by definition closed), we conclude by Lemma 3.10.7 that the image of U in C_K/D_K is profinite. But U is open in C_K, so its image is open in C_K/D_K. Hence C_K/D_K is locally profinite, and in particular totally disconnected by Lemma 3.10.6. Since D_K is the closure of the connected subgroup D_K' in C_K, it is itself a connected subgroup. Then by Lemma 3.10.1, we have $D_K = C_K^0$. We have already seen that C_K/D_K is Hausdorff totally disconnected. To show it is profinite, we need to check that it is compact. Clearly $\|\cdot\| : C_K \to \mathbb{R}_{>0}$ restricts to a surjection $D_K' \to \mathbb{R}_{>0}$. Hence $C_K = D_K C_K^1$. Since C_K^1 is compact, C_K/D_K is compact.

Finally, we need to check that D_K is equal to the set of divisible elements. Since C_K/D_K is profinite, by Lemma 3.10.8 all divisible elements of C_K are contained in D_K. Conversely, we need to check that for any $n \in \mathbb{Z}_{\geq 1}$, the image of the n-th power map $C_K \to C_K, x \mapsto x^n$ contains D_K. This image already contains D_K' since every element of $(\prod_{v \in V_{K,\infty}} K_v^\times)^0 \cong \mathbb{R}_{>0}^r \times (\mathbb{C}^\times)^s$ is divisible, so it suffices to check that this image is closed. We have a (non-canonical) isomorphism $C_K = C_K^1 \times \mathbb{R}_{>0}$. Clearly the n-th power map on $\mathbb{R}_{>0}$ has closed image ($= \mathbb{R}_{>0}$). The n-th power map on C_K^1 has closed image because C_K^1 is compact Hausdorff. □

The function field case is slightly different, but the ideas are similar.

Proposition 3.10.9. *Let K be a function field. Then C_K^1 is profinite and C_K is locally profinite. In particular C_K is totally disconnected and $C_K^0 = \{e\}$. The only divisible element of C_K is e.*

Proof. Let $U = \prod_{v \in V_K} \mathcal{O}_{K_v}^\times$. This is an open subgroup of $\mathbb{A}_K^\times$, and profinite. Its image in C_K is open, and profinite by Lemma 3.10.7. Hence C_K is locally profinite, and in particular totally disconnected by Lemma 3.10.6. Now C_K^1 is Hausdorff and compact, and it is totally disconnected since C_K is. Hence C_K^1 is profinite. We have a non-canonical isomorphism $C_K \cong C_K^1 \times q^{\mathbb{Z}}$. The factor C_K^1 has no non-trivial divisible elements since it is profinite (Lemma 3.10.8). The factor $q^{\mathbb{Z}} \cong \mathbb{Z}$ clearly has no non-trivial divisible elements. □

Remark 3.10.10. For K a number field, global class field theory states that the profinite group C_K/D_K is canonically isomorphic to the abelianized absolute Galois group $G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$. For K a function field, we have $C_K \cong C_K^1 \times q^{\mathbb{Z}}$, and the profinite completion $\widehat{C_K} \cong C_K^1 \times q^{\widehat{\mathbb{Z}}}$. In this case global class field theory states that $\widehat{C_K}$ is canonically isomorphic to G_K^{ab}.

4. Class field theory

4.1. Class field theory for $\mathbb{Q}$ and $\mathbb{Q}_p$.

For $\mathbb{Q}$ and $\mathbb{Q}_p$, the corresponding global and local class field theories involve essentially the cyclotomic extensions. We first recall some generalities about cyclotomic extensions.

Let K be a field of characteristic zero. For $m \in \mathbb{Z}_{\geq 1}$, let ζ_m denote a primitive m-th root of unity in a (fixed) algebraic closure $\overline{K}$ of K. The extension $K(\zeta_m)/K$ is the splitting field of $X^m - 1$, and is hence Galois. It is called the m-th cyclotomic extension of K. We have a canonical injective homomorphism

$$\alpha : \mathrm{Gal}(K(\zeta_m)/K) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times,$$

sending σ to $a + m\mathbb{Z}$ such that $\sigma(\zeta) = \zeta^a$ for any m-th root of unity. In particular, $K(\zeta_m)/K$ is an abelian extension whose degree divides $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$.

We define the m-th *cyclotomic polynomial* to be

$$\Phi_m(X) = \prod_{\text{primitive } m\text{-th roots of unity } \omega} (X - \omega).$$

A priori, $\Phi_m(X)$ has coefficients in a chosen algebraically closed field where we consider the roots of unity, but note that each $\Phi_m(X)$ is a monic polynomial and we have the recursive relations

$$\Phi_1(X) = X - 1, \quad \Phi_m(X) = \frac{X^m - 1}{\prod_{1 \leq d < m, d \mid m} \Phi_d(X)}.$$

Hence we have $\Phi_m(X) \in \mathbb{Z}[X]$, and the definition is independent of any choice of algebraically closed field.

Lemma 4.1.1. *The following conditions are equivalent.*

1. *$\Phi_m(X)$ is irreducible in $K[X]$.*
2. *$\alpha : \mathrm{Gal}(K(\zeta_m)/K) \to (\mathbb{Z}/m\mathbb{Z})^\times$ is an isomorphism.*
3. *$[K(\zeta_m) : K] = \phi(m)$.*

(4) $\Phi_m(X)$ *is the minimal polynomial of* ζ_m *over* K.

Proof. Easy exercise. □

Theorem 4.1.2 (Gauss)**.** *For any* $m \in \mathbb{Z}_{\geq 1}$, $\Phi_m(X)$ *is irreducible in* $\mathbb{Q}[X]$.

Exercise 4.1.3. We prove the theorem in steps. Assume Φ_m is not irreducible in $\mathbb{Q}[X]$. Since it is a monic polynomial in $\mathbb{Z}[X]$, it is not irreducible in $\mathbb{Z}[X]$ by Gauss's Lemma. Hence $\Phi_m = fg$, with $f, g \in \mathbb{Z}[X]$, f irreducible, and $\deg f, \deg g \geq 1$.

(1) Suppose ζ is a root of f such that ζ^p is a root of g for some prime p coprime to m. Show that f divides g^p inside $\mathbb{F}_p[X]$.
(2) Under the above assumption, show that Φ_m has a multiple root, which is a contradiction.
(3) Use the above results to show that every primitive m-th root of unity is a root of f, finishing the proof.

As a consequence, we have an isomorphism $\alpha : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$. Define

$$\psi_m : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}), \quad x \mapsto \alpha^{-1}(x^{-1}).$$

For any finite abelian extension of global fields L/K, and for any non-archimedean place v of K, the decomposition group $D(L/v) \subset \mathrm{Gal}(L/K)$ is well defined. If v is unramified in L/K, then for any place w of L above v, $D(L/v) = D(w/v)$ is canonically isomorphic to $\mathrm{Gal}(l_w/k_v)$, where l_w denotes the residue field of L at w and k_v denotes the residue field of K at v. This is a cyclic group with a distinguished generator, namely the Frobenius $l_w \to l_w, x \mapsto x^{\# k_v}$. Moreover, this Frobenius element of $D(L/v)$ is independent of the choice of w. We shall denote it by Frob_v and call it the Frobenius element at v of $\mathrm{Gal}(L/K)$.

Proposition 4.1.4. *A prime* $p \in \mathbb{Q}$ *is unramified in* $\mathbb{Q}(\zeta_m)$ *if and only if* p *does not divide* m. *In this case,* $\psi_m(p^{-1}) \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ *is the Frobenius at* p.

Exercise 4.1.5. Admit the first statement in the proposition. Also admit that the ring of integers in $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$. Prove that $\psi_m(p^{-1})$ is the Frobenius at p. (Hint: the more difficult part is to prove that this actually lies in the decomposition group.)

For $m|m'$, we have $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{m'})$, and we have a commutative diagram

$$\begin{tikzcd}
(\mathbb{Z}/m'\mathbb{Z})^\times \arrow[r, "\psi_{m'}"] \arrow[d] & \mathrm{Gal}(\mathbb{Q}(\zeta_{m'})/\mathbb{Q}) \arrow[d] \\
(\mathbb{Z}/m\mathbb{Z})^\times \arrow[r, "\psi_m"] & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})
\end{tikzcd}$$

where the vertical map on the left is $a + m'\mathbb{Z} \mapsto a + m\mathbb{Z}$, and the vertical map on the right is restriction. Taking inverse limit over m, we obtain an isomorphism of profinite groups

$$\psi : \widehat{\mathbb{Z}}^\times = \varprojlim_m (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}).$$

Here $\mathbb{Q}_{\mathrm{cyc}}$ denotes the union of all $\mathbb{Q}(\zeta_m)$ in $\overline{\mathbb{Q}}$, and we identify $\varprojlim_m (\mathbb{Z}/m\mathbb{Z})^\times$ with $\widehat{\mathbb{Z}}^\times$, the group of invertible elements of the ring $\widehat{\mathbb{Z}} =$ the profinite completion of $\mathbb{Z}$.

Exercise 4.1.6. Equip $\widehat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$ with the inverse limit topology (where each $\mathbb{Z}/m\mathbb{Z}$ is discrete), so it is the profinite completion of $\mathbb{Z}$. Equip $\widehat{\mathbb{Z}}^\times$ with the subspace topology inherited along $\widehat{\mathbb{Z}}^\times \hookrightarrow \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}, x \mapsto (x, x^{-1})$. Show that there is a natural isomorphism of topological groups $\widehat{\mathbb{Z}}^\times \xrightarrow{\sim} \varprojlim_m (\mathbb{Z}/m\mathbb{Z})^\times$ (where the right hand side has the inverse limit topology). Also show that there is a natural isomorphism of topological groups $\widehat{\mathbb{Z}}^\times \xrightarrow{\sim} \prod_p \mathbb{Z}_p^\times$. (Compare with Exercise 2.2.10.)

Theorem 4.1.7 (Kronecker–Weber theorem)**.** *We have* $\mathbb{Q}_{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$.

Thus ψ is an isomorphism $\widehat{\mathbb{Z}}^\times \xrightarrow{\sim} G_{\mathbb{Q}}^{\mathrm{ab}}$. The left hand side is related to the idele class group as follows.

Lemma 4.1.8. *The group* $\mathbb{A}_{\mathbb{Q}}^\times$ *is generated by its subgroups* $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times = \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times$ *and* $\mathbb{Q}^\times$. *The intersection of the two subgroups is trivial.*

Proof. The argument is similar to Example 3.3.4. For any $(x_v)_v \in \mathbb{A}_{\mathbb{Q}}^\times$, let $y = \prod_p p^{\mathrm{ord}_p(x_p)} \in \mathbb{Q}^\times$. Then $y^{-1} \cdot (x_v)_v$ lies in $\mathbb{R}^\times \times \widehat{\mathbb{Z}}^\times$. If the coordinate in $\mathbb{R}^\times$ is negative, then we can multiply this element by $-1 \in \mathbb{Q}^\times$ to move it into $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times$. This shows that the two subgroups in question generate $\mathbb{A}_{\mathbb{Q}}^\times$. Obviously their intersection is trivial. □

By the lemma, we have a topological isomorphism $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \xrightarrow{\sim} C_{\mathbb{Q}}$ induced by the inclusion $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}}^\times$. Clearly this isomorphism maps $\mathbb{R}_{>0} \times \{1\}$ to $D_{\mathbb{Q}} = C_{\mathbb{Q}}^0$. Hence $C_{\mathbb{Q}}/D_{\mathbb{Q}}$ is canonically identified with $\widehat{\mathbb{Z}}^\times$. In this way we can view ψ as an isomorphism

$$\psi : C_{\mathbb{Q}}/D_{\mathbb{Q}} \xrightarrow{\sim} G_{\mathbb{Q}}^{\mathrm{ab}}.$$

We shall also view ψ as a map from $C_{\mathbb{Q}}$ or $\mathbb{A}_{\mathbb{Q}}^\times$ towards $G_{\mathbb{Q}}^{\mathrm{ab}}$. It is called the *global Artin map* for $\mathbb{Q}$.

For each prime p, we have a canonical injective homomorphism $\mathbb{Q}_p^\times \to \mathbb{A}_{\mathbb{Q}}^\times$ sending y to $(x_v)_v$ with $x_v = 1$ for $v \neq p$ and $x_p = y$. By composition we obtain an (injective) homomorphism $\mathbb{Q}_p^\times \to C_{\mathbb{Q}}$.

Corollary 4.1.9. *Let p be a prime, and $m \in \mathbb{Z}_{\geq 1}$ not divisible by p. Then the composite homomorphism*

$$\mathbb{Q}_p^\times \to C_{\mathbb{Q}} \xrightarrow{\psi} G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$$

maps any uniformizer of $\mathbb{Q}_p^\times$ *to the Frobenius at* p.

Proof. Let π be a uniformizer in $\mathbb{Q}_p^\times$, and let x be its image in $\mathbb{A}_{\mathbb{Q}}^\times$. Thus $x = (x_v)_v$ with $x_v = 1$ for $v \neq p$ and $x_p = \pi$. Let y be the element $p \in \mathbb{Q}^\times$ viewed as an element of $\mathbb{A}_{\mathbb{Q}}^\times$ via the diagonal embedding $\mathbb{Q}^\times \to \mathbb{A}_{\mathbb{Q}}^\times$. Then $y^{-1}x = (z_v)_v$ with $z_\infty = p^{-1} \in \mathbb{R}_{>0}$, $z_v = p^{-1} \in \mathbb{Z}_v^\times$ for $v \notin \{\infty, p\}$, and $z_p = p^{-1}\pi \in \mathbb{Z}_p^\times$. Hence $y^{-1}x \in \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times$. The composite map $\mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times \xrightarrow{\sim} C_{\mathbb{Q}} \to C_{\mathbb{Q}}/D_{\mathbb{Q}} \cong \widehat{\mathbb{Z}}^\times$ is just projection to the second factor. Hence the image of x under $\mathbb{A}_{\mathbb{Q}}^\times \to C_{\mathbb{Q}}/D_{\mathbb{Q}} \cong \widehat{\mathbb{Z}}^\times$ is the element whose component in $\mathbb{Z}_v^\times$ is p^{-1} for $v \neq p$ and whose component in $\mathbb{Z}_p^\times$ is $p^{-1}\pi$. The projection of this element in $(\mathbb{Z}/m\mathbb{Z})^\times$ is p^{-1}. Thus the corollary follows from Proposition 4.1.4. □

In Proposition 4.2.5 below, we will see that the conclusion of the corollary (or just for almost all primes) uniquely characterizes ψ.

Now we discuss the local class field theory for $\mathbb{Q}_p$.

Theorem 4.1.10 (Local Kronecker–Weber theorem)**.** *We have* $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_{p,\mathrm{cycl}} = \bigcup_m \mathbb{Q}_p(\zeta_m)$.

To simplify notation we write K_m for $\mathbb{Q}_p(\zeta_m)$. Thus $G^{\mathrm{ab}}_{\mathbb{Q}_p} \cong \varprojlim_m \mathrm{Gal}(K_m/\mathbb{Q}_p)$. For each m, we write α_m for the canonical injection $\mathrm{Gal}(K_m/\mathbb{Q}_p) \to (\mathbb{Z}/m\mathbb{Z})^\times$. The main difference from the situation for $\mathbb{Q}$ is that α_m is not always an isomorphism.

Write $m = np^r$ where n is not divisible by p.

Fact 4.1.11. *The extension $K_n/\mathbb{Q}_p$ is unramified, and the extension $K_{p^r}/\mathbb{Q}_p$ is totally ramified.*

Clearly K_m is the compositum of K_n and K_{p^r}. It follows from the above fact that $K_n/\mathbb{Q}_p$ and $K_{p^r}/\mathbb{Q}_p$ are linearly disjoint. Hence $\mathrm{Gal}(K_m/\mathbb{Q}_p) \cong \mathrm{Gal}(K_n/\mathbb{Q}_p) \times \mathrm{Gal}(K_{p^r}/\mathbb{Q}_p)$. By Chinese Remainder Theorem we also have $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times$. The map $\alpha_m : \mathrm{Gal}(K_m/\mathbb{Q}_p) \to (\mathbb{Z}/m\mathbb{Z})^\times$ is compatible with the maps $\alpha_n : \mathrm{Gal}(K_n/\mathbb{Q}_p) \to (\mathbb{Z}/n\mathbb{Z})^\times$ and $\alpha_{p^r} : \mathrm{Gal}(K_{p^r}/\mathbb{Q}_p) \to (\mathbb{Z}/p^r\mathbb{Z})^\times$ with respect to the direct product decompositions.

Fact 4.1.12. *The map α_n sends the Frobenius to $p + n\mathbb{Z}$. In particular, $[K_n : \mathbb{Q}_p]$ is equal to the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$, and the image of α_n is the subgroup generated by p, denoted by $\langle p \rangle_{(\mathbb{Z}/n\mathbb{Z})^\times}$. The map α_{p^r} is an isomorphism.*

Define a map

$$j_m : \mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \to \mathrm{im}(\alpha_m) = \langle p \rangle_{(\mathbb{Z}/n\mathbb{Z})^\times} \times (\mathbb{Z}/p^r\mathbb{Z})^\times \subset (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times,$$

sending p^n to $p^n \in \langle p \rangle_{(\mathbb{Z}/n\mathbb{Z})^\times}$, and sending $x \in \mathbb{Z}_p^\times$ to the image of x^{-1} under the natural projection $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^r\mathbb{Z})^\times$. Then define

$$\psi_m : \mathbb{Q}_p^\times \xrightarrow{j_m} \mathrm{im}(\alpha_m) \xrightarrow{\alpha_m^{-1}} \mathrm{Gal}(K_m/\mathbb{Q}_p).$$

The maps ψ_m are continuous, and they form a compatible family. We therefore obtain a continuous homomorphism

$$\psi : \mathbb{Q}_p^\times \to \varprojlim_m \mathrm{Gal}(K_m/\mathbb{Q}_p) \cong G^{\mathrm{ab}}_{\mathbb{Q}_p}.$$

This is called the *local Artin map* for $\mathbb{Q}_p$.

The local Artin map satisfies various deep properties. We state only two which are relatively straightforward.

For the first property, recall that the maximal unramified extension $\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p$ is an abelian extension and there are canonical isomorphisms $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}$, where the topological generator $1 \in \widehat{\mathbb{Z}}$ corresponds to the Frobenius. We therefore have a canonical quotient map $G^{\mathrm{ab}}_{\mathbb{Q}_p} \to \widehat{\mathbb{Z}}$, which we denote by ord.

Fact 4.1.13. *The following diagram commutes:*

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[r, "\psi"] \arrow[d, "\mathrm{ord}_p"] & G^{\mathrm{ab}}_{\mathbb{Q}_p} \arrow[d, "\mathrm{ord}"] \\
\mathbb{Z} \arrow[r] & \widehat{\mathbb{Z}}
\end{tikzcd}$$

The second property is the so-called *Local Global Compatibility*. Fix a prime p. For each $m \in \mathbb{Z}_{\geq 1}$ and each place $\mathfrak{p}$ of $\mathbb{Q}(\zeta_m)$ above p, the field $\mathbb{Q}(\zeta_m)_{\mathfrak{p}}$ is the compositum of its subfields $\mathbb{Q}_p$ and $\mathbb{Q}(\zeta_m)$ (cf. Exercise 1.6.6 (1)). Thus $\mathbb{Q}(\zeta_m)_{\mathfrak{p}} \cong \mathbb{Q}_p(\zeta_m)$. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)_{\mathfrak{p}}/\mathbb{Q}_p)$ is canonically identified with the decomposition group $D(\mathbb{Q}(\zeta_m)/p) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. We thus obtain a map $i_m : \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. It is independent of the choice of $\mathfrak{p}$ by commutativity. The maps i_m for varying m form a morphism between the two inverse systems. Hence we obtain a map

$$i : G_{\mathbb{Q}_p}^{\mathrm{ab}} \to G_{\mathbb{Q}}^{\mathrm{ab}}.$$

Fact 4.1.14 (Local-Global compatibility)**.** *The following diagram commutes:*

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[r, "\psi"] \arrow[d] & G_{\mathbb{Q}_p}^{\mathrm{ab}} \arrow[d, "i"] \\
\mathbb{A}_{\mathbb{Q}}^\times \arrow[r, "\psi"] & G_{\mathbb{Q}}^{\mathrm{ab}}.
\end{tikzcd}$$

4.2. **Global class field theory.** Let K be a global field.

Theorem 4.2.1 (Reciprocity Law)**.** *There is a continuous homomorphism $\psi_K : C_K \to G_K^{\mathrm{ab}}$ with dense image, called the* global Artin map*, satisfying the following properties. For each finite abelian extension L/K, write $\psi_{L/K}$ for the composite map $C_K \xrightarrow{\psi_K} G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$.*

(1) *For each $v \in V_K$, consider the composite map $f_v : K_v^\times \to C_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K)$. If v is non-archimedean, then f_v kills $\mathcal{O}_{K_v}^\times$ if and only v is unramified in L. When this holds, f_v sends any uniformizer to $\mathrm{Frob}_v \in \mathrm{Gal}(L/K)$. If v is archimedean and unramified in L (i.e., either v is complex or every place of L above v is real), then $f_v = 1$. If v is archimedean and ramifies in L (i.e., v is real and every place of L above v is complex) then f_v factors through the sign map $K_v^\times = \mathbb{R}^\times \to \{\pm 1\}$ and sends -1 to the complex conjugation in $\mathrm{Gal}(L/K)$ arising from a complex embedding $L \hookrightarrow \mathbb{C}$ corresponding to a complex place above v.*

(2) *The map $\psi_{L/K}$ is surjective, and its kernel is $\mathrm{N}_{L/K}(C_L)$.*

Remark 4.2.2. By Lemma 4.2.6, condition (1) for almost all places $v \in V_K$ already uniquely characterizes $\psi_{L/K}$. Hence ψ is unique.

Remark 4.2.3. The surjectivity of $\psi_{L/K}$ follows from the property that ψ_K has dense image. By (2), for every finite abelian extension L/K, the subgroup $\mathrm{N}_{L/K}(C_L) \subset C_K$ is open and of finite index. This is highly non-trivial.

Theorem 4.2.4 (Existence Theorem)**.** *A subgroup of C_K is open and of finite index if and only if it is of the form $\mathrm{N}_{L/K}(C_L)$ for a finite abelian extension L/K.*

Theorems 4.2.1 and 4.2.4 are the two main theorems of global class field theory.

We now show that a weaker version of condition (1) in Theorem 4.2.1 already uniquely characterizes ψ_K:

Proposition 4.2.5. *Let L/K be a finite abelian extension of global fields. Let ϕ, ϕ' be two continuous homomorphisms $C_K \to \mathrm{Gal}(L/K)$. Assume that there is a finite subset $S \subset V_K$ containing all archimedean places and all places which ramify in L such that for all $v \in V_K - S$, the composite maps $K_v^\times \to C_K \xrightarrow{\phi} \mathrm{Gal}(L/K)$ and $K_v^\times \to C_K \xrightarrow{\phi'} \mathrm{Gal}(L/K)$ both send every uniformizer to Frob_v. Then $\phi = \phi'$. In particular, the global Artin map $\psi_K : C_K \to G_K^{\mathrm{ab}}$ is unique.*

The key to the proof is the following lemma.

Lemma 4.2.6. *Let K be a global field, and let S be a finite subset of V_K. Then the subgroup $(\mathbb{A}_K^S)^\times = \{x \in \mathbb{A}_K^\times \mid x_v = 1,\ \forall v \in S\}$ of $\mathbb{A}_K^\times$ has dense image in C_K.*

Remark 4.2.7. The notation $(\mathbb{A}_K^S)^\times$ is justified as follows: Define $\mathbb{A}_K^S$ to be the restricted product of K_v for $v \notin S$, and define $(\mathbb{A}_K^S)^\times$ to be its group of invertible elements, equipped with the subspace topology via $(\mathbb{A}_K^S)^\times \to \mathbb{A}_K^S \times \mathbb{A}_K^S, x \mapsto (x, x^{-1})$. Then as a topological group $(\mathbb{A}_K^S)^\times$ is the restricted product of $K_v^\times$ for $v \notin S$. Moreover, the natural bijection between $(\mathbb{A}_K^S)^\times$ defined this way and the subgroup of $\mathbb{A}_K^\times$ in Lemma 4.2.6 (with the subspace topology inherited from $\mathbb{A}_K^\times$) is a topological isomorphism.

Proof of Lemma 4.2.6. It suffices to prove that for any $x \in \mathbb{A}_K^\times$ and any open neighborhood U of x, we have $U \cap (K^\times \cdot (\mathbb{A}_K^S)^\times) \neq \emptyset$. Up to shrinking U, we may assume that $U = \prod_{v\in T} U_v \times \prod_{v\notin T} \mathcal{O}_{K_v}^\times$, where T is a finite subset of V_K containing S, and each U_v is an open neighborhood of x_v in $K_v^\times$. By Strong Approximation (Theorem 3.7.1), there exists $y \in K$ such that $y \in K_v$ lies in U_v for each $v \in T$. (This is merely a very weak consequence of Strong Approximation.) In particular $y \neq 0$. Define $z = (z_v) \in \mathbb{A}_K^\times$ by $z_v = y$ for $v \in T$ and $z_v = 1$ for $v \notin T$. Then $y^{-1} z \in (\mathbb{A}_K^T)^\times \subset (\mathbb{A}_K^S)^\times$, and $z \in U$. Hence $z \in U \cap (K^\times \cdot (\mathbb{A}_K^S)^\times)$. □

Proof of Proposition 4.2.5. We claim that for $x \in (\mathbb{A}_K^S)^\times$, we have

$$\phi(x) = \phi'(x) = \prod_{v \in V_K - S} \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)}$$

(where the product is finite). The proposition then follows from the claim and Lemma 4.2.6. Let $T \subset V_K$ be a finite subset containing S such that $x_v \in \mathcal{O}_{K_v}^\times$ for all $v \notin T$ and such that $\prod_{v\in T}\{1\} \times \prod_{v \in V_K - T} \mathcal{O}_{K_v}^\times$ is contained in $\ker(\phi) \cap \ker(\phi')$ (which can be arranged since $\ker(\phi)$ and $\ker(\phi')$ are open subgroups of C_K). For each v, write i_v for the map $K_v^\times \to C_K$. Then the two elements x and $\prod_{v \in T-S} i_v(x_v)$ in C_K differ by an element of $\ker(\phi) \cap \ker(\phi')$. Hence

$$\phi(x) = \phi(\prod_{v\in T-S} i_v(x_v)) = \prod_{v \in T-S} \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)} = \prod_{v\in V_K - S} \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)},$$

and the same computation holds for ϕ'. □

As a consequence of Theorems 4.2.1 and 4.2.4, we have a classification of finite abelian extensions of K.

Corollary 4.2.8 (Classification of finite abelian extensions)**.** *The map*

$$\{\textit{finite abelian extensions } L/K \textit{ in } K^s\} \to \{\textit{open finite index subgroups of } C_K\},$$

sending L to $\mathrm{N}_{L/K}(C_L)$ is an inclusion-reversing bijection.

Proof. The map is surjective by Theorem 4.2.4. Injectivity and the inclusion-reversing property follow from the following claim: For finite abelian extensions L and L' of K in K^s, we have $L \subset L'$ if and only if $\mathrm{N}_{L'/K}(C_{L'}) \subset \mathrm{N}_{L/K}(C_L)$. The "only if" direction follows from the transitivity of norms: The composition

$$C_{L'} \xrightarrow{\mathrm{N}_{L'/L}} C_L \xrightarrow{\mathrm{N}_{L/K}} C_K$$

is equal to $\mathrm{N}_{L'/K}$. We now show the "if" direction. Let $M = LL' \subset K^{\mathrm{ab}}$. This is a finite abelian extension of K. We have a commutative diagram

$$\begin{tikzcd}
 & \mathrm{Gal}(M/K) \arrow[d, "\mathrm{restr}"'] \arrow[rdd, "\mathrm{restr}"] & \\
C_K \arrow[ru, "\psi_{M/K}"] \arrow[r, "\psi_{L/K}"] \arrow[rrd, "\psi_{L'/K}"'] & \mathrm{Gal}(L/K) & \\
 & & \mathrm{Gal}(L'/K)
\end{tikzcd}$$

By Theorem 4.2.1(2), all the arrows are surjective. By Theorem 4.2.1(2) and our assumption, $\ker(\psi_{L'/K}) \subset \ker(\psi_{L/K})$. Therefore we have

$$\ker(\mathrm{Gal}(M/K) \to \mathrm{Gal}(L'/K)) \subset \ker(\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)).$$

By Galois theory we conclude that $L \subset L'$. □

4.3. **Further information on the global Artin map.** The global Artin map $\psi_K : C_K \to G_K^{\mathrm{ab}}$ is not an isomorphism. However, it induces a topological isomorphism

$$C_K/D_K \xrightarrow{\sim} G_K^{\mathrm{ab}}$$

when K is a number field, and a topological isomorphism

$$C_K \xrightarrow{\sim} W_K^{\mathrm{ab}}$$

when K is a global function field and W_K^{ab} is the Weil group inside G_K^{ab} which we will define. We prove these statements using Theorems 4.2.1 and 4.2.4.

Proposition 4.3.1. *If K is a number field, then $\psi_K : C_K \to G_K^{\mathrm{ab}}$ is surjective, its kernel is D_K, and it induces a topological isomorphism $C_K/D_K \xrightarrow{\sim} G_K^{\mathrm{ab}}$.*

Proof. Since D_K is connected and G_K^{ab} is totally disconnected, we have $D_K \subset \ker \psi_K$. Thus ψ_K induces a continuous homomorphism $C_K/D_K \to G_K^{\mathrm{ab}}$. By Proposition 3.10.4, C_K/D_K is profinite, so the image of ψ_K is closed. But this image is dense (which is stated in Theorem 4.2.1), so ψ_K is surjective. We now show that $\ker \psi_K = D_K$. By Theorem 4.2.1(2) and Theorem 4.2.4, $\ker \psi_K$ is contained in all open finite index subgroups of C_K. In particular D_K is also contained in all such subgroups. The image of any open finite index subgroup of C_K in C_K/D_K is an open subgroup of C_K/D_K, and conversely the inverse image of any open subgroup of C_K/D_K is an open finite index subgroup of C_K (since C_K/D_K is compact). Hence $\ker(\psi_K)/D_K$ is contained in all open subgroups of C_K/D_K. Since C_K/D_K is profinite, the intersection of all its open subgroups is trivial. Thus $\ker(\psi_K) = D_K$.

It follows that ψ_K induces a continuous bijective homomorphism $C_K/D_K \to G_K^{\mathrm{ab}}$. This must be a homeomorphism since both sides are Hausdorff. □

Exercise 4.3.2. If K is a number field, then every open subgroup of C_K is of finite index.

The situation with a global function field is more complicated. Let K be a global function field of characteristic p, and let k be the algebraic closure of $\mathbb{F}_p$ in K. Then k is a finite field. For every n, let k_n be the degree n extension of k. Let $K_n = K \otimes_k k_n$. This is a field extension of K. It is a Galois extension, and $\mathrm{Gal}(K_n/K) \cong \mathrm{Gal}(k_n/k) \cong \mathbb{Z}/n\mathbb{Z}$. Hence K_n/K is an abelian extension. We write Frob_k for the canonical generator of $\mathrm{Gal}(K_n/K)$ corresponding to the automorphism $x \mapsto x^{|k|}$ in $\mathrm{Gal}(k_n/k)$. As an automorphism of K_n, Frob_k is the map $k_n \otimes_K K \to k_n \otimes_K K, x \otimes y \mapsto x^{|k|} \otimes y$.

Lemma 4.3.3. *The extension K_n/K is unramified at every place $v \in V_K$. Moreover, $\mathrm{Frob}_v \in \mathrm{Gal}(K_n/K)$ is given by $\mathrm{Frob}_v = \mathrm{Frob}_k^{[k_v:k]}$, where k_v denotes the residue field at v.*

Proof. Let $v \in V_K$. Let $k' = k_v \cap k_n$. Fix a uniformizer $t \in K_v$. Then we have a canonical isomorphism $K_v \cong k_v(\!(t)\!)$. We have

$$K_n \otimes_K K_v \cong k_n \otimes_k k_v(\!(t)\!) \cong k_n \otimes_k k' \otimes_{k'} k_v(\!(t)\!) \cong k_n^{\oplus[k':k]} \otimes_{k'} k_v(\!(t)\!) \cong \big(k_n \otimes_{k'} k_v(\!(t)\!)\big)^{\oplus[k':k]}.$$

It is easy to see that $k_n \otimes_{k'} k_v$ is a field, and we have $k_n \otimes_{k'} k_v(\!(t)\!) \cong (k_n \otimes_{k'} k_v)(\!(t)\!)$, which is a local field and an unramified extension of $k_v(\!(t)\!)$. Hence v is unramified in K_n in view of Fact 1.4.3. More precisely, for every place w of K_n above v, we have $K_{n,w} \cong (k_n \otimes'_k k_v)(\!(t)\!)$.

Now a general element $\mathrm{Frob}_k^i \in \mathrm{Gal}(K_n/K) \cong \mathrm{Gal}(k_n/k)$ belongs to the decomposition group $D(K_n/v)$ if and only if it acts trivially on $k' \subset k_n$. In this case, Frob_k^i induces the automorphism $x \otimes y \mapsto x^{|k|^i} \otimes y$ on the residue field $k_n \otimes_{k'} k_v$ of every place of K_n above v. Thus $\mathrm{Frob}_v = \mathrm{Frob}_k^i$ if and only if

$$\begin{cases} x^{|k|^i} = x, \quad \forall x \in k'; \\ x^{|k_v|} \otimes y^{|k_v|} = x^{|k|^i} \otimes y, \quad \forall x \otimes y \in k_n \otimes_{k'} k_v. \end{cases}$$

This holds if and only if $i \equiv [k_v : k] \pmod n$. Hence we have $\mathrm{Frob}_v = \mathrm{Frob}_k^{[k_v:k]}$. □

Lemma 4.3.4. *The image of $\|\cdot\| : \mathbb{A}_K^\times \to \mathbb{R}_{>0}$ is $|k|^{\mathbb{Z}}$. We have a commutative diagram*

$$\begin{tikzcd} C_K \arrow[r, "\|\cdot\|"] \arrow[d, "\psi_K"] & {|k|^{\mathbb{Z}}} \arrow[d] & , \\ G_K^{\mathrm{ab}} \arrow[r] & \mathrm{Gal}(K_n/K) = \langle \mathrm{Frob}_k \rangle \cong \mathbb{Z}/n\mathbb{Z} & \end{tikzcd}$$

where the vertical map on the right sends $|k|^{-1}$ to Frob_k.

Proof. Since for each $v \in V_K$ we have $k_v \supset k$, the image of $\|\cdot\|$ is contained in $|k|^{\mathbb{Z}}$. Assume this image is $|k|^{r\mathbb{Z}}$ for some $r \in \mathbb{Z}_{\geq 1}$. By Lemma 4.3.3, the extension K_n/K is everywhere unramified. Hence by the proof of Proposition 4.2.5, for each $x \in \mathbb{A}_K^\times$ we have

$$\psi_{K_n/K}(x) = \prod_{v \in V_K} \mathrm{Frob}_v^{\mathrm{ord}_v(x_v)} \in \mathrm{Gal}(K_n/K).$$

By Lemma 4.3.3, the above formula becomes

$$\psi_{K_n/K}(x) = \prod_{v \in V_K} \mathrm{Frob}_k^{[k_v:k]\,\mathrm{ord}_v(x_v)}.$$

But $\psi_{K_n/K}$ is a surjection onto $\mathrm{Gal}(K_n/K)$, so there exists $v_0 \in V_K$ such that $[k_{v_0} : k] \equiv 1 \pmod n$. Then $|k|^{r\mathbb{Z}}$ contains $|k_{v_0}|^{\mathbb{Z}} = |k|^{[k_{v_0}:k]\mathbb{Z}}$. Hence r divides $[k_{v_0} : k]$, and so r is coprime to n. But this holds for all n, so $r = 1$.

To show the commutativity of the diagram, we simply compare the above formula for $\psi_{K_n/K}$ with the formula

$$\|x\| = \prod_{v \in V_K} |k_v|^{-\mathrm{ord}_v(x_v)} = \prod_{v \in V_K} |k|^{-[k_v:k]\,\mathrm{ord}_v(x_v)}.$$

□

We have $\mathrm{Gal}(\bigcup_n K_n/K) \cong \varprojlim_n \mathrm{Gal}(K_n/K) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}}$. Here the topological generator $1 \in \mathbb{Z} \subset \widehat{\mathbb{Z}}$ corresponds to $\mathrm{Frob}_k \in \varprojlim_n \mathrm{Gal}(K_n/K)$, i.e., the element whose image in each $\mathrm{Gal}(K_n/K)$ is Frob_k. We denote by ord the natural map

$$G_K^{\mathrm{ab}} \to \mathrm{Gal}(\bigcup_n K_n/K) \cong \widehat{\mathbb{Z}}.$$

This map also has the following alternative interpretation: The algebraic closure of k in K^{ab} is algebraically closed (because for each n we have $k_n \subset K_n \subset K^{\mathrm{ab}}$), and we denote it by $\bar{k}$. Thus $\mathrm{Gal}(\bar{k}/k) \cong \widehat{\mathbb{Z}}$, where 1 corresponds to Frob_k. The map ord is just the restriction map $G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(\bar{k}/k)$.

We also denote by ord the homomorphism $C_K \to \mathbb{Z}$ such that for each $x \in C_K, \|x\| = |k|^{-\mathrm{ord}(x)}$. Then by Lemma 4.3.4 we have a commutative diagram

$$\begin{tikzcd}
C_K \arrow[r, "\mathrm{ord}"] \arrow[d, "\psi_K"] & \mathbb{Z} \arrow[d, hook] \\
G_K^{\mathrm{ab}} \arrow[r, "\mathrm{ord}"] & \widehat{Z}
\end{tikzcd}.$$

In particular, $\psi_K(C_K)$ is contained in $\mathrm{ord}^{-1}(\mathbb{Z}) \subset G_K^{\mathrm{ab}}$.

Definition 4.3.5. The *abelianized Weil group* for a global function field K is the subgroup $\mathrm{ord}^{-1}(\mathbb{Z}) \subset G_K^{\mathrm{ab}}$. Let $I'_K = \mathrm{ord}^{-1}(0) \subset G_K^{\mathrm{ab}}$. We equip W_K^{ab} with the unique topology such that I'_K is open in W_K^{ab} and such that the subspace topology on I'_K inherited from W_K^{ab} agrees with the subspace topology inherited from G_K^{ab}.

Concretely, we can pick group-theoretic section $\mathbb{Z} \to W_K^{\mathrm{ab}}$ of $\mathrm{ord} : W_K^{\mathrm{ab}} \to \mathbb{Z}$. Then we obtain a group isomorphism $W_K^{\mathrm{ab}} \cong I'_K \times \mathbb{Z}$ (since W_K^{ab} is abelian). The topology on W_K^{ab} is such that this isomorphism is a homeomorphism, where the right hand side has the product topology, with I'_K having the subspace topology inherited from G_K^{ab} and $\mathbb{Z}$ having discrete topology. From this we also see that the topology on W_K^{ab} makes it a topological group.

Exercise 4.3.6. The inclusion map $W_K^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ is continuous and has dense image, but it is not a homeomorphism onto the image.

Exercise 4.3.7. Denote the composite map $G_K = \mathrm{Gal}(K^s/K) \to G_K^{\mathrm{ab}} \xrightarrow{\mathrm{ord}} \widehat{\mathbb{Z}}$ also by ord. Let $W_K = \mathrm{ord}^{-1}(\mathbb{Z}) \subset G_K$ and $I_K = \mathrm{ord}^{-1}(\mathbb{Z}) \subset G_K$. Fix a set-theoretic section $\mathbb{Z} \to W_K$ of ord and thereby obtain a bijection $W_K \cong I_K \times \mathbb{Z}$. Equip W_K with the topology such that this bijection is a homeomorphism, with I_K having the subspace topology inherited from G_K and $\mathbb{Z}$ having the discrete topology. Show that this topology on W_K is independent of the choice of the section. Show that W_K is a topological group. Show that W_K^{ab} is naturally identified with the abelianization of W_K as a topological group (i.e., W_K modulo the closure of the derived subgroup).

We then have a commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & C_K^1 \arrow[r] \arrow[d, "\psi_K"] & C_K \arrow[r, "\mathrm{ord}"] \arrow[d, "\psi_K"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
1 \arrow[r] & I'_K \arrow[r] & W_K^{\mathrm{ab}} \arrow[r, "\mathrm{ord}"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Proposition 4.3.8. *The maps $\psi_K : C_K \to W_K^{\mathrm{ab}}$ and $\psi_K : C_K^1 \to I_K'$ are topological isomorphisms.*

Proof. Fix a group-theoretic section $s : \mathbb{Z} \to C_K$ of $\mathrm{ord} : C_K \to \mathbb{Z}$. Use this to identify $C_K \cong C_K^1 \times \mathbb{Z}$ as topological groups. Note that $\psi_K \circ s : \mathbb{Z} \to W_K^{\mathrm{ab}}$ is a section of $\mathrm{ord} : W_K^{\mathrm{ab}} \to \mathbb{Z}$, and we use this to identify $W_K^{\mathrm{ab}} \cong I_K' \times \mathbb{Z}$ as topological groups. Under these identifications, the map $\psi_K : C_K \to W_K^{\mathrm{ab}}$ becomes $C_K^1 \times \mathbb{Z} \to I_K' \times \mathbb{Z}, (x, n) \mapsto (\psi_K(x), n)$. Thus it suffices to prove that $\psi_K : C_K^1 \to I_K'$ is a topological isomorphism. This map is continuous since $\psi_K : C_K^1 \to G_K^{\mathrm{ab}}$ is continuous and I_K' has the subspace topology in G_K^{ab}. Recall from Proposition 3.10.9 that C_K^1 is profinite. In particular it is compact. The group I_K' is Hausdorff. Hence it suffices to show that $\psi_K : C_K^1 \to G_K^{\mathrm{ab}}$ is a bijection.

To show injectivity, suppose $x \in C_K^1$ is such that $\psi_K(x) = 1$. By Theorem 4.2.1(2) and Theorem 4.2.4, x lies in every open finite index subgroup of C_K. Let U be an arbitrary open subgroup of C_K^1 (which is automatically of finite index). Then $U \times \mathbb{Z} \subset C_K^1 \times \mathbb{Z} \cong C_K$ is an open finite index subgroup of C_K, so it must contain x. It follows that $x \in U$. Since U is arbitrary and C_K^1 is profinite, we conclude that $x = 1$. This proves injectivity.

It remains to prove the surjectivity of $\psi_K : C_K^1 \to I_K'$. Let $g \in I_K'$. Since $\psi_K : C_K \to G_K^{\mathrm{ab}}$ has dense image, there is a sequence $(x_n)_{n \geq 1} \subset C_K$ such that $\psi_K(x_n) \to g$ in G_K^{ab}. Thus $\mathrm{ord}(x_n) = \mathrm{ord}(\psi_K(x_n)) \to \mathrm{ord}(g) = 0$ in $\widehat{\mathbb{Z}}$. This means for any $m \in \mathbb{Z}_{\geq 1}$, for all sufficiently large n the integer $\mathrm{ord}(x_n)$ is divisible by m. Let $y \in C_K$ be such that $\mathrm{ord}(y) = 1$. We claim that $\psi_K(y^{-\mathrm{ord}(x_n)}) \to 1$ in G_K^{ab}. Since G_K^{ab} is profinite, we only need to show that for any open subgroup U of G_K^{ab}, the image of $\psi_K(y^{-\mathrm{ord}(x_n)})$ in G_K^{ab}/U is trivial for all sufficiently large n. This is true since for all sufficiently large n, the order $|G_K^{\mathrm{ab}}/U|$ divides $\mathrm{ord}(x_n)$, and $\psi_K(y^{-\mathrm{ord}(x_n)}) = \psi_K(y^{-1})^{\mathrm{ord}(x_n)}$.

By the claim, we have $\psi_K(x_n y^{-\mathrm{ord}(x_n)}) \to g$ in G_K^{ab}. Since each $x_n y^{-\mathrm{ord}(x_n)}$ lies in C_K^1, this implies that g lies in the closure of $\psi_K(C_K^1)$ in G_K^{ab}. But C_K^1 is compact, so $\psi_K(C_K^1)$ is closed in G_K^{ab}. This proves the surjectivity. □

4.4. **Functoriality of the global Artin map.** Let L/K be a finite separable extension of global fields. Choose a K-isomorphism $L^s \cong K^s$, and thereby identify $G_L = \mathrm{Gal}(L^s/L)$ with an open subgroup of $G_K = \mathrm{Gal}(K^s/K)$. The inclusion $G_L \hookrightarrow G_K$ induces a continuous homomorphism $i : G_L^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$, which is independent of all choices.

Theorem 4.4.1 (Norm functoriality)**.** *We have a commutative diagram*

$$\begin{tikzcd}
C_L \arrow[r, "\psi_L"] \arrow[d, "\mathrm{N}_{L/K}"] & G_L^{\mathrm{ab}} \arrow[d, "i"] \\
C_K \arrow[r, "\psi_K"] & G_K^{\mathrm{ab}}
\end{tikzcd}$$

The second form of functoriality involves a *transfer map* $V : G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$. We first define it for groups without topology.

Let G be an abstract group (without topology) and H a finite index subgroup of G. We will define a canonical homomorphism $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$, called the *transfer map*. The most natural origin of this map is the *restriction map* $\mathbf{H}_1(G, \mathbb{Z}) \to \mathbf{H}_1(H, \mathbb{Z})$ between group homology. The two homology groups are canonically identified with G^{ab} and H^{ab} respectively. Here we define V by hand as follows.

Choose a set theoretic section $\theta : H\backslash G \to G$ of the projection $G \to H\backslash G$. For each $g \in G$ and $t \in H\backslash G$, we have $\theta(t)g \in H\theta(tg)$ tautologically. Hence there is a unique element

$x_{t,g} \in H$ such that

$$\theta(t)g = x_{t,g}\theta(tg).$$

Define a map

$$\tilde{V} : G \to H, \quad g \mapsto \prod_{t \in H\backslash G} x_{t,g}.$$

We check that the composition of $\tilde{V}$ with $H \to H^{\mathrm{ab}}$ is a group homomorphism, and therefore $\tilde{V}$ induces a group homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. For $g_1, g_2 \in G$, we have

$$\theta(t)g_1g_2 = x_{t,g_1}\theta(tg_1)g_2 = x_{t,g_1}x_{tg_1,g_2}\theta(tg_1g_2).$$

Hence

$$x_{t,g_1g_2} = x_{t,g_1}x_{tg_1,g_2}.$$

Therefore, inside H^{ab}, we have

$$\begin{aligned}\tilde{V}(g_1g_2) = \prod_{t \in H\backslash G} x_{t,g_1}x_{tg_1,g_2} &= \left(\prod_{t \in H\backslash G} x_{t,g_1}\right) \cdot \left(\prod_{t \in H\backslash G} x_{tg_1,g_2}\right) \\ &= \left(\prod_{t \in H\backslash G} x_{t,g_1}\right) \cdot \left(\prod_{t \in H\backslash G} x_{t,g_2}\right) = \tilde{V}(g_1)\tilde{V}(g_2).\end{aligned}$$

Hence $\tilde{V}$ induces a group homomorphism $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

Exercise 4.4.2. The homomorphism $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is independent of the choice of θ.

Now suppose G is a topological group and H is an open subgroup of G of finite index. The map $\tilde{V} : G \to H$ constructed above is automatically continuous. The same computation as above shows that the composition of $\tilde{V}$ with $H \to H^{\mathrm{ab}}$, where H^{ab} is the abelianization as a topological group (i.e. H modulo the closure of the derived subgroup) is a homomorphism. It is therefore a continuous homomorphism, and induces a continuous homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

Exercise 4.4.3. Verify that $\tilde{V} : G \to H$ is continuous.

Applying the above construction to the open subgroup (of finite index) $G_L \subset G_K$, we obtain the transfer map $V : G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$.

Theorem 4.4.4. *[Transfer functoriality] We have a commutative diagram*

$$\begin{tikzcd}
C_L \arrow[r, "\psi_L"] & G_L^{\mathrm{ab}} \\
C_K \arrow[u, hook] \arrow[r, "\psi_K"] & G_K^{\mathrm{ab}} \arrow[u, "V"]
\end{tikzcd}$$

where the vertical map on the left is the closed embedding induced by $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_L^\times$ (see Proposition 3.9.4).

4.5. **Local class field theory.** Let K be a non-archimedean local field, with residue field k. The following two theorems are the main theorems of local class field theory.

Theorem 4.5.1 (Local Reciprocity Law)**.** *There is a continuous homomorphism $\psi_K : K^\times \to G_K^{\mathrm{ab}}$ with dense image, called the* local Artin map*, satisfying the following conditions:*

(1) *For each finite unramified extension L/K, the composition $\psi_{L/K} : K^\times \xrightarrow{\psi_K} G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$ sends every uniformizer in $K^\times$ to the Frobenius element in $\mathrm{Gal}(L/K)$.*
(2) *For each finite abelian extension L/K, the composition the composition $\psi_{L/K} : K^\times \xrightarrow{\psi_K} G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$ is surjective and its kernel is $\mathrm{N}_{L/K}(L^\times)$.*

Remark 4.5.2. It follows that $\mathrm{N}_{L/K}(L^\times)$ as above is open and of finite index in $K^\times$.

Theorem 4.5.3 (Local Existence Theorem)**.** *A subgroup of $K^\times$ is open and of finite index if and only if it is of the form $\mathrm{N}_{L/K}(L^\times)$ for a finite abelian extension L/K.*

Corollary 4.5.4 (Classification of finite abelian extensions)**.** *The map*

$$\{\textit{finite abelian extensions } L/K \textit{ in } K^s\} \to \{\textit{open finite index subgroups of } K^\times\},$$

sending L to $\mathrm{N}_{L/K}(L^\times)$ is an inclusion-reversing bijection.

Proof. This follows from Theorems 4.5.1 and 4.5.3, by the same argument as in the proof of Corollary 4.2.8. □

Proposition 4.5.5. *Assume Corollary 4.5.4. Then the local Artin map ψ_K as in Theorem 4.5.1 is unique.*

Proof. Suppose ψ_K, ψ'_K are two Artin maps. Since $K^\times$ is generated by uniformizers as a group, it suffices to show that for any fixed uniformizer π, we have $\psi_K(\pi) = \psi'_K(\pi)$.

Let L/K be an arbitrary finite abelian extension. Then $\mathrm{N}_{L/K}(L^\times)$ is open and of finite index in $K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_L^\times$. It can be easily seen that any open and finite index subgroup of $\pi^{\mathbb{Z}} \times \mathcal{O}_L^\times$ contains a subgroup of the form $\pi^{n\mathbb{Z}} \times U_L^m$ for some $n, m \in \mathbb{Z}_{\geq 1}$. Note that $\pi^{n\mathbb{Z}} \times \mathcal{O}_K^\times$ and $\pi^{\mathbb{Z}} \times U_L^m$ are both open and of finite index in $K^\times$. Hence they are respectively of the form $\mathrm{N}_{E_n/K}(E_n^\times)$ and $\mathrm{N}_{K_{\pi,m}/K}(K_{\pi,m}^\times)$ for unique finite abelian extensions E_n/K and $K_{\pi,m}/K$. Thus we can find $n, m \in \mathbb{Z}_{\geq 1}$ such that

$$\mathrm{N}_{L/K}(L^\times) \supset \pi^{n\mathbb{Z}} \times U_L^m = \mathrm{N}_{E_n/K}(E_n^\times) \cap \mathrm{N}_{K_{\pi,m}/K}(K_{\pi,n}^\times).$$

The right hand side contains (in fact, equals, by the same proof as Corollary 4.2.8)

$$\mathrm{N}_{E_n \cdot K_{\pi,m}/K}((E_n \cdot K_{\pi,m})^\times).$$

Since the bijection in Corollary 4.5.4 is inclusion-reversing, we conclude that $L \subset E_n \cdot K_{\pi,m}$. Thus we have shown that

$$K^{\mathrm{ab}} = \bigcup_{n,m \geq 1} E_n \cdot K_{\pi,m}.$$

It remains to show that for each n and m, we have $\psi_{E_n/K}(\pi) = \psi'_{E_n/K}(\pi)$ and $\psi_{K_{\pi,m}/K}(\pi) = \psi'_{K_{\pi,m}/K}(\pi)$. Let K_n be the unique degree n unramified extension of K. It follows from Proposition 2.3.3 that $\mathrm{N}_{K_n/K}(K_n^\times) = \pi^{n\mathbb{Z}} \times \mathcal{O}_K^\times$. Hence by Corollary 4.5.4 we have $K_n = E_n$. Then since ψ_K and ψ'_K both satisfy condition (1) in Theorem 4.5.1, we have $\psi_{E_n/K}(\pi) = \psi'_{E_n/K}(\pi) = \mathrm{Frob} \in \mathrm{Gal}(K_n/K)$. Since $\pi \in \mathrm{N}_{K_{\pi,n}/K}(K_{\pi,n}^\times)$, and since ψ_K and ψ'_K both satisfy condition (2) in Theorem 4.5.1, we have $\psi_{K_{\pi,m}/K}(\pi) = \psi'_{K_{\pi,m}/K}(\pi) = 1$. □

Remark 4.5.6. This proof of uniqueness of ψ_K relies on Corollary 4.5.4, which relies on Theorem 4.5.3. This is unlike the global case, where the uniqueness of the global Artin map could be proved unconditionally.

Similar to the global function field case, we define $\mathrm{ord} : G_K^{\mathrm{ab}} \to \mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \widehat{\mathbb{Z}}$, where $1 \in \mathbb{Z}$ corresponds to the Frobenius. Define $W_K^{\mathrm{ab}} \subset G_K^{\mathrm{ab}}$ to be the inverse image of $\mathbb{Z}$ under ord, and define $I'_K \subset G_K^{\mathrm{ab}}$ to be the kernel of ord. Equip W_K^{ab} with the topology such that I'_K is open and I'_K has the subspace topology inherited from G_K^{ab}.

Proposition 4.5.7. *We have a commutative diagram with exact rows, and the vertical maps are topological isomorphisms:*

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\psi_K"] & K^\times \arrow[r, "\mathrm{ord}"] \arrow[d, "\psi_K"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
1 \arrow[r] & I'_K \arrow[r] & W_K^{\mathrm{ab}} \arrow[r, "\mathrm{ord}"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Proof. This follows from the two main theorems Theorem 4.5.1 and Theorem 4.5.3, in the same way as Proposition 4.3.8. □

Similar to the global Artin map, the local Artin map satisfies norm and transfer functoriality.

Theorem 4.5.8 (Norm and transfer functoriality)**.** *Let L/K be a finite separable extension. Then we have a commutative diagram*

$$\begin{tikzcd}
L^\times \arrow[r, "\psi_L"] \arrow[d, "\mathrm{N}_{L/K}"] & G_L^{\mathrm{ab}} \arrow[d, "i"] \\
K^\times \arrow[r, "\psi_K"] & G_K^{\mathrm{ab}}
\end{tikzcd}$$

where i is induced by the inclusion $G_L \hookrightarrow G_K$. We have a commutative diagram

$$\begin{tikzcd}
L^\times \arrow[r, "\psi_L"] & G_L^{\mathrm{ab}} \\
K^\times \arrow[r, "\psi_K"] \arrow[u, hook] & G_K^{\mathrm{ab}} \arrow[u, "V"']
\end{tikzcd}$$

where V is the transfer map.

Finally, we state the local-global compatibility of Artin maps. Let K be a global field, and v a non-archimedean place of K. As before, if we choose a K-algebra embedding $i : K^s \hookrightarrow (K_v)^s$, then we obtain a closed embedding $G_{K_v} \hookrightarrow G_K$, whose image is the decomposition group of the place of K^s over v determined by i. The induced map $G_{K_v}^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ is independent of the choice of i.

Theorem 4.5.9 (Local-global compatibility)**.** *We have a commutative diagram*

$$\begin{tikzcd}
K_v^\times \arrow[r, "\psi_{K_v}"] \arrow[d, hook] & G_{K_v}^{\mathrm{ab}} \arrow[d] \\
C_K \arrow[r, "\psi_K"] & G_K^{\mathrm{ab}}.
\end{tikzcd}$$

4.6. **Lubin-Tate theory.** Let K be a non-archimedean local field. Fix a uniformizer π. For each $n \in \mathbb{Z}_{\geq 1}$, Lubin–Tate theory explicitly constructs a finite abelian extension $K_{\pi,n}/K$ (which is actually equal to $K_{\pi,n}$ in the proof of Proposition 4.5.5), together with an explicit isomorphism $\alpha_n : \mathcal{O}_K^\times / U_K^n \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,n}/K)$. For instance, for $K = \mathbb{Q}_p$ and $\pi = p$, we have $K_{\pi,n} = \mathbb{Q}_p(\zeta_{p^n})$, and α_n is the usual isomorphism $(\mathbb{Z}/p^n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$. For $n|n'$, we have $K_{\pi,n} \subset K_{\pi,n'}$. The α_n are compatible for varying n, and in the inverse limit we obtain a topological isomorphism $\alpha : \mathcal{O}_K^\times \xrightarrow{\sim} \mathrm{Gal}(K_\pi/K)$, where $K_\pi := \bigcup_n K_{\pi,n}$.

Each $K_{\pi,n}$ is totally ramified over K, and hence linearly disjoint from any unramified extension of K. Thus we have

$$\mathrm{Gal}(K^{\mathrm{ur}} \cdot K_\pi/K) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_\pi/K).$$

This allows us to define

$$\begin{aligned} \psi_K^{\mathrm{LT}} : K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times &\to \mathrm{Gal}(K^{\mathrm{ur}} \cdot K_\pi/K) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_\pi/K) \\ (\pi^r, x) &\mapsto (\mathrm{Frob}^r, \alpha(x^{-1})). \end{aligned}$$

Assume Theorem 4.5.1, i.e., the existence of an (abstract) local Artin map ψ_K. We will use Lubin-Tate theory to prove the following:

- Local Kronecker–Weber: $K^{\mathrm{ur}} \cdot K_\pi = K^{\mathrm{ab}}$.
- The map $\psi_K^{\mathrm{LT}} : K^\times \to G_K^{\mathrm{ab}}$ (here the target is G_K^{ab} by the above statement) is independent of π, and it is equal to the abstract ψ_K. (In particular, this proves the uniqueness of ψ_K, and gives an explicit description of ψ_K.)
- Theorem 4.5.3.

We need the notion of a formal group law. This can be motivated in two ways. First, suppose we have a Lie group (or a group object in any reasonable geometric setting, such as a group variety over a field), and suppose we fix local coordinates near the identity element such that the identity element has coordinate 0. If the group is "analytic", then the multiplication operation for elements sufficiently close to the identity, can be described in terms of their coordinates by power series. In other words, if $t(g)$ is the coordinate of a group element g, then $t(gh)$ is a (vector-valued) power series in $t(g)$ and $t(h)$, at least for g, h sufficiently close to the identity. This power series must satisfy some algebraic properties reflecting the axioms for a group.

As a second motivation, consider $\Lambda = \{x \in \overline{K} \mid |x| < 1\}$. Note that for any $F(X,Y) \in \mathcal{O}_K[\![X,Y]\!]$, and any $x, y \in \Lambda$, the power series $F(x,y)$ converges in Λ. Thus we can define a group structure on Λ by $(x,y) \mapsto F(x,y)$ as long as $F(X,Y)$ satisfies suitable axioms.

Definition 4.6.1. Let R be a commutative ring. A (one-dimensional, commutative) *formal group law* F over R is a formal power series $F(X,Y) \in R[\![X,Y]\!]$ satisfying the following conditions:

(1) (Deforming standard addition.) $F(X,Y) \equiv X + Y \mod (X,Y)^2$.
(2) (Commutativity.) $F(X,Y) = F(Y,X)$.
(3) (Associativity.) $F(X, F(Y,Z)) = F(F(X,Y), Z) \in R[\![X,Y,Z]\!]$. (Here the substitutions make sense because F has no constant term.)

Exercise 4.6.2. Let F be a formal group law. Then $F(X,0) = F(0,X) = X$ (i.e., "0 is the zero element"), and there exists a unique $i(X) \in R[\![X]\!]$ ("the inversion operation") such that $i(X) \equiv -X \mod (X^2)$ and $F(X, i(X)) = 0$.

Example 4.6.3. The additive group $\mathbb{G}_a$ is given by $F(X,Y) = X + Y$. The multiplicative group $\mathbb{G}_m$ is given by $F(X,Y) = (1+X)(1+Y) - 1 = X + Y + XY$. (Think of X

as the coordinate of a group element $1 + X$, on which the group operation is the usual multiplication.)

Definition 4.6.4. Let F, G be formal group laws over R. By a *homomorphism* $f : F \to G$, we mean an element $f(X) \in R[\![X]\!]$ such that $f(0) = 0$ and $G(f(X), f(Y)) = f(F(X,Y))$. For two homomorphisms $f_1, f_2 : F \to G$, their sum is defined as

$$f_1 +_G f_2 := G(f_1(X), f_2(X)).$$

This is another homomorphism $F \to G$. For homomorphisms $f : F \to G$ and $g : G \to H$, define their composition

$$g \circ f := g(f(X)).$$

This is a homomorphism $F \to H$.

Under this definition of homomorphisms and their compositions, we obtain the category of formal group laws over R. In particular, we obtain a notion of isomorphism.

Exercise 4.6.5. A homomorphism $f : F \to G$ between formal group laws over R is an isomorphism if and only if $f'(0) \in R$ lies in $R^\times$.

For a formal group law F, the set of endomorphisms $\mathrm{End}(F)$ is a ring, where multiplication is composition and addition is $(f_1, f_2) \mapsto f_1 +_F f_2$.

Exercise 4.6.6. Check that $\mathrm{End}(F)$ is indeed a ring.

Definition 4.6.7. Let R_0 be a subring of R. By a *formal R_0-module over R*, we mean a pair $(F, [\cdot]_F)$, where F is a formal group law over R, and $[\cdot]_F$ is a ring homomorphism $R_0 \to \mathrm{End}(F)$ such that for every $a \in R_0$, we have $[a]_F(X) \equiv aX \mod (X^2)$.

Let K be a non-archimedean local field. Fix a uniformizer π. Let the residue field be $\mathbb{F}_q$.

Definition 4.6.8. A *Lubin–Tate formal group law* with respect to (K, π) is a formal $\mathcal{O}_K$-module $(F, [\cdot]_F)$ over $\mathcal{O}_K$ such that $[\pi]_F(X) \equiv X^q \mod \mathfrak{m}_K$. (Here we say two formal power series over $\mathcal{O}_K$ are congruent modulo $\mathfrak{m}_K$ if they are coefficient-wise congruent.)

Example 4.6.9. Let $K = \mathbb{Q}_p$ and $\pi = p$. We define a formal $\mathbb{Z}_p$-module over $\mathbb{Z}_p$ as follows. The underlying formal group is $\mathbb{G}_m$, i.e., $F(X,Y) = (1+X)(1+Y) - 1$. For $a \in \mathbb{Z}_p$, define

$$[a]_F = (1+X)^a - 1 := \sum_{n \geq 1} \binom{a}{n} X^n.$$

Here, $\binom{a}{n}$ is defined to be $a(a-1)\cdots(a-n+1)/n!$. As a function in a, this is a continuous function $\mathbb{Z}_p \to \mathbb{Q}_p$. Since it takes $\mathbb{Z}$ into $\mathbb{Z}$, it takes $\mathbb{Z}_p$ into $\mathbb{Z}_p$. Thus $[a]_F \in \mathbb{Z}_p[\![X]\!]$. One checks that $[\cdot]_F$ makes F a formal $\mathbb{Z}_p$-module over $\mathbb{Z}_p$. We have $[p]_F = (1+X)^p - 1 \equiv X^p \mod p$, so $(F, [\cdot]_F)$ is a Lubin-Tate formal group law.

Exercise 4.6.10. In the above example, check that $[\cdot]_F$ makes F a formal $\mathbb{Z}_p$-module over $\mathbb{Z}_p$.

Remark 4.6.11. If $F \in \mathcal{O}_K[\![X,Y]\!]$ is a formal group law over $\mathcal{O}_K$ and $e \in \mathcal{O}_K[\![X]\!]$ is an endomorphism of F, then $(F \mod \mathfrak{m}_K) \in \mathbb{F}_q[\![X,Y]\!]$ is a formal group law over $\mathbb{F}_q$, and $(e \mod \mathfrak{m}_K) \in \mathbb{F}_q[\![X]\!]$ is an endomorphism of it. Moreover, for any formal group law F over $\mathbb{F}_q$, the power series $e(X) = X^q$ is always an endomorphism of F. This is the “Frobenius endomorphism”.

Definition 4.6.12. Let $\mathcal{E}_\pi = \{e(X) \in \mathcal{O}_K[\![X]\!] \mid e(X) \equiv \pi X \mod (X^2),\ e(X) \equiv X^q \mod \mathfrak{m}_K\}$.

Clearly if $(F, [\cdot]_F)$ is a Lubin–Tate formal group law with respect to (K, π), then $[\pi]_F \in \mathcal{E}_\pi$.

Theorem 4.6.13. *We have a bijection from the set of Lubin–Tate formal group laws with respect to (K, π) to the set $\mathcal{E}_\pi$, sending $(F, [\cdot]_F)$ to $[\pi]_F$.*

Lemma 4.6.14 (Key Lemma)**.** *Let $e, \bar{e} \in \mathcal{E}_\pi$. Let $n \geq 1$ and $a_1, \dots, a_n \in \mathcal{O}_K$. Then there exists a unique $\phi(X_1, \dots, X_n) \in \mathcal{O}_K[\![X_1, \dots, X_n]\!]$ such that*

$$\phi(X_1, \dots, X_n) \equiv a_1X_1 + \cdots + a_nX_n \mod (X_1, \dots, X_n)^2$$

and

$$e(\phi(X_1, \dots, X_n)) = \phi(\bar{e}(X_1), \dots, \bar{e}(X_n)).$$

Proof. Set $\phi_1 = a_1X_1 + \cdots + a_nX_n$. We inductively construct ϕ_k by $\phi_k = \phi_{k-1} + Q_k$, where Q_k is a degree k homogeneous polynomial in $\mathcal{O}_K[X_1, \dots, X_n]$. These should satisfy:

$$e(\phi_k(X_1, \dots, X_n)) \equiv \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) \mod (X_1, \dots, X_n)^{k+1}. \tag{4.1}$$

Then $\phi = \lim_k \phi_k = \phi_1 + Q_2 + Q_3 + \cdots$ satisfies the desired conditions. This proves the existence of ϕ. For the uniqueness, let $\bar{\phi}$ be another candidate of ϕ, and let $\bar{\phi}_k$ be the part of $\bar{\phi}$ consisting of terms of degree at most k. Then $\bar{\phi}_k$ must satisfy (4.1). In the inductive construction of ϕ_k, we shall see that Q_k has a unique choice. Hence each ϕ_k is uniquely determined by ϕ_{k-1}. Since $\phi_1 = \bar{\phi}_1$, we have $\phi_k = \bar{\phi}_k$ for all k, and hence $\phi = \bar{\phi}$.

We now construct ϕ_k inductively such that (4.1) holds. For $k = 1$, (4.1) holds because $e(X) \equiv \bar{e}(X) \equiv \pi X \mod (X^2)$, which implies that the two sides are both congruent to $a_1\pi X_1 + \cdots + a_n\pi X_n \mod (X_1, \dots, X_n)^2$. Suppose ϕ_k has been constructed and it satisfies (4.1). Let Q_{k+1} be a degree $k+1$ homogeneous polynomial, to be determined. Let $\phi_{k+1} = \phi_k + Q_{k+1}$. Then

$$e(\phi_{k+1}(\underline{X})) \equiv e(\phi_k(\underline{X})) + e'(\phi_k(\underline{X}))Q_{k+1}(\underline{X}) \mod (X_1, \dots, X_n)^{k+2}.$$

Since $\phi_k(0) = 0$, we have $e'(\phi_k(\underline{X})) \equiv e'(0) \mod (X_1, \dots, X_n)$, and so $e'(\phi_k(\underline{X}))Q_{k+1}(\underline{X}) \equiv e'(0)Q_{k+1}(\underline{X}) = \pi Q_{k+1}(\underline{X}) \mod (X_1, \dots, X_n)^{k+2}$. Thus

$$e(\phi_{k+1}(\underline{X})) \equiv e(\phi_k(\underline{X})) + \pi Q_{k+1}(\underline{X}) \mod (X_1, \dots, X_n)^{k+2}.$$

On the other hand,

$$\begin{aligned}\phi_{k+1}(\bar{e}(X_1), \dots, \bar{e}(X_n)) &= \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) + Q_{k+1}(\bar{e}(X_1), \dots, \bar{e}(X_n)) \\ &\equiv \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) + Q_{k+1}(\pi X_1, \cdots, \pi X_n) \mod (X_1, \dots, X_n)^{k+2} \\ &= \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) + \pi^{k+1}Q_{k+1}(\underline{X})\end{aligned}$$

where the congruence is because $\bar{e}(X_i) \equiv \pi X_i \mod (X_i^2)$ and the last equality is because Q_{k+1} is homogeneous of degree $k+1$. Hence (4.1) is equivalent to

$$(\pi^{k+1} - \pi)Q_{k+1}(\underline{X}) \equiv e(\phi_k(\underline{X})) - \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) \mod (X_1, \dots, X_n)^{k+2}.$$

By the induction hypothesis, the right hand side has no terms of degree $\leq k$. So we can and must take Q_{k+1} to be $(\pi^{k+1} - \pi)^{-1}$ times the degree $k+1$ homogeneous part of $e(\phi_k(\underline{X})) - \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n))$. We still need to ensure that Q_{k+1} has coefficients in $\mathcal{O}_K$, for which it suffices to show that $e(\phi_k(\underline{X})) - \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) \equiv 0 \mod \mathfrak{m}_K$. This is true because

$$e(\phi_k(\underline{X})) - \phi_k(\bar{e}(X_1), \dots, \bar{e}(X_n)) \equiv \phi_k(\underline{X})^q - \phi_k(X_1^q, \dots, X_n^q) \equiv 0 \mod \mathfrak{m}_K.$$

(This is the "Frobenius property" of the polynomial X^q over $\mathcal{O}_K/\mathfrak{m}_K = \mathbb{F}_q$.) □

Proposition 4.6.15. *For each $e \in \mathcal{E}_\pi$, there exists a unique formal group F_e over $\mathcal{O}_K$ such that $e \in \mathrm{End}(F_e)$.*

Proof. The power series $F_e = F(X,Y)$ must satisfy $F(X,Y) \equiv X+Y \mod (X,Y)^2$ and $F(e(X),e(Y)) = e(F(X,Y))$. By Lemma 4.6.14, there is a unique such F. It remains to show that this F is a formal group. All the axioms are checked by using the uniqueness in Lemma 4.6.14. For instance, to show $F(F(X,Y),Z) = F(X,F(Y,Z))$, call the left hand side G_1 and the right hand side G_2. Then $G_1 \equiv G_2 \equiv X+Y+Z \mod (X,Y,Z)^2$, and we have $G_1(e(X),e(Y),e(Z)) = F(F(e(X),e(Y)),e(Z)) = F(e(F(X,Y)),e(Z)) = e(F(F(X,Y),Z)) = e(G_1(X,Y,Z))$, and similarly $G_2(e(X),e(Y),e(Z)) = e(G_2(X,Y,Z))$. Hence $G_1 = G_2$ by the uniqueness in Lemma 4.6.14. □

Proposition 4.6.16. *For each $e \in \mathcal{E}_\pi$, there is a unique ring homomorphism $[\cdot]_{F_e} : \mathcal{O}_K \to F_e$ making F_e a formal $\mathcal{O}_K$-module and such that $[\pi]_{F_e} = e$. In particular, the formal $\mathcal{O}_K$-module F_e is Lubin–Tate with respect to (K,π).*

Proof. For each $a \in \mathcal{O}_K$, we need to find a power series $[a] = [a]_{F_e} \in \mathcal{O}_K[\![X]\!]$ such that

(1) $[a](X) \equiv aX \mod (X^2)$.
(2) $[ab] = [a] \circ [b]$
(3) $[\pi] = e$
(4) $[a] \circ e = e \circ [a]$.
(5) $[a+b](X) = F_e([a](X),[b](X))$.

Here, (1) (2) (5) are the axioms for a formal $\mathcal{O}_K$-module, and (3) is the requirement in the proposition. (4) is a consequence of (2) and (3). Now (1) and (4) uniquely determine $[a]$, by Lemma 4.6.14. To show (2) (3) (5), one easily check that in each case the right hand side satisfies the unique characterization of the left hand side (i.e., (1) and (4)). For instance, to prove (5), we have

$$F_e([a](X),[b](X)) \equiv [a](X) + [b](X) \equiv aX + bX \mod (X^2),$$

and

$$F_e([a](e(X)),[b](e(X))) = F_e(e([a](X)), e([b](X))) = e(F_e([a](X),[b](X))).$$

□

Proof of Theorem 4.6.13. The inverse map is given by $e \mapsto (F_e, [\cdot]_{F_e})$. □

Proposition 4.6.17. *For $e, \bar{e} \in \mathcal{E}_\pi$, there exists a unique formal $\mathcal{O}_K$-module homomorphism $\phi = \phi_{e,\bar{e}} : F_e \to F_{\bar{e}}$ such that $\phi'(0) = 1$. In particular, ϕ is an isomorphism.*

Proof. The power series $\phi \in \mathcal{O}_K[\![X]\!]$ must satisfy

(1) $\phi(X) \equiv X \mod (X^2)$.
(2) $\phi \circ [a]_{F_e} = [a]_{F_{\bar{e}}} \circ \phi$ for all $a \in \mathcal{O}_K$.
(3) $\phi \circ e = \bar{e} \circ \phi$.
(4) $\phi(F_e(X,Y)) = F_{\bar{e}}(\phi(X),\phi(Y))$.

Here (3) is the special case of (2) for $a = \pi$. By Lemma 4.6.14, (1) and (3) uniquely determine ϕ. To check (2), call the left hand side G_1 and the right hand side G_2. We have $G_1(X) \equiv G_2(X) \equiv aX \mod (X^2)$. We have

$$G_1(e(X)) = \phi \circ [a]_{F_e} \circ e = \phi \circ e \circ [a]_{F_e} = \bar{e} \circ \phi \circ [a]_{F_e} = \bar{e}(G_1(X)),$$

and similarly $G_2(e(X)) = \bar{e}(G_2(X))$. Hence $G_1 = G_2$ by the uniqueness in Lemma 4.6.14. To check (4), call the left hand side G_1 and the right hand side G_2. Then $G_1 \equiv G_2 \equiv X+Y \mod (X,Y)^2$. We have

$$G_1(e(X), e(Y)) = \phi(e(F_e(X,Y))) = \bar{e}(\phi(F_e(X,Y))) = \bar{e}(G_1(X,Y)),$$

and similarly $G_2(e(X), e(Y)) = \bar{e}(G_2(X,Y))$. Hence $G_1 = G_2$ by the uniqueness in Lemma 4.6.14. □

Let $\Lambda = \{x \in \overline{K} \mid |x| < 1\}$. Fix $e \in \mathcal{E}_\pi$. For $x, y \in \Lambda$, the power series $F_e(x,y)$ converges in Λ. In fact, there is a finite extension L/K containing x and y. The completeness of L, the condition that $|x|, |y| < 1$, and the fact that $F_e(X,Y)$ has coefficients in $\mathcal{O}_K$, guarantee that $F_e(x,y)$ converges in L. Moreover, $F_e(x,y) \in \mathfrak{m}_L$ since F_e has no constant term and its coefficients are in $\mathcal{O}_K$.

It is easy to see that the axioms for a formal group imply that Λ together with the binary operation $(x,y) \mapsto F_e(x,y)$ is an abelian group. Moreover, for each $a \in \mathcal{O}_K$, the power series $[a]_{F_e}(x)$ converges in Λ for a similar reason as above. The scalar multiplication $\mathcal{O}_K \times \Lambda \to \Lambda, (a,x) \mapsto [a]_{F_e}(x)$ is compatible with the above-mentioned abelian group structure on Λ, and we thus obtain an $\mathcal{O}_K$-module structure on Λ. We denote this $\mathcal{O}_K$-module by Λ_e.

For each $\mathcal{O}_K$-module M and $n \in \mathbb{Z}_{\geq 1}$, we write $M_n = \{x \in M \mid \mathfrak{m}_K^n x = 0\} = \{x \in M \mid \pi^n x = 0\}$.

Definition 4.6.18. For π a uniformizer of K and $n \in \mathbb{Z}_{\geq 1}$, let $K_{\pi,n} = K(\Lambda_{e,n})$, where $e \in \mathcal{E}_\pi$.

Lemma 4.6.19. *The extension $K_{\pi,n}/K$ is independent of the choice of $e \in \mathcal{E}_\pi$.*

Proof. For $e, \bar{e} \in \mathcal{E}_\pi$, let $\phi : F_e \to F_{\bar{e}}$ be the isomorphism as in Proposition 4.6.17. Then we have an $\mathcal{O}_K$-module isomorphism $\Lambda_e \xrightarrow{\sim} \Lambda_{\bar{e}}, x \mapsto \phi(x)$. Here, the power series $\phi(x)$ converges in Λ. This isomorphism maps $\Lambda_{e,n}$ onto $\Lambda_{\bar{e},n}$. Moreover, for $x \in \Lambda_e$, if x lies in a finite extension L/K, then $\phi(x)$ also lies in L since ϕ is a power series with coefficients in $\mathcal{O}_K$. Hence $K(\Lambda_{\bar{e},n}) \subset K(\Lambda_{e,n})$. (Here we are not using that $K(\Lambda_{\bar{e},n})$ or $K(\Lambda_{e,n})$ are finite over K.) By symmetry we have equality. □

Lemma 4.6.20. *The extension $K_{\pi,n}/K$ is finite Galois.*

Proof. Let $e(X) = X^q + \pi X$. Then $e \in \mathcal{E}_\pi$, and so $K_{\pi,n} = K(\Lambda_{e,n})$. By definition, $\Lambda_{e,n}$ is the set of all roots in Λ of the polynomial $[\pi^n]_{F_e}$, which is the n-fold composition $e^{(n)}(X) = e \circ e \circ \cdots \circ e(X)$. The leading term of $e^{(n)}(X)$ is X^{q^n}, and we have $e^{(n)}(X) \equiv X^{q^n} \mod \mathfrak{m}_K$. Hence all slopes of its Newton polygon are negative, which means that all its roots in $\bar{K}$ are in Λ. This proves that $K_{\pi,n}$ is finite and normal over K.

We show that $K_{\pi,n}$ is separable over K by induction on n. We may assume that K has characteristic $p > 0$, so $q = 0$ in K. We have $e'(X) = \pi$, so $e(X)$ has no multiple roots. Hence $K_{\pi,1}$ is separable over K. It remains to prove that $K_{\pi,n+1}$ is separable over $K_{\pi,n}$. Note that for any $\alpha \in \Lambda_{e,n+1}$, we have $[\pi]_{F_e}(\alpha) = e(\alpha) \in \Lambda_{e,n}$. Hence $K_{\pi,n+1}$ is generated over $K_{\pi,n}$ by some roots of $e(X) - \beta$ for β running over $\Lambda_{e,n}$. The derivative of $e(X) - \beta$ is again π, so $e(X) - \beta$ has no multiple roots. Thus $K_{\pi,n+1}$ is separable over $K_{\pi,n}$, as desired. □

Lemma 4.6.21. *Let $e \in \mathcal{E}_\pi$. The multiplication-by-π map $\Lambda_e \to \Lambda_e$ is surjective and its kernel has cardinality q.*

Proof. We may assume that $e(X) = X^q + \pi X$. For surjectivity, we need to show that for any $\beta \in \Lambda$, the polynomial $e(X) - \beta$ has a root in Λ. The Newton polygon of this polynomial have only negative slopes, so all its roots in $\overline{K}$ are in Λ. To show that the kernel has cardinality q, we need to show that $e(X)$ has q distinct roots in Λ, or equivalently, that $e(X)$ has no multiple roots (since all its roots are in Λ). Clearly 0 is a simple root of $e(X)$, so we only need to show that $g(X) = e(X)/X = X^{q-1} + \pi$ has no multiple roots. We have $g'(X) = (q-1)X^{q-2}$, but $X = 0$ is not a root of $g(X)$. □

Proposition 4.6.22. *For $e \in \mathcal{E}_\pi$ and $n \in \mathbb{Z}_{\geq 1}$, the $\mathcal{O}_K$-module $\Lambda_{e,n}$ is isomorphic to $\mathcal{O}_K/\mathfrak{m}_K^n$.*

Proof. By the surjectivity in Lemma 4.6.21, we have a short exact sequence of $\mathcal{O}_K$-modules

$$0 \to \Lambda_{e,1} \xrightarrow{\text{inclusion}} \Lambda_{e,n+1} \xrightarrow{\text{mult. by } \pi} \Lambda_{e,n} \to 0.$$

By Lemma 4.6.21, $|\Lambda_{e,1}| = q$. Hence by induction $|\Lambda_{e,n}| = q^n$. By the classification of finite-cardinality modules over the PID $\mathcal{O}_K$, we have

$$\Lambda_{e,n} \cong \bigoplus_{i=1}^{t} \mathcal{O}_K/\mathfrak{m}_K^{e_i}.$$

But the π-torsion in $\Lambda_{e,n}$ is exactly $\Lambda_{e,1}$, and it has q-elements. Hence $t = 1$, and we have $\Lambda_{e,n} \cong \mathcal{O}_K/\mathfrak{m}_K^n$ since its cardinality is q^n. □

Corollary 4.6.23. *For $e \in \mathcal{E}_\pi$ and $n \in \mathbb{Z}_{\geq 1}$, the scalar multiplication map induces a canonical isomorphism $(\mathcal{O}_K/\mathfrak{m}_K^n)^\times = \mathcal{O}_K^\times/U_K^n \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_K-\mathrm{mod}}(\Lambda_{e,n})$.*

Let $n \in \mathbb{Z}_{\geq 1}$. The action of $\mathrm{Gal}(K_{\pi,n}/K)$ on $K_{\pi,n}$ stabilizes $\Lambda_{e,n}$ for each $e \in \mathcal{E}_\pi$, since $\Lambda_{e,n}$ is defined inside the maximal ideal of $K_{\pi,n}$ by power series equations with coefficients in $\mathcal{O}_K$, and the Galois action is continuous. Similarly, the $\mathrm{Gal}(K_{\pi,n}/K)$-action on $\Lambda_{e,n}$ is via $\mathcal{O}_K$-module automorphisms. In view of Corollary 4.6.23, we obtain a homomorphism

$$\rho_{\pi,n} : \mathrm{Gal}(K_{\pi,n}/K) \to \mathcal{O}_K^\times/U_K^n$$

by considering the $\mathrm{Gal}(K_{\pi,n}/K)$-action on $\Lambda_{e,n}$. This homomorphism is independent of the choice of e since for $e, \bar{e} \in \mathcal{E}_\pi$ the canonical isomorphism $\Lambda_e \to \Lambda_{\bar{e}}$ is given by a power series over $\mathcal{O}_K$ and the latter is preserved by the Galois action. Moreover, $\rho_{\pi,n}$ is injective since $K_{\pi,n}$ is generated by $\Lambda_{e,n}$ over K. Thus $K_{\pi,n}/K$ is a finite abelian extension.

Example 4.6.24. For $K = \mathbb{Q}_p$ and $\pi = p$, $\rho_{\pi,n}$ is the usual homomorphism (isomorphism) $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ sending τ to $a + p^n\mathbb{Z}$ such that $\tau(\zeta_{p^n}) = \zeta_{p^n}^a$.

Theorem 4.6.25. *Let $n \in \mathbb{Z}_{\geq 1}$. The following statements hold.*

(1) *The extension $K_{\pi,n}/K$ is totally ramified and its degree is $(q-1)q^{n-1}$.*
(2) *The homomorphism $\rho_{\pi,n}$ is an isomorphism.*
(3) *We have $\pi \in \mathrm{N}_{K_{\pi,n}/K}(K_{\pi,n}^\times)$.*

Proof. Let $e(X) = X^q + \pi X$ and $g(X) = e(X)/X$. Let $\pi_1 \in \overline{K}$ be a non-zero root of $e(X)$, and for $i \geq 2$ we inductively pick $\pi_i \in \overline{K}$ to be a non-zero root of $e(X) - \pi_{i-1}$. By Newton polygon considerations, we know (by induction) that

$$\mathrm{ord}(\pi_i) = \frac{1}{(q-1)q^{i-1}}.$$

Here $\mathrm{ord} : \overline{K}^\times \to \mathbb{Q}$ is the valuation extending the normalized valuation $\mathrm{ord} : K^\times \to \mathbb{Z}$. By induction, $\pi_i \in \Lambda_{e,i}$. Therefore the ramification index $e(K_{\pi,n}/K)$ is at least the denominator of $\operatorname{ord}(\pi_n)$, namely $(q-1)q^{n-1}$. On the other hand, the right hand side of the injection $\rho_{\pi,n} : \mathrm{Gal}(K_{\pi,n}/K) \to \mathcal{O}_K^\times/U_K^n$ has cardinality $(q-1)q^{n-1}$. Statements (1) and (2) follow.

To show (3), let $u_n(X)$ be the composed polynomial $g \circ e \circ \cdots \circ e$ where e appears $n-1$ times. Then $\deg u_n = (q-1)q^{n-1}$, and by induction $u_n(\pi_n) = 0$. By the formula for $\operatorname{ord}(\pi_n)$, the degree of π_n over K is at least $(q-1)q^{n-1}$. Hence $K_{\pi,n} = K(\pi_n)$, and u_n is the minimal polynomial of π_n over K. Thus $\mathrm{N}_{K_{\pi,n}/K}(-\pi_n) = u_n(0) = \pi$. □

Remark 4.6.26. In the above proof, we found the explicit description $K_{\pi,n} = K[X]/(u_n(X))$.

For $n|n'$, we have $K_{\pi,n} \subset K_{\pi,n'}$, and we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(K_{\pi,n'}/K) \arrow[r, "\rho_{\pi,n'}"] \arrow[d] & \mathcal{O}_K^\times/U_K^{n'} \arrow[d] \\
\mathrm{Gal}(K_{\pi,n}/K) \arrow[r, "\rho_{\pi,n}"] & \mathcal{O}_K^\times/U_K^n
\end{tikzcd}$$

where the vertical map on the left is restriction and the vertical map on the right is induced by identity on $\mathcal{O}_K^\times$. Thus denoting $K_\pi := \bigcup_n K_{\pi,n}$ and taking inverse limit over n, we obtain a topological isomorphism $\rho_\pi : \mathrm{Gal}(K_\pi/K) \xrightarrow{\sim} \mathcal{O}_K^\times$.

Let K^{LT} be the compositum $K^{\mathrm{ur}} \cdot K_\pi$ inside K^{ab}. Since each $K_{\pi,n}$ is totally ramified over K, we have

$$\mathrm{Gal}(K^{\mathrm{LT}}/K) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_\pi/K).$$

We define

$$\psi_K^{\mathrm{LT}} : K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times \to \mathrm{Gal}(K^{\mathrm{LT}}/K) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_\pi/K)$$

by sending (π^r, x) to $(\mathrm{Frob}^r, \rho_\pi^{-1}(x^{-1}))$.

Theorem 4.6.27. *Both K^{LT} and ψ_K^{LT} are independent of the choice of the uniformizer π.*

We need to use the completion $\breve{K}$ of K^{ur} with respect to the canonical absolute value on K^{ur}. Note that $\breve{K}$ is completely discretely valued, and the normalized discrete valuation $\operatorname{ord} : \breve{K}^\times \to \mathbb{Z}$ extends that on $K^\times$. We have filtrations

$$\mathcal{O}_{\breve{K}} = \mathfrak{m}_{\breve{K}}^0 \supset \mathfrak{m}_{\breve{K}}^1 \supset \mathfrak{m}_{\breve{K}}^2 \supset \cdots$$

and

$$\mathcal{O}_{\breve{K}}^\times = U_{\breve{K}}^0 \supset U_{\breve{K}}^1 \supset U_{\breve{K}}^2 \supset \cdots$$

where $U_{\breve{K}}^i = 1 + \mathfrak{m}_{\breve{K}}^i$ for $i \geq 1$. By the completeness of $\breve{K}$, these two filtrations are complete in the sense that the natural projections induce isomorphisms

$$\mathcal{O}_{\breve{K}} \cong \varprojlim_n \mathcal{O}_{\breve{K}}/\mathfrak{m}_{\breve{K}}^n, \quad \mathcal{O}_{\breve{K}}^\times \cong \varprojlim_n \mathcal{O}_{\breve{K}}^\times/U_{\breve{K}}^n.$$

The element $\mathrm{Frob} \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ acts on K^{ur} as an isometry, and hence it extends to an isometry $\breve{K} \to \breve{K}$, which we still denote by Frob.

Lemma 4.6.28. *The endomorphisms $\mathcal{O}_{\breve{K}} \to \mathcal{O}_{\breve{K}}, x \mapsto x - \mathrm{Frob}(x)$ and $\mathcal{O}_{\breve{K}}^\times \to \mathcal{O}_{\breve{K}}^\times, x \mapsto x\,\mathrm{Frob}(x)^{-1}$ are both surjective.*

Proof. These endomorphisms preserve the filtrations above since Frob is an isometry. By Lemma 2.3.2, it suffices to check that the corresponding endomorphisms on the successive quotients $\mathfrak{m}_{\breve{K}}^i/\mathfrak{m}_{\breve{K}}^{i+1}$ and $U_{\breve{K}}^i/U_{\breve{K}}^{i+1}$ are surjective (for all $i \geq 0$). In the first case for all $i \geq 0$ and in the second case for $i \geq 1$, we are reduced to the surjectivity of $\mathcal{O}_{\breve{K}}/\mathfrak{m}_{\breve{K}} = \overline{\mathbb{F}}_q \to$

$\overline{\mathbb{F}}_q, x \mapsto x - \mathrm{Frob}(x) = x - x^q$. In the second case for $i = 0$, we are reduced to the surjectivity of $\overline{\mathbb{F}}_q^\times \to \overline{\mathbb{F}}_q^\times, x \mapsto x\,\mathrm{Frob}(x)^{-1} = x^{1-q}$. □

We now let π, ϖ be two uniformizers in K, and write $\varpi = \pi u$, with $u \in \mathcal{O}_K^\times$. Let $e \in \mathcal{E}_\pi$ and $f \in \mathcal{E}_\varpi$. For any formal power series over $G(X_1, \dots, X_n)$ over $\mathcal{O}_{\breve{K}}$, we define $\mathrm{Frob}(G)$ by applying Frob to each coefficient of G. The following lemma generalizes the uniqueness in Lemma 4.6.14.

Lemma 4.6.29. *Suppose $G_1(X_1, \dots, X_n), G_2(X_1, \dots, X_n) \in \mathcal{O}_{\breve{K}}[\![X_1, \dots, X_n]\!]$ satisfy*

$$G_1(X_1, \dots, X_n) \equiv G_2(X_1, \dots, X_n) \mod (X_1, \dots, X_n)^2$$

and

$$\mathrm{Frob}(G_i)(e(X_1), \dots, e(X_n)) = f(G_i(X_1, \dots, X_n))$$

for $i = 1, 2$. Then $G_1 = G_2$.

Proof. Write G for G_1, and let Q_k be the homogeneous degree k part of G. It suffices to show that for $k \geq 2$, Q_k is uniquely determined by Q_i for $i \leq k-1$ and the condition that $\mathrm{Frob}(G)(e(X_1), \dots, e(X_n)) = f(G(X_1, \dots, X_n))$. The degree k homogeneous part of $\mathrm{Frob}(G)(e(X_1), \dots, e(X_n))$ is equal to the degree k homogeneous part R of $\sum_{i \leq k-1} \mathrm{Frob}(Q_i)(e(X_1), \dots, e(X_n))$ plus $\mathrm{Frob}(Q_k)(\pi X_1, \dots, \pi X_n) = \pi^k \mathrm{Frob}(Q_k)(\underline{X})$. The degree k homogeneous part of $f(G(X_1, \dots, X_n))$ is equal to the degree k homogeneous part S of $f(\sum_{i \leq k-1} Q_i(\underline{X}))$ plus $\varpi Q_k(\underline{X})$. Thus Q_k is determined by

$$R + \pi^k \mathrm{Frob}(Q_k) = S + \varpi Q_k.$$

Here R and S are determined by Q_i for $i \leq k-1$. We must show that the above equation, where R and S are viewed as fixed, uniquely determines Q_k. This boils down to the claim that for any fixed $\beta \in \mathcal{O}_{\breve{K}}$, the equation

$$\varpi x - \pi^k \mathrm{Frob}(x) + \beta = 0$$

has at most one solution $x \in \breve{K}$. Suppose x and y are two solutions. Then

$$\varpi(x - y) = \pi^k \mathrm{Frob}(x - y).$$

If $x \neq y$, then the two sides have different valuations (since Frob preserves the valuation), a contradiction. □

Proposition 4.6.30. *The formal $\mathcal{O}_K$-modules F_e and F_f over $\mathcal{O}_{\breve{K}}$ are isomorphic. More precisely, fix $\epsilon \in \mathcal{O}_{\breve{K}}^\times$ such that $\mathrm{Frob}(\epsilon) = \epsilon u$ (which exists by Lemma 4.6.28). There exists $\theta(X) \in \mathcal{O}_{\breve{K}}[\![X]\!]$ satisfying the following conditions.*

1. $\theta(X) \equiv \epsilon X \mod (X^2)$.
2. $\mathrm{Frob}(\theta(X)) = \theta([u]_{F_e}(X))$.
3. $f \circ \theta = \mathrm{Frob}(\theta) \circ e$.
4. $\theta(F_e(X, Y)) = F_f(\theta(X), \theta(Y))$.
5. $\theta([a]_{F_e}(X)) = [a]_{F_f}(\theta(X)), \ \forall a \in \mathcal{O}_K$.

Note that conditions (1) (4) (5) imply that θ is an isomorphism $F_e \xrightarrow{\sim} F_f$ between formal $\mathcal{O}_K$-modules over $\mathcal{O}_{\breve{K}}$. Indeed, by (1), (4), and Exercise 4.6.5, θ is an isomorphism of formal groups. Then (5) immediately implies that the inverse of θ is also compatible with the formal $\mathcal{O}_K$-module structures.

Proof. We first construct $\theta(X) = \sum_{i=1}^{\infty} a_i X^i$ satisfying (1) and (2). Let $a_1 = \epsilon$, and construct $a_i \in \mathcal{O}_{\breve{K}}$ inductively such that

$$\mathrm{Frob}(\sum_{i=1}^{n} a_i X^i) \equiv \sum_{i=1}^{n} a_i [u]_{F_e}(X)^i \mod (X^{n+1}).$$

That this holds for $n = 1$ is precisely our assumption that $\mathrm{Frob}(\epsilon) = \epsilon u$. Now suppose $a_1, \dots, a_n$ are constructed. To construct a_{n+1}, we need $\mathrm{Frob}(a_{n+1})$ to be equal to the coefficient C of X^{n+1} in $\sum_{i=1}^{n} a_i [u]_{F_e}(X)^i$ plus $a_{n+1} u^{n+1}$. Thus we need to solve $\mathrm{Frob}(a_{n+1}) - u^{n+1} a_{n+1} = C$ for a_{n+1}. By Lemma 4.6.28, we can write $u^{n+1} = b\,\mathrm{Frob}(b)^{-1}$ for a fixed $b \in \mathcal{O}_{\breve{K}}^{\times}$. Thus $y = b a_{n+1}$ should satisfy $\mathrm{Frob}(y) - y = \mathrm{Frob}(b) C$. By Lemma 4.6.28, we can solve this equation in $y \in \mathcal{O}_{\breve{K}}$. Thus we have shown the existence of θ satisfying (1) and (2).

We now show that such θ can be modified to satisfy (3). By (1) and Exercise 4.6.5, θ has composition inverse $\theta^{-1} \in \mathcal{O}_{\breve{K}}[\![X]\!]$. Let $h = \mathrm{Frob}(\theta) \circ e \circ \theta^{-1} \in \mathcal{O}_{\breve{K}}[\![X]\!]$. Then by (2) we have

$$h = \theta \circ [u]_{F_e} \circ e \circ \theta^{-1} = \theta \circ [u\pi]_{F_e} \circ \theta^{-1} = \theta \circ e \circ [u]_{F_e} \circ \theta^{-1}.$$

Since e and $[u]_{F_e}$ have coefficients in $\mathcal{O}_K$, we have

$$\mathrm{Frob}(h) = \mathrm{Frob}(\theta) \circ e \circ [u]_{F_e} \circ \mathrm{Frob}(\theta^{-1}) = \mathrm{Frob}(\theta) \circ e \circ \theta^{-1} = h.$$

Hence $h \in \mathcal{O}_K[\![X]\!]$. We now check that $h \in \mathcal{E}_{\varpi}$. We have $h(0) = 0$, and the linear coefficient of h is $\epsilon u \pi \epsilon^{-1} = u\pi = \varpi$. Modulo $\mathfrak{m}_K$, we have

$$h \equiv \mathrm{Frob}(\theta) \circ (X \mapsto X^q) \circ \theta^{-1},$$

so

$$h(X) \equiv (\mathrm{Frob}(\theta))(\theta^{-1}(X)^q) \equiv \big(\theta(\theta^{-1}(X))\big)^q = X^q.$$

Thus $h \in \mathcal{E}_{\varpi}$, and we have the canonical isomorphism $\phi_{f,h} : F_f \xrightarrow{\sim} F_h$ as in Proposition 4.6.17. Let $\theta_1 = \phi_{f,h} \circ \theta$. Then θ_1 still satisfies conditions (1) and (2) (since $\mathrm{Frob}(\theta_1) = \phi_{f,h} \circ \mathrm{Frob}(\theta)$), and we have

$$\mathrm{Frob}(\theta_1) \circ e \circ \theta_1^{-1} = \phi_{f,h} \circ h \circ \phi_{h,f} = f.$$

Thus θ_1 also satisfies (3).

We now assume that θ satisfies (1) (2) (3). One then checks that θ satisfies (4) and (5) using Lemma 4.6.29. For (4), call the left hand side $G_1(X,Y)$ and right hand side $G_2(X,Y)$. Then

$$\mathrm{Frob}(G_1)(e(X), e(Y)) = \mathrm{Frob}(\theta)(e(F_e(X,Y))) = f(\theta(F_e(X,Y))) = f(G_1(X,Y)),$$

and

$$\begin{aligned}\mathrm{Frob}(G_2)(e(X), e(Y)) = F_f\big(&\mathrm{Frob}(\theta)(e(X)), \mathrm{Frob}(\theta)(e(Y))\big) \\ &= F_f\big(f(\theta(X)), f(\theta(Y))\big) = f(G_2(X,Y)).\end{aligned}$$

Moreover, $G_1(X) \equiv G_2(X) \equiv \epsilon(X+Y) \mod (X,Y)^2$. Hence $G_1 = G_2$.

For (5), call the left hand side G_1 and the right hand side G_2. Then

$$\mathrm{Frob}(G_1)(e(X)) = \mathrm{Frob}(\theta) \circ [a]_{F_e} \circ e(X) = \mathrm{Frob}(\theta) \circ e \circ [a]_{F_e}(X) = f \circ \theta \circ [a]_{F_e}(X) = f(G_1(X)),$$

and

$$\mathrm{Frob}(G_2)(e(X)) = [a]_{F_f} \circ \mathrm{Frob}(\theta) \circ e(X) = [a]_{F_f} \circ f \circ \theta(X) = f(G_2(X)).$$

Moreover $G_1 \equiv G_2 \equiv \epsilon a X \mod (X^2)$, so $G_1 = G_2$. □

Proof of Theorem 4.6.27. We first show that K^{LT} is independent of π. Let π, ϖ be two uniformizers of K. We shall show that $K^{\mathrm{ur}} \cdot K_{\pi,n} = K^{\mathrm{ur}} \cdot K_{\varpi,n}$ for each $n \geq 1$. Let $e = X^q + \pi X \in \mathcal{E}_\pi$ and $f = X^q + \varpi X \in \mathcal{E}_\varpi$. Let θ be as in Proposition 4.6.30, with respect to π, ϖ, e, f. Let C be the completion of $\overline{K}$. There is a natural embedding $\breve{K} \to C$. We make the set $\Lambda' = \{x \in C \mid |x| < 1\}$ into $\mathcal{O}_K$-modules Λ'_e and Λ'_f using F_e and F_f respectively. Note that the $\mathfrak{m}_K^n$-torsion $\Lambda'_{e,n}$ in Λ'_e is actually equal to $\Lambda_{e,n}$, because both sets consist of all the roots of the polynomial $e^{(n)} = e \circ \cdots \circ e$ in $\overline{K}$. Similarly, $\Lambda'_{f,n} = \Lambda_{f,n}$. Clearly θ induces an $\mathcal{O}_K$-module isomorphism $\Lambda'_e \xrightarrow{\sim} \Lambda'_f, x \mapsto \theta(x)$, and hence a bijection $\Lambda'_{e,n} \xrightarrow{\sim} \Lambda'_{f,n}$. Thus we have

$$\Lambda_{f,n} = \theta(\Lambda_{e,n}).$$

Since $\theta(X) \in \mathcal{O}_{\breve{K}}[\![X]\!]$, every element of $\theta(\Lambda_{e,n})$ can be arbitrarily approximated by elements of $\mathcal{O}_{\breve{K}}[\Lambda_{e,n}]$, and hence arbitrarily approximated by elements of $\mathcal{O}_{K^{\mathrm{ur}}}[\Lambda_{e,n}]$. Thus $\Lambda_{f,n} = \theta(\Lambda_{e,n})$ is contained in the topological closure of $K^{\mathrm{ur}} \cdot K_{\pi,n}$ in C. Therefore $K_{\varpi,n}$ is contained in this topological closure. By symmetry, the topological closures of $K^{\mathrm{ur}} \cdot K_{\pi,n}$ and $K^{\mathrm{ur}} \cdot K_{\varpi,n}$ in C are equal. By Lemma 4.6.31 below, we can recover $K^{\mathrm{ur}} \cdot K_{\pi,n}$ from its topological closure in C by taking algebraic elements over K, and similarly for $K^{\mathrm{ur}} \cdot K_{\varpi,n}$. Hence $K^{\mathrm{ur}} \cdot K_{\pi,n} = K^{\mathrm{ur}} \cdot K_{\varpi,n}$ as desired. We have proved that K^{LT} is independent of π.

We now show that ψ_K^{LT} is independent of π. We write ψ_π for the version of ψ_K^{LT} defined using π. We only need to show that $\psi_\pi(\varpi) = \psi_\varpi(\varpi)$ whenever π, ϖ are two uniformizers. Indeed, if we know this, then for any uniformizer π' we have $\psi_\pi(\varpi) = \phi_{\pi'}(\varpi)$, since they are both equal to $\phi_\varpi(\varpi)$. Keeping π and π' fixed and letting ϖ vary, we conclude that $\psi_\pi = \psi_{\pi'}$.

We now show that $\psi_\pi(\varpi) = \psi_\varpi(\varpi)$. Recall that $\psi_\varpi(\varpi)$ acts as the Frobenius on K^{ur} and acts trivially on $K_{\varpi,n}$ for all n. Write $\varpi = \pi u$. Now $\psi_\pi(\varpi) = \psi_\pi(\pi u)$ also acts as the Frobenius on K^{ur}, and it sends $x \in \Lambda_{e,n}$ to $[u^{-1}]_{F_e}(x)$. Thus it sends $\theta(x) \in \Lambda_{f,n}$ to $\mathrm{Frob}(\theta)([u^{-1}]_{F_e}(x))$, since it acts on the coefficients of θ, which are in $\breve{K}$, as Frob. By property (2) in Proposition 4.6.30, $\mathrm{Frob}(\theta)([u^{-1}]_{F_e}(x)) = \theta(x)$. Thus $\psi_\pi(\varpi)$ fixes $\theta(x)$ for every $x \in \Lambda_{e,n}$. Since $\Lambda_{f,n} = \theta(\Lambda_{e,n})$, we see that $\psi_\pi(\varpi)$ fixes $\Lambda_{f,n}$. Hence $\psi_\pi(\varpi)$ acts trivially on $K_{\varpi,n}$ for all n. □

Lemma 4.6.31. *Let L be an intermediate extension of $\overline{K}/K$ such that $\mathrm{ord}(L^\times) = \frac{1}{e}\mathbb{Z} \subset \mathbb{Q}$ for some $e \in \mathbb{Z}_{\geq 1}$. Then L is algebraically closed inside its completion $\hat{L}$.*

Remark 4.6.32. If L/K is finite, then $L = \hat{L}$, and there is nothing to prove.

Proof. Suppose not. Then there is a non-trivial finite extension L_1/L inside $\hat{L}$. By our assumption, the canonical absolute value on L is a discrete valuation. Hence we have (see [Ser79, §II.3, Thm. 1 (iii)], cf. Fact 1.4.3)

$$L_1 \otimes_L \hat{L} \cong \prod_w L_{1,w}$$

where w runs over places of L_1 over the canonical place of L. Every such w must be over the canonical place of K. Since K is complete and L_1 is algebraic over K, there is only one such w. We conclude that $[L_{1,w} : \hat{L}] = [L_1 : L]$. This is by hypothesis > 1, so $\hat{L}$ is a proper closed subset of $L_{1,w}$. In particular, L is not dense in L_1 for the topology on L_1 defined by w. This topology on L_1 is just the subspace topology $L_1 \subset \hat{L}$, and L is dense in $\hat{L}$, a contradiction. □

Remark 4.6.33. In Lemma 4.6.31, we crucially used that L is algebraic over a *complete* discretely valued field. For instance $\mathbb{Q}$ is not algebraically closed inside its p-adic completion $\mathbb{Q}_p$.

Theorem 4.6.34. *Assume Theorem 4.5.1, and let ψ_K be a local Artin map as in that theorem. The following statements hold.*

(1) *(Local Kronecker–Weber.) We have $K^{\mathrm{ab}} = K^{\mathrm{LT}}$.*
(2) *(Explicit formula for the local Artin map.) We have $\psi_K = \psi_K^{\mathrm{LT}}$. (Here both maps have the same target $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \mathrm{Gal}(K^{\mathrm{LT}}/K)$.) In particular, ψ_K is unique.*
(3) *The Local Existence Theorem (Theorem 4.5.3) holds.*

Lemma 4.6.35. *Assume Theorem 4.5.1. Then for finite abelian extensions L/K and L'/K in K^{ab}, we have $L \subset L'$ if and only if $\mathrm{N}_{L/K}(L^\times) \supset \mathrm{N}_{L'/K}(L'^{,\times})$.*

Proof. The same as the proof of Corollary 4.2.8. □

Lemma 4.6.36. *Assume Theorem 4.5.1. The composition of $\psi_K : K^\times \to G_K^{\mathrm{ab}}$ with the restriction map $G_K^{\mathrm{ab}} \to \mathrm{Gal}(K^{\mathrm{LT}}/K)$ is equal to ψ_K^{LT}.*

Proof. It suffices to show that the two maps send every uniformizer π in K to the same image. We have $K^{\mathrm{LT}} = K^{\mathrm{ur}} \cdot K_\pi$, so it suffices to show that $\psi_K(\pi)|_{K^{\mathrm{ur}}} = \psi_K^{\mathrm{LT}}(\pi)|_{K^{\mathrm{ur}}}$ and $\psi_K(\pi)|_{K_\pi} = \psi_K^{\mathrm{LT}}(\pi)|_{K_\pi}$. In other words, we need to show that $\psi_K(\pi)$ acts on every finite unramified extension L/K as the Frobenius, and acts trivially on $K_{\pi,n}$ for every $n \geq 1$. The first property is condition (1) in Theorem 4.5.1. The second property follows from condition (2) in Theorem 4.5.1 and the fact that $\pi \in \mathrm{N}_{K_{\pi,n}/K}(K_{\pi,n}^\times)$ (Theorem 4.6.25 (3)). □

For $r \in \mathbb{Z}_{\geq 1}$, let K_r/K be the degree r unramified extension. For a uniformizer $\pi \in K$ and $r, n \in \mathbb{Z}_{\geq 1}$, let $N_{\pi,r,n} := \pi^{r\mathbb{Z}} \times U_K^n \subset K^\times$. Let $K_{\pi,r,n} := K_r \cdot K_{\pi,n}$.

Lemma 4.6.37. *Assume Theorem 4.5.1. We have $\mathrm{N}_{K_{\pi,r,n}/K}(K_{\pi,r,n}^\times) = N_{\pi,r,n}$.*

Proof. By the definition of ψ_K^{LT}, $N_{\pi,r,n}$ is contained in the kernel of

$$K^\times \xrightarrow{\psi_K^{\mathrm{LT}}} \mathrm{Gal}(K^{\mathrm{LT}}/K) \to \mathrm{Gal}(K_{\pi,r,n}/K).$$

By Lemma 4.6.36, this kernel is equal to the kernel of $\psi_{K_{\pi,r,n}/K}$. By Theorem 4.5.1 (2), the latter kernel is equal to $\mathrm{N}_{K_{\pi,r,n}/K}(K_{\pi,r,n}^\times)$. Thus we have $N_{\pi,r,n} \subset \mathrm{N}_{K_{\pi,r,n}/K}(K_{\pi,r,n}^\times)$. To prove that they are equal, it suffices to show that the have the same finite index in $K^\times$. By Theorem 4.5.1 (2), the index of $N_{K_{\pi,r,n}/K}(K_{\pi,r,n}^\times)$ in $K^\times$ is equal to $[K_{\pi,r,n} : K]$, and this is equal to $r(q-1)q^{n-1}$ by Theorem 4.6.25. Clearly the index of $N_{\pi,r,n}$ in $K^\times$ is also this number, as desired. □

Proof of Theorem 4.6.34. Let π be a uniformizer in K. For part (1), let L/K be an arbitrary finite abelian extension. We need to show that L is contained in $K_{\pi,r,n}$ for suitable r, n. By Lemmas 4.6.35 and 4.6.37, it suffices to show that $\mathrm{N}_{L/K}(L^\times)$ contains $N_{\pi,r,n}$ for suitable r, n. By Theorem 4.5.1 (2), $\mathrm{N}_{L/K}(L^\times)$ is a finite index open subgroup of $K^\times$. It is easy to see that every finite index open subgroup of $K^\times$ contains $N_{\pi,r,n}$ for suitable r, n. This proves part (1).

Part (2) follows from part (1) and Lemma 4.6.36.

For part (3), we need to show that a subgroup of $K^\times$ is finite index and open if and only if it is of the form $\mathrm{N}_{L/K}(L^\times)$ for some finite abelian extension L/K. The "if" part follows from Theorem 4.5.1 (2). We now prove the "only if" part. Let $U \subset K^\times$ be a finite index open subgroup. Then, as we mentioned earlier, U contains $N_{\pi,r,n}$ for suitable r, n. By Theorem

4.5.1 (2) and Lemma 4.6.37, ψ_K induces an isomorphism $K^\times/N_{\pi,r,n} \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,r,n}/K)$. Let H be the image of $U/N_{\pi,r,n}$ under this isomorphism. Let $L = K_{\pi,r,n}^H$. Then L/K is a finite abelian extension, and clearly $\ker \psi_{L/K} = U$. By Theorem 4.5.1 (2), this implies that $U = \mathrm{N}_{L/K}(L^\times)$. □

4.7. **Ideal theoretic formulation of global class field theory.** Let K be a global field. For simplicity, we shall assume that K is a number field, and ignore the global function field case.

Definition 4.7.1. A *modulus* of K is a formal finite product $v_1^{e_1}\cdots v_n^{e_n}$ with $v_i \in V_K$ and $e_i \in \mathbb{Z}_{\geq 1}$, satisfying the following conditions:

- No v_i is a complex place.
- If v_i is a real place, then $e_i = 1$.

Sometimes we also allow e_i to be 0, with the understanding that in that case v_i does not really appear in the modulus. If $\mathfrak{m}, \mathfrak{m}'$ are two moduli of K, we define the obvious notion of divisibility $\mathfrak{m}|\mathfrak{m}'$. If a place v appears in $\mathfrak{m}$, we also write $v|\mathfrak{m}$. In this case, we shall denote by e_v the exponent of v in $\mathfrak{m}$ (when no confusion arises).

Definition 4.7.2. Let $\mathfrak{m}$ be a modulus. Define the following subgroup of $\mathbb{A}_K^\times$:

$$U_\mathfrak{m} = \prod_{v\in V_{K,\infty}, v\nmid\mathfrak{m}} K_v^\times \times \prod_{v\in V_{K,\infty}, v|\mathfrak{m}} K_{v,>0} \times \prod_{v\in V_{K,f}, v\nmid\mathfrak{m}} \mathcal{O}_{K_v}^\times \times \prod_{v\in V_{K,f}, v|\mathfrak{m}} U_{K_v}^{e_v}.$$

Clearly $U_\mathfrak{m}$ is an open subgroup of $\mathbb{A}_K^\times$. If $\mathfrak{m}|\mathfrak{m}'$, then $U_\mathfrak{m} \supset U_{\mathfrak{m}'}$.

Exercise 4.7.3. Every open subgroup of $\mathbb{A}_K^\times$ contains $U_\mathfrak{m}$ for some modulus $\mathfrak{m}$.

Definition 4.7.4. Let $\mathfrak{m}$ be a modulus.

(1) Let $I_K^{(\mathfrak{m})}$ be the group of fractional ideals of K which are coprime to $\mathfrak{m}$, i.e., fractional ideals of the form $\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}$ where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$, $n_i \in \mathbb{Z}-\{0\}$, and none of $\mathfrak{p}_i$ appears in $\mathfrak{m}$. More formally, $I_K^{(\mathfrak{m})}$ is the free abelian group $\mathbb{Z}[v \in V_{K,f}, v \nmid \mathfrak{m}]$ generated by the finite places of K not dividing $\mathfrak{m}$.

(2) Let $K_{(\mathfrak{m})}^\times$ be the multiplicative group consisting of $x \in K^\times$ such that for every archimedean place $v|\mathfrak{m}$ we have $x \in K_{v,>0}$ (here $K_v = \mathbb{R}$) and for every non-archimedean place $v|\mathfrak{m}$ we have $x \in U_{K_v}^{e_v} = 1 + \mathfrak{m}_{K_v}^{e_v}$. Here $e_v \geq 1$ is the exponent of v in $\mathfrak{m}$.

Note that if $x \in K_{(\mathfrak{m})}^\times$, then the principal fractional ideal $x\mathcal{O}_K$ lies in $I_K^{(\mathfrak{m})}$ since $x \in \mathcal{O}_{K_v}^\times$ for every non-archimedean $v|\mathfrak{m}$. Thus we obtain a group homomorphism $K_{(\mathfrak{m})}^\times \to I_K^{(\mathfrak{m})}$ sending x to $x\mathcal{O}_K$. If we identify $I_K^{(\mathfrak{m})}$ with $\mathbb{Z}[v \in V_{K,f}, v \nmid \mathfrak{m}]$, then this homomorphism sends x to

$$\sum_{v\in V_{K,f}, v\nmid\mathfrak{m}} \mathrm{ord}_v(x)[v].$$

Definition 4.7.5. The *ray class group* with respect to a modulus $\mathfrak{m}$ is the cokernel of the map $K_{(\mathfrak{m})}^\times \to I_K^{(\mathfrak{m})}$. It is denoted by $\mathrm{Cl}_\mathfrak{m}(K)$.

Example 4.7.6. If $\mathfrak{m} = 1$ is trivial, then $\mathrm{Cl}_\mathfrak{m}(K)$ is the usual class group $\mathrm{Cl}(K)$ of the number field K.

Example 4.7.7. Let $K = \mathbb{Q}$, and $\mathfrak{m} = \infty p_1^{e_1} \cdots p_n^{e_n}$, where p_i are prime numbers and $e_i \in \mathbb{Z}_{\geq 1}$. Let $m = p_1^{e_1} \cdots p_n^{e_n}$. Since $\mathrm{Cl}(\mathbb{Q}) = 1$, every fractional ideal in $\mathbb{Q}$ is principal. Thus every fractional ideal has a unique positive rational generator. Hence the group $I_{\mathbb{Q}}^{(\mathfrak{m})}$ is identified with the group of positive rational numbers of the form a/b where $a, b \in \mathbb{Z}_{\geq 1}$ are both coprime m. There is a natural surjective homomorphism $I_{\mathbb{Q}}^{(\mathfrak{m})} \to (\mathbb{Z}/m\mathbb{Z})^\times$ sending a/b as above to $\bar{a}\bar{b}^{-1}$. The kernel of this homomorphism consists of a/b such that $a/b \in \mathbb{R}_{>0}$ and such that for each $1 \leq i \leq n$ we have $a/b \in 1 + p_i^{e_i}\mathbb{Z}_p \subset \mathbb{Q}_p^\times$. This is exactly $\mathbb{Q}_{(\mathfrak{m})}^\times$. Hence we have a short exact sequence

$$1 \to \mathbb{Q}_{(\mathfrak{m})}^\times \to I_{\mathbb{Q}}^{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^\times.$$

In particular, $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q})$ is canonically identified with $(\mathbb{Z}/m\mathbb{Z})^\times$.

Similarly, if $\mathfrak{m} = m$, then $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q})$ is canonically identified with $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$.

We now need to relate the ray class group to ideles.

Definition 4.7.8. Let $\mathfrak{m}$ be a modulus. Define the following subgroup of $\mathbb{A}_K^\times$:

$$V_{\mathfrak{m}} = \prod_{v \in V_{K,\infty}, v \nmid \mathfrak{m}} K_v^\times \times \prod_{v \in V_{K,\infty}, v \mid \mathfrak{m}} K_{v,>0} \times \prod'_{v \in V_{K,f}, v \nmid \mathfrak{m}} K_v^\times \times \prod_{v \in V_{K,f}, v \mid \mathfrak{m}} U_{K_v}^{e_v}.$$

Here the restricted product is with respect to the $\mathcal{O}_{K_v}^\times$.

Clearly projection to the components indexed by $v \in V_{K,f}, v \nmid \mathfrak{m}$ induces an isomorphism

$$V_{\mathfrak{m}}/U_{\mathfrak{m}} \xrightarrow{\sim} \prod'_{v \in V_{K,f}, v \nmid \mathfrak{m}} K_v^\times/\mathcal{O}_{K_v}^\times.$$

The maps ord_v induce an isomorphism from the right hand side to $\bigoplus_{v \in V_{K,f}, v \nmid \mathfrak{m}} \mathbb{Z} \cong I_K^{(\mathfrak{m})}$. Hence we obtain a canonical isomorphism

$$V_{\mathfrak{m}}/U_{\mathfrak{m}} K_{(\mathfrak{m})}^\times \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}}(K).$$

Here, on the left hand side, $K_{(\mathfrak{m})}^\times$ is a subgroup of $K^\times$, which embeds diagonally into $\mathbb{A}_K^\times$ as usual. It is easy to see that $V_{\mathfrak{m}} \cap K^\times = K_{(\mathfrak{m})}^\times$, so the quotient makes sense.

On the other hand, since $V_{\mathfrak{m}} \cap K^\times = K_{(\mathfrak{m})}^\times$, we have an injection

$$V_{\mathfrak{m}}/U_{\mathfrak{m}} K_{(\mathfrak{m})}^\times \hookrightarrow \mathbb{A}_K^\times/K^\times U_{\mathfrak{m}}.$$

We claim that this is a surjection. Indeed, if we let $S = V_{K,\infty} \cup \{v \in V_{K,f} \mid v \nmid \mathfrak{m}\}$, then by Lemma 4.2.6, $(\mathbb{A}_K^S)^\times$ has dense image in $C_K = \mathbb{A}_K^\times/K^\times$. Since $U_{\mathfrak{m}}$ is open in $\mathbb{A}_K^\times$, $(\mathbb{A}_K^S)^\times$ surjects onto $\mathbb{A}_K^\times/K^\times U_{\mathfrak{m}}$. Clearly $(\mathbb{A}_K^S)^\times \subset V_{\mathfrak{m}}$, so the claim is proved.

In conclusion, we have canonical isomorphisms

$$V_{\mathfrak{m}}/U_{\mathfrak{m}} K_{(\mathfrak{m})}^\times \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}}(K).$$

and

$$V_{\mathfrak{m}}/U_{\mathfrak{m}} K_{(\mathfrak{m})}^\times \xrightarrow{\sim} \mathbb{A}_K^\times/K^\times U_{\mathfrak{m}}.$$

We write $\bar{U}_{\mathfrak{m}}$ for the image of $U_{\mathfrak{m}}$ in $C_K = \mathbb{A}_K^\times/K^\times$. Composing the above two isomorphisms we obtain a canonical isomorphism

$$C_K/\bar{U}_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}}(K).$$

Remark 4.7.9. Note that for a general element $x = (x_v)_v \in \mathbb{A}_K^\times$, there is no direct formula for its image under $\mathbb{A}_K^\times \to C_K/\bar{U}_\mathfrak{m} \xrightarrow{\sim} \mathrm{Cl}_\mathfrak{m}(K)$. Nevertheless, by our previous argument, the isomorphism $C_K/\bar{U}_\mathfrak{m} \xrightarrow{\sim} \mathrm{Cl}_\mathfrak{m}(K)$ is characterized as follows. Let $S = V_{K,\infty} \cup \{v \in V_{K,f} \mid v \nmid \mathfrak{m}\}$ as before. Then the natural map $(\mathbb{A}_K^S)^\times \to C_K/\bar{U}_\mathfrak{m}$ is surjective, and the composite map

$$(\mathbb{A}_K^S)^\times \to C_K/\bar{U}_\mathfrak{m} \xrightarrow{\sim} \mathrm{Cl}_\mathfrak{m}(K)$$

sends $(x_v)_{v\notin S}$ to $\sum_{v\notin S} \mathrm{ord}_v(x_v)[v]$.

Corollary 4.7.10. *For any modulus* $\mathfrak{m}$, *the group* $\mathrm{Cl}_\mathfrak{m}(K)$ *is finite. If* $\mathfrak{m}|\mathfrak{m}'$, *then the natural map* $\mathrm{Cl}_{\mathfrak{m}'}(K) \to \mathrm{Cl}_\mathfrak{m}(K)$ *induced by the inclusion* $\mathbb{Z}[v \in V_{K,f}, v \nmid \mathfrak{m}'] \hookrightarrow \mathbb{Z}[v \in V_{K,f}, v \nmid \mathfrak{m}], [v] \mapsto [v]$, *is surjective.*

Proof. Since $\bar{U}_\mathfrak{m}$ is an open subgroup of C_K, it is of finite index in C_K by Exercise 4.3.2. Alternatively, clearly the idele norm $\|\cdot\| : \mathbb{A}_K^\times \to \mathbb{R}_{>0}$ is surjective on $U_\mathfrak{m}$, hence the compact C_K^1 surjects onto $C_K/\bar{U}_\mathfrak{m}$. But the latter is discrete since $\bar{U}_\mathfrak{m}$ is open in C_K, so it is finite. The surjectivity follows from Remark 4.7.9 and the surjectivity of the natural map $C_K/\bar{U}_{\mathfrak{m}'} \to C_K/\bar{U}_\mathfrak{m}$. □

By Corollary 4.2.8, we have a bijection between finite abelian extensions of K in K^{ab} and finite index open subgroups of C_K. Let $K_\mathfrak{m}/K$ be the finite abelian extension corresponding to $\bar{U}_\mathfrak{m} \subset C_K$. This is called the *ray class field* corresponding to $\mathfrak{m}$. By Theorem 4.2.1, the Artin map induces an isomorphism

$$\psi_{K_\mathfrak{m}/K} : C_K/\bar{U}_\mathfrak{m} \xrightarrow{\sim} \mathrm{Gal}(K_\mathfrak{m}/K).$$

By identifying the left hand side with $\mathrm{Cl}_\mathfrak{m}(K)$, we also regard this as an isomorphism

$$\psi_{K_\mathfrak{m}/K} : \mathrm{Cl}_\mathfrak{m}(K) \xrightarrow{\sim} \mathrm{Gal}(K_\mathfrak{m}/K).$$

Proposition 4.7.11. *The following statements hold.*

(1) *(Abstract Kronecker–Weber.) We have* $K^{\mathrm{ab}} = \bigcup_\mathfrak{m} K_\mathfrak{m}$, *where* $\mathfrak{m}$ *runs through all moduli.*

(2) *Let* $\mathfrak{m}$ *be a modulus. For any* $v \in V_K$ *not dividing* $\mathfrak{m}$, v *is unramified in* $K_\mathfrak{m}$. *(If* v *is archimedean, this means that either* v *is complex or every place of* $K_\mathfrak{m}$ *above* v *is real.) The Artin map* $\mathrm{Cl}_\mathfrak{m}(K) \xrightarrow{\sim} \mathrm{Gal}(K_\mathfrak{m}/K)$ *sends every* $[v]$, *where* $v \in V_{K,f}, v \nmid \mathfrak{m}$, *to* Frob_v.

(3) *If* $\mathfrak{m}|\mathfrak{m}'$, *then* $K_\mathfrak{m} \subset K_{\mathfrak{m}'}$. *We have a commutative diagram*

$$\begin{tikzcd}
\mathrm{Cl}_{\mathfrak{m}'}(K) \arrow[r, "\psi_{K_{\mathfrak{m}'}/K}", "\sim"'] \arrow[d] & \mathrm{Gal}(K_{\mathfrak{m}'}/K) \arrow[d, "\mathrm{res}"] \\
\mathrm{Cl}_\mathfrak{m}(K) \arrow[r, "\psi_{K_\mathfrak{m}/K}", "\sim"'] & \mathrm{Gal}(K_\mathfrak{m}/K)
\end{tikzcd}$$

where the vertical arrow on the left is the natural map.

(4) *For any two moduli* $\mathfrak{m}, \mathfrak{m}'$, *we have* $K_\mathfrak{m} \cap K_{\mathfrak{m}'} = K_{\gcd(\mathfrak{m},\mathfrak{m}')}$. *Here the* gcd *of two moduli are defined in the obvious way.*

Proof. (1) For any finite abelian extension L/K, the subgroup $H = \mathrm{N}_{L/K}(C_L) \subset C_K$ is open. Hence its preimage in $\mathbb{A}_K^\times$ is open, and it contains $U_\mathfrak{m}$ for some $\mathfrak{m}$ by Exercise 4.7.3. Then H contains $\bar{U}_\mathfrak{m}$, and so L is contained in $K_\mathfrak{m}$ since the bijection in Corollary 4.2.8 is inclusion-reversing.

(2) For $v \in V_K$ not dividing $\mathfrak{m}$, to show that v is unramified in $K_{\mathfrak{m}}$ we need to show that the image of $K_{v,>0}$ in C_K is contained in $\bar{U}_{\mathfrak{m}}$ when v is archimedean and that the image of $\mathcal{O}_{K_v}^\times$ in C_K is contained in $\bar{U}_{\mathfrak{m}}$ when v is non-archimedean, in view of Theorem 4.2.1. This follows directly from the definition of $U_{\mathfrak{m}}$.

(3) Since $U_{\mathfrak{m}} \supset U_{\mathfrak{m}'}$, we have $K_{\mathfrak{m}} \subset K_{\mathfrak{m}'}$. By Remark 4.7.9, in the diagram

$$\begin{tikzcd}
(\mathbb{A}_K^{S'})^\times \arrow[r, two heads] \arrow[d, hook] & C_K/U_{\mathfrak{m}'} \arrow[r, "\sim"] \arrow[d] & \mathrm{Cl}_{\mathfrak{m}'}(K) \arrow[d] \\
(\mathbb{A}_K^{S})^\times \arrow[r, two heads] & C_K/U_{\mathfrak{m}} \arrow[r, "\sim"] & \mathrm{Cl}_{\mathfrak{m}}(K)
\end{tikzcd}$$

the outer square commutes. Here $S = V_{K,\infty} \cup \{v \in V_{K,f} \mid v \nmid \mathfrak{m}\}$, $S' = V_{K,\infty} \cup \{v \in V_{K,f} \mid v \nmid \mathfrak{m}'\}$, and the vertical arrow in the middle is induced by identity on C_K. Since the first horizontal map in each row is surjective, and since the left hand side square commutes, it follows that the right hand side square commutes. The desired statement then follows.

(4) Let $L_1/K, L_2/K$ be finite abelian extensions in K^{ab}. Let $L = L_1 \cap L_2$. Let $H_i = \mathrm{N}_{L_i/K}(C_{L_i})$ and $H = \mathrm{N}_{L/K}(C_L)$. Since $H = \ker \psi_{L/K}, H_i = \ker \psi_{L_i/K}$, and $\mathrm{Gal}(K^{\mathrm{ab}}/L) = \mathrm{Gal}(K^{\mathrm{ab}}/L_1) \cdot \mathrm{Gal}(K^{\mathrm{ab}}/L_2)$, we have $H = H_1 \cdot H_2$. By this general fact, for (4) it suffices to prove that $U_{\gcd(\mathfrak{m},\mathfrak{m}')} = U_{\mathfrak{m}} \cdot U_{\mathfrak{m}'}$. This can be checked directly from the definition. □

Let L/K be a finite abelian extension in K^{ab}. By Proposition 4.7.11 (1) and (4), there exists a unique minimal modulus $\mathfrak{m}$ such that $L \subset K_{\mathfrak{m}}$. Namely, $\mathfrak{m}$ is the gcd of all moduli $\mathfrak{n}$ such that $L \subset K_{\mathfrak{n}}$. We call this $\mathfrak{m}$ the *conductor* of L/K, and denote it by $\mathfrak{f}_{L/K}$.

Proposition 4.7.12. *A place of K divides $\mathfrak{f}_{L/K}$ if and only if it ramifies in L.*

Proof. Let v be a place of K not dividing $\mathfrak{f}_{L/K}$. Then by Proposition 4.7.11 (2), v is unramified in $K_{\mathfrak{f}_{L/K}}$. But $L \subset K_{\mathfrak{f}_{L/K}}$, so v is unramified in L.

Conversely, suppose v is a place of K which is unramified in L. Let $\mathfrak{m}$ be a modulus of K such that $L \subset K_{\mathfrak{m}}$. Then $H := \mathrm{N}_{L/K}(C_L)$ contains $\mathrm{N}_{K_{\mathfrak{m}}/K}(C_{K_{\mathfrak{m}}}) = \bar{U}_{\mathfrak{m}}$. By Theorem 4.2.1, $H = \ker \psi_{L/K}$ and $\psi_{L/K}$ kills the image of $\mathcal{O}_{K_v}^\times$ (resp. $K_v^\times$) in C_K when v is non-archimedean (resp. real), we know that H contains the image of $\mathcal{O}_{K_v}^\times$ (resp. $K_v^\times$) in C_K. Let $\mathfrak{n}$ be the modulus obtained from $\mathfrak{m}$ by deleting the power of v. Then $U_{\mathfrak{n}}$ is generated by $U_{\mathfrak{m}}$ and the image of $\mathcal{O}_{K_v}^\times$ (resp. $K_v^\times$) in $\mathbb{A}_K^\times$. Hence $U_{\mathfrak{n}} \subset H$, and it follows that $L \subset K_{\mathfrak{n}}$. Therefore $\mathfrak{f}_{L/K}$ divides $\mathfrak{n}$, and v does not divide $\mathfrak{f}_{L/K}$. □

Definition 4.7.13. Let L/K be a finite abelian extension in K^{ab}. A modulus $\mathfrak{m}$ of K is said to be *admissible for L/K*, if it satisfies the following two conditions:

(1) Every finite place v of K not dividing $\mathfrak{m}$ is unramified in L.

(2) By (1), define the map $I_K^{(\mathfrak{m})} = \mathbb{Z}[v \in V_{K,f}, v \nmid \mathfrak{m}] \to \mathrm{Gal}(L/K), [v] \mapsto \mathrm{Frob}_v$. This maps factors through $\mathrm{Cl}_{\mathfrak{m}}(K)$.

When this is the case, we call the map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$ the Artin map.

This definition does not rely on any knowledge about class field theory. One can think of this definition as an "explicit" relation between $\mathfrak{m}$ and L/K.

Proposition 4.7.14. *A modulus $\mathfrak{m}$ is admissible for L/K if and only if $L \subset K_{\mathfrak{m}}$.*

Proof. Suppose $L \subset K_{\mathfrak{m}}$. Then every finite place v not dividing $\mathfrak{m}$ is unramified in $K_{\mathfrak{m}}$ by Proposition 4.7.11 (2), and hence unramified in L. The map $I_K^{(\mathfrak{m})} \to \mathrm{Gal}(L/K), [v] \mapsto \mathrm{Frob}_v$

factors as

$$I_K^{(\mathfrak{m})} \to \mathrm{Cl}_{\mathfrak{m}}(K) \xrightarrow{\psi_{K_{\mathfrak{m}}/K}} \mathrm{Gal}(K_{\mathfrak{m}}/K) \to \mathrm{Gal}(L/K).$$

Hence $\mathfrak{m}$ is admissible for L/K.

Conversely, suppose $\mathfrak{m}$ is admissible for L/K. Let $\mathfrak{n}$ be a modulus of K such that $\mathfrak{m}|\mathfrak{n}$ and $L \subset K_{\mathfrak{n}}$. In particular, we also have $K_{\mathfrak{m}} \subset K_{\mathfrak{n}}$. Consider the diagram

$$\begin{tikzcd}
\mathrm{Cl}_{\mathfrak{n}}(K) \arrow[r, "\psi_{K_{\mathfrak{n}}/K}", "\sim"'] \arrow[d] & \mathrm{Gal}(K_{\mathfrak{n}}/K) \arrow[d, "\mathrm{res}"] \arrow[rdd, "\mathrm{res}"] & \\
\mathrm{Cl}_{\mathfrak{m}}(K) \arrow[r, "\psi_{K_{\mathfrak{m}}/K}", "\sim"'] \arrow[rrd, "f"'] & \mathrm{Gal}(K_{\mathfrak{m}}/K) & \\
& & \mathrm{Gal}(L/K)
\end{tikzcd}$$

Here the map f is the Artin map which exists since $\mathfrak{m}$ is admissible for L/K. The left upper square commutes. The outer diagram also commutes, as can be checked on each generator $[v]$ (with $v \in V_{K,f}, v \nmid \mathfrak{n}$) of $\mathrm{Cl}_{\mathfrak{n}}(K)$. Since $\psi_{K_{\mathfrak{n}}/K}$ and $\psi_{K_{\mathfrak{m}}/K}$ are isomorphisms, it follows that the restriction map $\mathrm{Gal}(K_{\mathfrak{n}}/K) \to \mathrm{Gal}(L/K)$ factors through the restriction map $\mathrm{Gal}(K_{\mathfrak{n}}/K) \to \mathrm{Gal}(K_{\mathfrak{m}}/K)$. By Galois theory, this means that $L \subset K_{\mathfrak{m}}$. □

The following result characterizes the ray class field $K_{\mathfrak{m}}$ "explicitly".

Corollary 4.7.15. *Let $\mathfrak{m}$ be a modulus of K. The extension $K_{\mathfrak{m}}/K$ is the unique finite abelian extension L/K in K^{ab} such that $\mathfrak{m}$ is admissible for L/K and such that the Artin map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$ is an isomorphism.*

Exercise 4.7.16. Let $\mathfrak{m}$ be a modulus $\mathbb{Q}$ of the form $\mathfrak{m} = \infty m$, as in Example 4.7.7. Use the above corollary to show that the ray class field corresponding to $\mathfrak{m}$ is $\mathbb{Q}(\zeta_m)$.

Definition 4.7.17. Let L/K be a finite abelian extension. Let $\mathfrak{m}$ be a modulus of K. Let $\mathrm{N}_{L/K}(\mathfrak{m})$ denote the subgroup of $\mathrm{Cl}_{\mathfrak{m}}(K)$ generated by elements of the form $f(L/v)[v]$, where $v \in V_{K,f}, v \nmid \mathfrak{m}$, and $f(L/v) = f(w/v)$ for any $w \in V_L$ above v.

Exercise 4.7.18. Let L/K be a finite abelian extension. The image of the composite map

$$C_L \xrightarrow{\mathrm{N}_{L/K}} C_K \to C_K/\bar{U}_{\mathfrak{m}} \cong \mathrm{Cl}_{\mathfrak{m}}(K)$$

is $\mathrm{N}_{L/K}(\mathfrak{m})$.

Proposition 4.7.19. *Let L/K be a finite abelian extension. Let $\mathfrak{m}$ be a modulus of K admissible for L/K. Then the Artin map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$ is surjective with kernel $\mathrm{N}_{L/K}(\mathfrak{m})$.*

Proof. This directly follows from Theorem 4.2.1 and Exercise 4.7.18. □

We summarize what we have proved in the following theorem, which is the ideal theoretic formulation of global class field theory.

Theorem 4.7.20. *Let K be a number field. The following statements hold.*

(1) *(Reciprocity Law.) For every finite abelian extension L/K, there is a modulus $\mathfrak{m}$ of K which is admissible for L/K. The Artin map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$ is surjective with kernel $\mathrm{N}_{L/K}(\mathfrak{m})$.*

(2) *(Existence Theorem.) For every modulus $\mathfrak{m}$, there is a unique finite abelian extension $K_{\mathfrak{m}}/K$ such that $\mathfrak{m}$ is admissible for $K_{\mathfrak{m}}$ and the Artin map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$ is an isomorphism.*

(3) *(Abstract Kronecker–Weber.) We have $K^{\mathrm{ab}} = \bigcup_{\mathfrak{m}} K_{\mathfrak{m}}$. Moreover, a finite abelian extension L/K in K^{ab} is contained in $K_{\mathfrak{m}}$ if and only if $\mathfrak{m}$ is admissible for L/K.*

(4) *Let L/K be a finite abelian extension. The conductor $\mathfrak{f}_{L/K}$, defined as the gcd of all admissible moduli for L/K, is divisible precisely by the places of K which ramify in L.*

5. Applications

5.1. Hilbert class field.

Let K be a number field. Let H/K be the ray class field corresponding to the trivial modulus. This is called the *Hilbert class field* of K. We have a canonical isomorphism $\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}(H/K)$. In particular, the degree $[H : K]$ is equal to the class number $h_K = |\,\mathrm{Cl}(K)|$ of K.

Similarly, let H^+/K be the ray class field corresponding to the modulus which is the product of all real places of K. This is called the *narrow Hilbert class field* of K. The ray class group in this case is the so-called *narrow class group* $\mathrm{Cl}(K)^+$ of K, namely the quotient of the group of all fractional ideals by the group of principal ideals generated by $x \in K^\times$ such that for every embedding $K \hookrightarrow \mathbb{R}$ the image of x is positive. (Such elements x are called totally positive.) We have a canonical isomorphism $\mathrm{Cl}(K)^+ \xrightarrow{\sim} \mathrm{Gal}(H^+/K)$.

Clearly H is contained in every ray class field of K, and in particular $H \subset H^+$.

The characterizations in the next proposition are the "original" definitions of Hilbert class field and narrow Hilbert class field.

Proposition 5.1.1. *The Hilbert class field H of K is the unique maximal abelian extension of K which is unramified at all places of K. The narrow Hilbert class field H^+ of K is the unique maximal abelian extension of K which is unramified at all finite places of K.*

Proof. Clearly H (resp. H^+) is unramified over all (resp. all finite) places of K. If L/K is another such finite abelian extension, then $\mathfrak{f}_{L/K}$ is trivial (resp. a product of some real places) since it is divisible precisely by the places which ramify in L. Hence $K_{\mathfrak{f}_{L/K}} = H$ (resp. $K_{\mathfrak{f}_{L/K}} \subset H^+$). Since $L \subset K_{\mathfrak{f}_{L/K}}$, we have $L \subset H$ (resp. $L \subset H^+$). □

The Hilbert class field can be used to prove the following interesting statement about class numbers.

Theorem 5.1.2. *Let L/K be a finite extension of number fields. Assume that there is a place v of K which is totally ramified in L, i.e., there is a unique place w of L above v, and L_w/K_v is totally ramified (for v archimedean this means L_w/K_v is $\mathbb{C}/\mathbb{R}$, and in particular $[L : K] = 2$). Then h_K divides h_L.*

Proof. Fix an embedding $L^{\mathrm{ab}} \hookrightarrow \overline{K}$. Let H_K be the Hilbert class field of K, and H_L the Hilbert class field of L. All the fields K, L, H_K, H_L are inside $\overline{K}$. Since H_K/K is finite abelian and everywhere unramified, $H_K \cdot L/L$ is also finite abelian and everywhere unramified. Hence $H_K \cdot L \subset H_L$ by the characterization of H_L. It follows that $h_L = [H_L : L]$ is divisible by $[H_K \cdot L : L]$. We now claim that $[H_K \cdot L : L] = h_K$.

The place v is both unramified and totally ramified in $H_K \cap L$, so $H_K \cap L = K$. Write $H_K = K(\alpha)$, and let $f(X) \in K[X]$ be the minimal polynomial of α over K. Then $\deg f = [H_K : K] = h_K$. To prove the claim it suffices to show that f is irreducible over L. Now f splits over H_K since H_K/K is Galois, and so every factor h of f in $L[X]$ is the product of some linear factors of f in $H_K[X]$. Hence $h \in (H_K \cap L)[X] = K[X]$, and this proves that f is still irreducible over L. □

For any finite extension of number fields L/K, there is a natural map $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ sending the class of a fractional ideal $\mathfrak{a}$ to the class of the fractional ideal $\mathfrak{a}\mathcal{O}_L$.

Exercise 5.1.3. If we canonically identify $\mathrm{Cl}(K)$ as $C_K/\bar{U}_1$ and $\mathrm{Cl}(L)$ as $C_L/\bar{U}_1$ (where 1 stands for the trivial modulus), then the natural map $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ is induced by the natural map $C_K \hookrightarrow C_L$ (which is induced by $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_L^\times$).

Theorem 5.1.4 (Artin's Principal Ideal Theorem)**.** *Let H be the Hilbert class field of K. Then the natural map $\mathrm{Cl}(K) \to \mathrm{Cl}(H)$ is trivial. In other words, for every non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a}\mathcal{O}_H$ is a principal ideal of $\mathcal{O}_H$.*

For the proof, we need to recall the transfer functoriality of the global Artin map. In Theorem 4.4.4, this was stated with infinite Galois groups. We now state a version involving finite Galois groups, which immediately follows from Theorem 4.4.4.

Let M/K be a finite Galois extension in $\overline{K}$. Let L/K be a finite extension in M. Let K_1/K be the maximal abelian subextension of M/K, and let L_1/L be the maximal abelian subextension of M/L. Thus $\mathrm{Gal}(K_1/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}}$, and $\mathrm{Gal}(L_1/L) = \mathrm{Gal}(M/L)^{\mathrm{ab}}$. Since $\mathrm{Gal}(M/L)$ is a subgroup of $\mathrm{Gal}(M/K)$, we have the transfer map

$$V : \mathrm{Gal}(K_1/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}} \to \mathrm{Gal}(L_1/L) = \mathrm{Gal}(M/L)^{\mathrm{ab}}.$$

The transfer functoriality now states that the following diagram commutes:

$$\begin{tikzcd}
C_L \arrow[r, "\psi_{L_1/L}"] & \mathrm{Gal}(L_1/L) \\
C_K \arrow[u, hook] \arrow[r, "\psi_{K_1/K}"] & \mathrm{Gal}(K_1/K) \arrow[u, "V"]
\end{tikzcd}$$

Another ingredient needed in the proof of Theorem 5.1.4 is the following result in group theory, called the "Principal Ideal Theorem in group theory". We take it as a black box. For references, see [Mil20, V.3.19].

Theorem 5.1.5. *Let G be a finite group, with derived subgroup G_{der}. Then the transfer map $G^{\mathrm{ab}} \to (G_{\mathrm{der}})^{\mathrm{ab}}$ is trivial.*

Proof of Theorem 5.1.4. Let H' be the Hilbert class field of H, taken inside $\overline{K}$. Then H' is the maximal finite abelian everywhere unramified extension of H in $\overline{K}$. Since H/K is Galois, every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ stabilizes H. Then by the characterization of H', σ also stabilizes H'. Hence H'/K is Galois. Every subextension L/K in H' is everywhere unramified. Hence by the characterization of H, we know that H is the maximal abelian extension of K inside H'/K. By the above discussion on transfer functoriality applied to $M = H', L = H, K_1 = H, L_1 = H'$, and by Exercise 5.1.3, we have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Cl}(L) \arrow[r, "\sim"] & \mathrm{Gal}(H'/H) \\
\mathrm{Cl}(K) \arrow[u] \arrow[r, "\sim"] & \mathrm{Gal}(H/K) \arrow[u, "V"]
\end{tikzcd}$$

It remains to show that $V : \mathrm{Gal}(H/K) \to \mathrm{Gal}(H'/H)$ is trivial. Since $\mathrm{Gal}(H/K) = \mathrm{Gal}(H'/K)^{\mathrm{ab}}$, we have $\mathrm{Gal}(H'/H) = \mathrm{Gal}(H'/K)_{\mathrm{der}}$. Thus V being trivial is a special case of Theorem 5.1.5. □

5.2. **Weber L-functions.** Let K be a number field. The Dedekind zeta function for K is defined as

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} (\mathrm{N}\mathfrak{a})^{-s}.$$

Here $\mathfrak{a}$ runs over non-zero integral ideals, and $\mathrm{N}\mathfrak{a} := [\mathcal{O}_K : \mathfrak{a}]$. The variable s is a complex variable. We shall see that the infinite series converges to an analytic function on $\mathrm{Re}(s) > 1$, has meromorphic continuation to $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, and is analytic there except a simple pole at $s = 1$. By the unique factorization into prime ideals, we have

$$\zeta_K(s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - (\mathrm{N}\mathfrak{p})^{-s}}, \quad \mathrm{Re}(s) > 1.$$

We consider the following more refined version.

Definition 5.2.1. Let $\mathfrak{m}$ be a modulus, and let $\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}(K)$. Define the *partial zeta function*

$$\zeta_{K,\mathfrak{m}}(s, \mathfrak{K}) = \sum_{\mathfrak{a} \subset \mathcal{O}_K, \mathfrak{a} \in \mathfrak{K}} (\mathrm{N}\mathfrak{a})^{-s}.$$

Here $\mathfrak{a}$ runs over the integral ideals which are coprime to $\mathfrak{m}$ and whose class in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is $\mathfrak{K}$.

Theorem 5.2.2. *The series defining* $\zeta_{K,\mathfrak{m}}(s, \mathfrak{K})$ *converges to an analytic function on* $\mathrm{Re}(s) > 1$. *Moreover,* $\zeta_{K,\mathfrak{m}}(s, \mathfrak{K})$ *has meromorphic continuation to* $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, *and is analytic there except a simple pole at* $s = 1$. *The residue at* $s = 1$ *is a positive real number depending only on* $\mathfrak{m}$, *not on* $\mathfrak{K}$. *Denote the residue by* $\rho_{\mathfrak{m}}$.

We postpone the proof. Later we will also give an explicit formula for $\rho_{\mathfrak{m}}$.

The relationship between the partial zeta functions and the Dedekind zeta function is that when $\mathfrak{m} = 1$, we have

$$\zeta_K(s) = \sum_{\mathfrak{K} \in \mathrm{Cl}(K)} \zeta_{K,1}(s, \mathfrak{K}).$$

In particular, Theorem 5.2.2 implies the properties of $\zeta_K(s)$ stated above, and moreover the residue of $\zeta_K(s)$ at $s = 1$ is equal to $h_K \cdot \rho_1$.

Remark 5.2.3. In fact, $\zeta_{K,\mathfrak{m}}(s, \mathfrak{K})$ (and hence $\zeta_K(s)$) has meromorphic continuation to the whole complex plane and satisfies a functional equation. We will not prove it in this course.

Recall that for a finite abelian group G, its *Pontryagin dual* is the abelian group of characters $G^\vee = \mathrm{Hom}(G, \mathbb{C}^\times) = \mathrm{Hom}(G, S^1)$. By the classification of finite abelian groups, it is easy to see that $G^\vee$ is non-canonically isomorphic to G. The canonical double dual map $G \to (G^\vee)^\vee$ is an isomorphism. We have

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \chi = 1 \in G^\vee, \\ 0, & \chi \in G^\vee - \{1\}; \end{cases} \qquad \sum_{\chi \in G^\vee} \chi(g) = \begin{cases} |G|, & g = 1 \in G, \\ 0, & g \in G - \{1\}. \end{cases}$$

Definition 5.2.4. For $\chi \in \mathrm{Cl}_{\mathfrak{m}}(K)^\vee$, define the *Weber L-function*

$$L_{K,\mathfrak{m}}(s, \chi) = \sum_{\mathfrak{a} \subset \mathcal{O}_K, \text{coprime to } \mathfrak{m}} \chi(\mathfrak{a})(\mathrm{N}\mathfrak{a})^{-s} = \sum_{\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}(K)} \chi(\mathfrak{K}) \zeta_{K,\mathfrak{m}}(s, \mathfrak{K}).$$

Corollary 5.2.5. *The function* $L_{K,\mathfrak{m}}(s, \chi)$ *is meromorphic on* $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, *and is analytic away from* $s = 1$. *If* $\chi \neq 1$, *then it is analytic at* $s = 1$. *If* $\chi = 1$, *then it has a simple pole at* $s = 1$, *with residue* $|\mathrm{Cl}_{\mathfrak{m}}(K)| \cdot \rho_{\mathfrak{m}}$.

Proof. This follows from Theorem 5.2.2 as the residue at $s = 1$ is given by $\rho_{\mathfrak{m}} \sum_{\mathfrak{K}\in \mathrm{Cl}_{\mathfrak{m}}(K)} \chi(\mathfrak{K})$. □

Example 5.2.6. Again by the unique factorization into prime ideals and the multiplicativity of χ, we have

$$L_{K,\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\text{ prime},\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s}}, \quad \mathrm{Re}(s) > 1.$$

In particular,

$$L_{K,\mathfrak{m}}(s,1) = \sum_{\mathfrak{K}\in\mathrm{Cl}_{\mathfrak{m}}(K)} \zeta_{K,\mathfrak{m}}(s,\mathfrak{K}) = \prod_{\mathfrak{p}\text{ prime},\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-(\mathrm{N}\mathfrak{p})^{-s}} = \zeta_K(s) \prod_{\mathfrak{p}\text{ prime},\mathfrak{p}\mid\mathfrak{m}} (1-(\mathrm{N}\mathfrak{p})^{-s}).$$

The function $\prod_{\mathfrak{p}\text{ prime},\mathfrak{p}\mid\mathfrak{m}}(1-(\mathrm{N}\mathfrak{p})^{-s})$ is of course an entire function on $\mathbb{C}$ and its zeros are well understood. Hence the analytic property of $L_{K,\mathfrak{m}}(s,1)$ is closely related to that of $\zeta_K(s)$. For instance, comparing the residues at $s=1$ we obtain

$$|\,\mathrm{Cl}_{\mathfrak{m}}(K)| \cdot \rho_{\mathfrak{m}} = h_K \cdot \rho_1 \cdot \prod_{\mathfrak{p}\text{ prime},\mathfrak{p}\mid\mathfrak{m}} (1-(\mathrm{N}\mathfrak{p})^{-1}). \tag{5.1}$$

Example 5.2.7. Let $\mathfrak{m} = \infty m$ be a modulus for $\mathbb{Q}$, as in Example 4.7.7. Then $\mathrm{Cl}_{\mathfrak{m}}(G) = (\mathbb{Z}/m\mathbb{Z})^{\times}$. For a character χ on this group, the associated Weber L-function is the classical Dirichlet L-function

$$L(s,\chi) = \sum_{n\geq 1,(n,m)=1} \chi(n)n^{-s} = \prod_{p,p\nmid m} \frac{1}{1-\chi(p)p^{-s}}.$$

The following result is where we use class field theory.

Lemma 5.2.8. *Let E/K be a finite abelian extension. Let $\mathfrak{m}$ be a modulus admissible for E/K. Let $\mathfrak{n}$ be the modulus of E that is the product of all the finite places of E which divide places of K appearing in $\mathfrak{m}$. Then*

$$L_{E,\mathfrak{n}}(s,1) = \prod_{\chi\in\mathrm{Gal}(E/K)^{\vee}} L_{K,\mathfrak{m}}(s,\tilde{\chi}).$$

Here $\tilde{\chi}$ is the composition of $\chi : \mathrm{Gal}(E/K) \to \mathbb{C}^{\times}$ with the Artin map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(E/K)$.

Proof. A prime ideal of E is coprime to $\mathfrak{n}$ if and only if it is over a prime ideal of K coprime to $\mathfrak{m}$. Let $\mathfrak{p}$ be a prime ideal of K coprime to $\mathfrak{m}$. Since $\mathfrak{m}$ is admissible for E/K, $\mathfrak{p}$ is unramified in E. Thus $\mathfrak{p}\mathcal{O}_E = \mathfrak{q}_1\cdots\mathfrak{q}_g$ where the $\mathfrak{q}_i$ are distinct prime ideals of E. It suffices to check that

$$\prod_{i=1}^{g} \frac{1}{1-(\mathrm{N}\mathfrak{q}_i)^{-s}} = \prod_{\chi\in\mathrm{Gal}(E/K)^{\vee}} \frac{1}{1-\tilde{\chi}(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s}}. \tag{5.2}$$

We shall proceed somewhat formally and ignore the necessary analytic justifications. Taking the logarithm of the left hand side, we obtain

$$\sum_{i=1}^{g}\sum_{n=1}^{\infty}(\mathrm{N}\mathfrak{q}_i)^{-sn}/n = g\sum_{n=1}^{\infty} y^{fn}/n,$$

where $y = (\mathrm{N}\mathfrak{p})^{-s}$, and $f = f(\mathfrak{q}_i/\mathfrak{p}) = [E:K]/g$. The logarithm of the right hand side of (5.2) is

$$\sum_{\chi\in\mathrm{Gal}(E/K)^{\vee}}\sum_{n=1}^{\infty}\tilde{\chi}(\mathfrak{p})^n y^n/n = \sum_{n=1}^{\infty}(\sum_{\chi\in\mathrm{Gal}(E/K)^{\vee}} \mu_n(\chi))y^n/n.$$

Here μ_n is the character on $\mathrm{Gal}(E/K)^\vee$ sending χ to $\tilde{\chi}(\mathfrak{p})^n$. Note that $\tilde{\chi}(\mathfrak{p})^n = \chi(\mathrm{Frob}_\mathfrak{p})^n$, and $\mathrm{Frob}_\mathfrak{p}$ has order f in $\mathrm{Gal}(E/K)$. Thus μ_n is trivial precisely when n is divisible by f. Thus the above is equal to

$$\sum_{n\geq 1,\ f|n} [E:K]y^n/n = \sum_{n=1}^{\infty}[E:K]y^{fn}/fn = g\sum_{n=1}^{\infty} y^{fn}/n,$$

as desired. □

Theorem 5.2.9. *Let $\chi \in \mathrm{Cl}_\mathfrak{m}(K)^\vee$ be non-trivial. Then $L_{K,\mathfrak{m}}(s,\chi)$ is analytic and non-zero at $s=1$.*

Proof. In Lemma 5.2.8, take E to be the ray class field $K_\mathfrak{m}$. Then we get

$$L_{E,\mathfrak{n}}(s,1) = \prod_{\chi\in \mathrm{Cl}_\mathfrak{m}(K)^\vee} L_{K,\mathfrak{m}}(s,\chi).$$

For $\chi \neq 1$, each $L_{K,\mathfrak{m}}(s,\chi)$ is analytic at $s=1$. Moreover both $L_{E,\mathfrak{n}}(s,1)$ and $L_{K,\mathfrak{m}}(s,1)$ have a simple pole at $s=1$. Hence $L_{K,\mathfrak{m}}(s,\chi)$ must be non-zero at $s=1$ for non-trivial χ, because otherwise the possible zeros will cancel with the pole of $L_{K,\mathfrak{m}}(s,1)$. □

5.3. **Digression: analytic properties of the partial zeta function.** We make an analytic digression in order to prove Theorem 5.2.2. We will also give an explicit formula for the residue $\rho_\mathfrak{m}$.

We first need some general facts about *Dirichlet series*, namely series of the form

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Here a_n are fixed complex numbers, and s is a complex variable.

Lemma 5.3.1. *If $f(s)$ converges for some $s_0 \in \mathbb{C}$, then it converges for all s such that $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, and the convergence is uniform on any compact subset of this region.*

Proof. We shall use the following form of summation by parts: If $\{x_n\}_{n\geq 1}, \{y_n\}_{n\geq 1}$ are two sequences, and if $X_N = \sum_{n=1}^N x_n$, then for $N > M \geq 1$ we have

$$\sum_{n=M+1}^{N} x_n y_n = X_N y_N - X_M y_{M+1} + \sum_{n=M+1}^{N-1} X_n(y_n - y_{n+1}).$$

Let $P_N(s) = \sum_{n=1}^N a_n n^{-s}$. Suppose $\mathrm{Re}(s) > \mathrm{Re}(s_0)$. We need to show that $\{P_N(s)\}_N$ is a Cauchy sequence. For $N > M$, we apply summation by parts to

$$P_N(s) - P_M(s) = \sum_{n=M+1}^{N} \frac{a_n}{n^{s_0}}\frac{1}{n^{s-s_0}}.$$

Taking $x_n = a_n/n^{s_0}$ and $y_n = 1/n^{s-s_0}$, we get

$$(5.3)\quad P_N(s) - P_M(s) = \frac{P_N(s_0)}{N^{s-s_0}} - \frac{P_M(s_0)}{(M+1)^{s-s_0}} + \sum_{n=M+1}^{N-1} P_n(s_0)\left(\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}}\right)$$

$$= \frac{P_N(s_0)}{N^{s-s_0}} - \frac{P_M(s_0)}{(M+1)^{s-s_0}} + \sum_{n=M+1}^{N-1} P_n(s_0)(s-s_0)\int_n^{n+1}\frac{dx}{x^{s-s_0+1}}.$$

The terms

$$\left|\frac{P_N(s_0)}{N^{s-s_0}}\right| = \frac{|P_N(s_0)|}{N^{\mathrm{Re}(s-s_0)}} \quad \text{and} \quad \left|\frac{P_M(s_0)}{(M+1)^{s-s_0}}\right| = \frac{|P_M(s_0)|}{(M+1)^{\mathrm{Re}(s-s_0)}}$$

tend to zero as $N, M \to \infty$, and the convergence is uniform if s stays in a compact set in $\{\mathrm{Re}(s) > \mathrm{Re}(s_0)\}$. If s stays in such a compact set, then $\mathrm{Re}(s - s_0) \geq \delta$ for some $\delta > 0$, and $|s - s_0| \leq A$ for some $A > 0$. Let $C = A \cdot \sup_{n\geq 1} |P_n(s_0)|$, which is finite since $f(s_0)$ converges. Then

$$\left|\sum_{n=M+1}^{N-1} P_n(s_0)(s-s_0)\int_n^{n+1}\frac{dx}{x^{s-s_0+1}}\right| \leq C\sum_{n=M+1}^{N-1}\int_n^{n+1}\frac{dx}{x^{1+\delta}} \leq C\int_{M+1}^{+\infty}\frac{dx}{x^{1+\delta}}.$$

This tends to zero as $N, M \to \infty$, and the convergence is uniform on the given compact set. □

Define $\sigma_0 \in [-\infty, +\infty]$ to be $\inf\{\mathrm{Re}(s) \mid f(s) \text{ converges}\}$. This is called the *abscissa of convergence* of the Dirichlet series $f(s)$. Then $f(s)$ converges for all $\mathrm{Re}(s) > \sigma_0$ and diverges for all $\mathrm{Re}(s) < \sigma_0$. The convergence in $\mathrm{Re}(s) > \sigma_0$ is uniform on compact sets, and therefore $f(s)$ is an analytic function on this region.

Lemma 5.3.2. *Let $A_n = \sum_{k=1}^n a_n$. Suppose there exist $C > 0$ and $\sigma_1 \geq 0$ such that $|A_n| \leq Cn^{\sigma_1}$ for all n, then $f(s) = \sum_{n=1}^\infty a_n n^{-s}$ converges for $\mathrm{Re}(s) > \sigma_1$.*

Proof. In (5.3), take $s_0 = 0$. Note that $P_N(s_0) = A_N$. Then we get

$$P_N(s) - P_M(s) = \frac{A_N}{N^s} - \frac{A_M}{(M+1)^s} + \sum_{n=M+1}^{N-1} A_n s\int_n^{n+1}\frac{dx}{x^{s+1}}.$$

The terms

$$\left|\frac{A_N}{N^s}\right| = \frac{|A_N|}{N^{\mathrm{Re}(s)}} \quad \text{and} \quad \left|\frac{A_M}{(M+1)^s}\right| = \frac{|A_M|}{(M+1)^{\mathrm{Re}(s)}}$$

tend to zero as $N, M \to \infty$, when $\mathrm{Re}(s) > \sigma_1$. We have

$$\begin{aligned}\left|\sum_{n=M+1}^{N-1} A_n s\int_n^{n+1}\frac{dx}{x^{s+1}}\right| &\leq \sum_{n=M+1}^{N-1}|s|C\int_n^{n+1}\frac{n^{\sigma_1}}{x^{\sigma_1}}\frac{1}{x^{1+\mathrm{Re}(s)-\sigma_1}}dx \\ &\leq |s|C\sum_{n=M+1}^{N-1}\int_n^{n+1}\frac{dx}{x^{1+\mathrm{Re}(s)-\sigma_1}} \leq |s|C\int_{M+1}^{+\infty}\frac{dx}{x^{1+\mathrm{Re}(s)-\sigma_1}}.\end{aligned}$$

This tends to zero as $N, M \to \infty$, when $\mathrm{Re}(s) > \sigma_1$. □

Remark 5.3.3. Suppose that $f(s) = \sum_{n\geq 1} a_n n^{-s}$ converges at some s_0. Then $a_n n^{-s_0} \to 0$, so $a_n = o(n^{\mathrm{Re}(s_0)})$. Then by comparing with the series $\sum_{n\geq 1} n^{-(1+\delta)}$ (with $\delta > 0$ arbitrary), we know that $f(s)$ converges *absolutely* for $\mathrm{Re}(s) \geq \mathrm{Re}(s) + 1 + \delta$. Thus if σ_0 is the abscissa of convergence, then $f(s)$ converges *absolutely* for $\mathrm{Re}(s) \geq \sigma_0 + 1$. In practice, suppose we want to check some algebraic relation between several Dirichlet series on $\mathrm{Re}(s) > \sigma_0$ where σ_0 is the maximum of their abscissa of convergence. Since they are all analytic on this region, it suffices to check the relation on $\mathrm{Re}(s) > \sigma_0 + 1$ (by the uniqueness of analytic continuation), and so we may assume that the Dirichlet series in question are all absolutely convergent. This allows us to justify operations such as reordering the infinite sums.

Example 5.3.4. The Riemann zeta function $\zeta(s) = \sum_{n\geq 1} n^{-s}$, as a Dirichlet series, converges for $\mathrm{Re}(s) > 1$, since the partial sums of the coefficients $A_n = n$. It diverges for $s = 1$, so the abscissa of convergence is 1.

For an integer $r \geq 2$, consider $\zeta_r(s) = \sum_{n\geq 1} a_n n^{-s}$, where

$$a_n = \begin{cases} 1, & r \nmid n; \\ 1-r, & r|n. \end{cases}.$$

Then the partial sums of coefficients are bounded, so $\zeta_r(s)$ converges for $\mathrm{Re}(s) > 0$. By Remark 5.3.3, we may reorder the summation and get

$$(1 - \frac{1}{r^{s-1}})\zeta(s) = \sum_n n^{-s} - r\sum_n (nr)^{-s} = \sum_n n^{-s} - r\sum_n b_n n^{-s} = \zeta_r(s),$$

where $b_n = 0$ for $r \nmid n$ and $b_n = 1$ for $r|n$. Hence

$$\zeta(s) = (1 - \frac{1}{r^{s-1}})^{-1}\zeta_r(s)$$

has meromorphic continuation to $\mathrm{Re}(s) > 0$. The only possible poles of $\zeta(s)$ in this region are at s satisfying $r^{s-1} = 1$. Since this holds for all $r \in \mathbb{Z}_{\geq 1}$, we must have $s = 1$. Thus the only possible pole of $\zeta(s)$ in $\mathrm{Re}(s) > 0$ is at $s = 1$. By comparing with the integral $\int x^{-s}dx$, for real $s > 1$ we have

$$\zeta(s) \geq \int_1^{+\infty} x^{-s}dx = \frac{1}{s-1},$$

and

$$\zeta(s) - 1 \leq \int_1^{+\infty} x^{-s}dx = \frac{1}{s-1}.$$

Hence

$$1 \leq (s-1)\zeta(s) \leq s.$$

It follows that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1.

Theorem 5.3.5. *Consider a Dirichlet series $f(s) = \sum_{n\geq 1} a_n n^{-s}$ with partial sums of coefficients $A_n = \sum_{k=1}^n a_k$. Suppose there exist $\rho \in \mathbb{C}, C > 0, 0 \leq \sigma_1 < 1$, such that*

$$|A_n - \rho n| \leq Cn^{\sigma_1}.$$

In other words, $A_n = \rho n + O(n^{\sigma_1})$. Then $f(s)$ converges for $\mathrm{Re}(s) > 1$, has meromorphic continuation to $\mathrm{Re}(s) > \sigma_1$, and the only possible pole in this region is a simple at $s = 1$. The residue at $s = 1$ is ρ.

Proof. Apply Lemma 5.3.2 to the Dirichlet series $f(s) - \rho\zeta(s)$, and use the fact that $\zeta(s)$ is meromorphic on $\mathrm{Re}(s) > 0$ with a simple pole at $s = 1$ with residue 1. □

We now come to the partial zeta functions. Let K be a number field, $\mathfrak{m}$ a modulus, $\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}(K)$. Then $\zeta_{K,\mathfrak{m}}(s, \mathfrak{K})$ is given by the Dirichlet series $\sum_{n\geq 1} a_n n^{-s}$ where a_n is the number of integral ideals $\mathfrak{a} \subset \mathcal{O}_K$ such that $\mathfrak{a} \in \mathfrak{K}$ and $\mathrm{N}\mathfrak{a} = n$. The partial sum of coefficients is thus given by $A_n =$ the number of integral ideals $\mathfrak{a} \subset \mathcal{O}_K$ such that $\mathfrak{a} \in \mathfrak{K}$ and $\mathrm{N}\mathfrak{a} \leq n$. We denote this number by $j(\mathfrak{K}, n)$.

In order to apply Theorem 5.3.5, we need to find an asymptotic formula for $j(\mathfrak{K}, n)$ of the form $j(\mathfrak{K}, n) = \rho n + O(n^{\sigma_1})$. We will use the following lemma for this.

Lemma 5.3.6. *Let D be a (measurable) subset in $\mathbb{R}^N$ such that ∂D is $(N-1)$-Lipschitz parametrizable, in the sense that ∂D is a finite union of images of Lipschitz functions $\mathbb{R}^{N-1} \to \mathbb{R}^N$ (i.e., functions satisfying $\|\phi(x) - \phi(y)\| \leq C \cdot \|x - y\|$). Let L be a lattice in $\mathbb{R}^N$, and let $x_0 \in \mathbb{R}^N$. Then*

$$\#\big(tD \cap (x_0 + L)\big) = \frac{\mathrm{vol}(D)}{\mathrm{vol}(L)} t^N + O(t^{N-1}), \quad \mathbb{R} \ni t \to +\infty.$$

Here $\mathrm{vol}(D)$ is the N-dimensional Lebesgue measure of D, and $\mathrm{vol}(L)$ denotes the volume of a fundamental parallelepiped for L.

Proof. See [Lan94, VI.2, Thm. 2]. □

Let $N = [K : \mathbb{Q}]$. Let r_1 be the number of real places and r_2 be the number of complex places. Consider

$$B := \prod_{v \in V_{K,\infty}} K_v \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1 + 2r_2} = \mathbb{R}^N.$$

Inside it we have the open subset

$$J = \prod_{v \in V_{K,\infty}, v \mid \mathfrak{m}} K_{v,>0} \times \prod_{v \in V_{K,\infty}, v \nmid \mathfrak{m}} K_v^{\times}.$$

Then J is a group under multiplication. We embed K diagonally into B as usual. Then $K_{(\mathfrak{m})}^{\times}$ is contained in J. Let $G_{\mathfrak{m}} := K_{(\mathfrak{m})}^{\times} \cap \mathcal{O}_K^{\times}$. Since the embedding $G_{\mathfrak{m}} \to J$ is a group homomorphism, $G_{\mathfrak{m}}$ acts on J by translation. Since $G_{\mathfrak{m}}$ is clearly a finite index subgroup of $\mathcal{O}_K^{\times}$, and the latter is finitely generated of rank $r = r_1 + r_2 - 1$ by Dirichlet's unit theorem, we know that $G_{\mathfrak{m}}$ is finitely generated of rank r. Let V be a free abelian subgroup of rank r inside $G_{\mathfrak{m}}$ such that $G_{\mathfrak{m}} = V \oplus (\text{torsion})$. Let $w_{\mathfrak{m}} = [G_{\mathfrak{m}} : V] =$ the size of the torsion subgroup of $G_{\mathfrak{m}}$. Define

$$c : B \to \mathbb{R}, \quad (x_v)_{v \in V_{K,\infty}} \mapsto \prod_{v \in V_{K,\infty}} \|x_v\|_v.$$

Lemma 5.3.7. *The action of V on J has a fundamental domain E with the following properties:*

1. *For any $t > 0$, we have $tE = E$. Here scalar multiplication by t is with respect to the vector space structure on B.*
2. *For any $t > 0$, define $E(t) = \{x \in E \mid c(x) \leq t\}$. Thus by (1) we have $E(t) = t^{1/N} E(1)$. Let $D = E(1)$. Then ∂D is $(N-1)$-Lipschitz parametrizable.*
3. *The N-dimensional volume of D inside $B \cong \mathbb{R}^N$ is*

$$2^{r_1 - s(\mathfrak{m})} \pi^{r_2} R_{\mathfrak{m}},$$

where $s(\mathfrak{m})$ is the number of real places of K dividing $\mathfrak{m}$, and $R_{\mathfrak{m}}$ is the $\mathfrak{m}$-regulator defined as follows. Choose a set of free generators $\{\epsilon_1, \ldots, \epsilon_r\}$ of V. Choose distinct $v_1, \ldots, v_r \in V_{K,\infty}$ (which has $r + 1 = r_1 + r_2$ elements). Then

$$R_{\mathfrak{m}} := \left|\det(\log \|\epsilon_i\|_{v_j})_{1 \leq i,j \leq r}\right|$$

Sketch of proof. For details see [Lan94, VI.3, Lem. 1, Pf. of Thm. 3]. Consider the map

$$g : J \to \prod_{v \in V_{K,\infty}} \mathbb{R}, \quad x = (x_v)_v \mapsto \big(\log \frac{\|x_v\|_v}{c(x)^{N_v/N}}\big)_v,$$

where N_v is 1 if v is real and 2 if v is complex. Note that g restricted to $V \subset J$ is induced by the usual embedding $\mathcal{O}_K^{\times} \to \prod_{v \in V_{K,\infty}} \mathbb{R}, x = (x_v)_v \mapsto (\log \|x_v\|_v)_v$, which is used in the usual proof of Dirichlet's unit theorem. Thus as in that proof, we know that $g(V)$ is a full rank lattice in H, the hyperplane in $\prod_{v\in V_{K,\infty}}\mathbb{R}$ defined by the sum of the coordinates being zero. Moreover, note that $g(J)\subset H$. Let $F\subset H$ be a fundamental parallelepiped for the lattice $g(V)\subset H$. Take E to be $g^{-1}(F)$. □

We now start to count $j(\mathfrak{K},n)$. We first claim that the class $\mathfrak{K}^{-1}$ contains an integral ideal. Indeed, any fractional ideal in this class is of the form $\prod_{i=1}^k \mathfrak{p}_i^{n_i}$ where $\mathfrak{p}_i$ are prime ideals coprime to $\mathfrak{m}$ and $n_i\in\mathbb{Z}$. Let h be the order of $\mathrm{Cl}_{\mathfrak{m}}(K)$. Then $\prod_{i=1}^k \mathfrak{p}_i^{hu+n_i}$ also lies in $\mathfrak{K}^{-1}$ for all $u\in\mathbb{Z}$. For sufficiently large u this is an integral ideal.

Fix an integral ideal $\mathfrak{b}$ in the class $\mathfrak{K}^{-1}$. If $\mathfrak{a}$ is an integral ideal in the class $\mathfrak{K}$, then $\mathfrak{ab}$ is trivial in $\mathrm{Cl}_{\mathfrak{m}}(K)$, and so it is of the form $x\mathcal{O}_K$ with $x\in K^\times_{(\mathfrak{m})}$. Moreover, x is well defined up to multiplication by $G_{\mathfrak{m}}$, and we have $x\in\mathfrak{b}$ since $\mathfrak{ab}\subset\mathfrak{b}$. We thus have a bijection

$$\{\text{integral } \mathfrak{a}\in\mathfrak{K}\}\xrightarrow{\sim}\{x\in K^\times_{(\mathfrak{m})}/G_{\mathfrak{m}}\mid x\in\mathfrak{b}\}.$$

Now if $\mathfrak{a}$ corresponds to x, then

$$\mathrm{N}(\mathfrak{a})=\mathrm{N}(\mathfrak{b})^{-1}\mathrm{N}(x\mathcal{O}_K)=\mathrm{N}(\mathfrak{b})^{-1}\prod_{v\in V_{K,f}}\|x\|_v^{-1}=\mathrm{N}(\mathfrak{b})^{-1}c(x).$$

Here in writing $c(x)$ we view x as an element of B via the embedding $K\hookrightarrow B$. Hence we get

$$j(\mathfrak{K},n)=\#\{x\in K^\times_{(\mathfrak{m})}/G_{\mathfrak{m}}\mid x\in\mathfrak{b},c(x)\le n\mathrm{N}(\mathfrak{b})\}=w_{\mathfrak{m}}^{-1}\#\{x\in K^\times_{(\mathfrak{m})}/V\mid x\in\mathfrak{b},c(x)\le n\mathrm{N}(\mathfrak{b})\}.$$

By embedding $K^\times_{(\mathfrak{m})}$ into J, we get

$$w_{\mathfrak{m}}j(\mathfrak{K},n)=\#E(n\mathrm{N}(\mathfrak{b}))\cap\{x\in K^\times_{(\mathfrak{m})}\cap\mathfrak{b}\subset J\}.$$

Let $\mathfrak{m}_0$ be the integral ideal obtained by deleting the archimedean places inside $\mathfrak{m}$, and viewing the formal product of finite places as a product of the corresponding prime ideals. An element $x\in\mathfrak{b}$ lies in $K^\times_{(\mathfrak{m})}$ if and only if $x\in\mathfrak{m}_0-\{0\}$ and $x\in K_{v,>0}$ for archimedean $v|\mathfrak{m}$. Since $\mathfrak{b}$ is coprime to $\mathfrak{m}$, we have $\mathfrak{b}\cap\mathfrak{m}_0=\mathfrak{b}\mathfrak{m}_0$. Thus we have

$$K^\times_{(\mathfrak{m})}\cap\mathfrak{b}=J\cap(\mathfrak{b}\mathfrak{m}_0).$$

Since $E(n\mathrm{N}(\mathfrak{b}))$ is inside J, we have

$$w_{\mathfrak{m}}j(\mathfrak{K},n)=\#E(n\mathrm{N}(\mathfrak{b}))\cap(\mathfrak{b}\mathfrak{m}_0)=\#\big((n\mathrm{N}(\mathfrak{b}))^{1/N}D\big)\cap(\mathfrak{b}\mathfrak{m}_0),$$

where the intersection is inside B. Now $\mathfrak{b}\mathfrak{m}_0\subset\mathcal{O}_K$ are two lattices in B, and the latter has volume $2^{-r_2}\sqrt{d_K}$ where d_K is the discriminant of K. Hence

$$\mathrm{vol}(\mathfrak{b}\mathfrak{m}_0)=[\mathcal{O}_K:\mathfrak{b}\mathfrak{m}_0]2^{-r_2}\sqrt{d_K}=\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{m}_0)2^{-r_2}\sqrt{d_K}.$$

Applying Lemma 5.3.6, we obtain

$$j(\mathfrak{K},n)=\frac{\mathrm{vol}(D)}{w_{\mathfrak{m}}\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{m}_0)2^{-r_2}\sqrt{d_K}}\mathrm{N}(\mathfrak{b})n+O(n^{1-\frac{1}{N}})=\frac{\mathrm{vol}(D)}{w_{\mathfrak{m}}\mathrm{N}(\mathfrak{m}_0)2^{-r_2}\sqrt{d_K}}n+O(n^{1-\frac{1}{N}}).$$

Plugging in the formula for $\mathrm{vol}(D)$ in Lemma 5.3.7, we obtain

$$j(\mathfrak{K},n)=\rho_{\mathfrak{m}}n+O(n^{1-\frac{1}{N}}),$$

with

$$\rho_{\mathfrak{m}}=\frac{2^{r_1-s(\mathfrak{m})}(2\pi)^{r_2}R_{\mathfrak{m}}}{w_{\mathfrak{m}}\sqrt{d_K}\mathrm{N}(\mathfrak{m}_0)}.$$

Note that $\rho_{\mathfrak{m}}$ is a positive real number, and it is independent of $\mathfrak{K}$.

By Theorem 5.3.5, $\zeta_{K,\mathfrak{m}}(s,\mathfrak{K})$ is meromorphic on $\mathrm{Re}(s) > 1 - \frac{1}{N}$ and the only pole in this region is a simple pole at $s = 1$, with residue $\rho_{\mathfrak{m}}$. This completes the proof of Theorem 5.2.2.

Corollary 5.3.8 (The analytic class number formula)**.** *We have*

$$\mathrm{Res}_{s=1} L_{K,\mathfrak{m}}(s,1) = \#\,\mathrm{Cl}_{\mathfrak{m}}(K) \cdot \rho_{\mathfrak{m}}.$$

Proof. By definition, $L_{K,\mathfrak{m}}(s,1) = \sum_{\mathfrak{K}\in \mathrm{Cl}_{\mathfrak{m}}(K)} \zeta_{K,\mathfrak{m}}(s,\mathfrak{K})$. Each summand has residue $\rho_{\mathfrak{m}}$ at $s = 1$. □

When $\mathfrak{m} = 1$, this recovers the usual analytic class number formula

$$\mathrm{Res}_{s=1} \zeta_K(s) = h_K \cdot \rho_1 = h_K \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K\sqrt{d_K}}.$$

Note the following interesting consequence. By (5.1), we have

$$\#\,\mathrm{Cl}_{\mathfrak{m}}(K) = h_K \frac{\rho_1}{\rho_m} \prod_{\mathfrak{p}|\mathfrak{m}} (1-(\mathrm{N}\mathfrak{p})^{-1}) = h_K \frac{2^{s(\mathfrak{m})} R_1 w_{\mathfrak{m}} \mathrm{N}(\mathfrak{m}_0)}{R_{\mathfrak{m}} w_K} \prod_{\mathfrak{p}|\mathfrak{m}} (1-(\mathrm{N}\mathfrak{p})^{-1}). \tag{5.4}$$

Example 5.3.9. Let $K = \mathbb{Q}$. Then the regulator $R_{\mathfrak{m}}$ is always 1 since $r_1 + r_2 - 1 = 0$. The discriminant is also 1. Thus

$$\rho_1 = \frac{2}{w_{\mathbb{Q}}} = 1.$$

Since we know $\mathrm{Res}_{s=1} \zeta(s) = 1$, the analytic class number formula yields

$$1 = h_{\mathbb{Q}} \rho_1 = h_{\mathbb{Q}},$$

implying that $\mathbb{Z}$ is PID. For $\mathfrak{m} = \infty m$, we have $w_{\mathfrak{m}} = 1$ and $\mathrm{N}(\mathfrak{m}_0) = m$, so $\rho_{\mathfrak{m}} = \frac{1}{m}$. Hence (5.4) yields

$$\#\,\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}) = m \prod_{p|m} (1-p^{-1}).$$

Since $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$, the above recovers the usual formula for $\phi(m)$. Thus (5.4) can be viewed as a generalization of this formula.

5.4. **Artin L-functions.** Let K be a number field. Let V be a finite dimensional vector space over $\mathbb{C}$, and $\rho : G_K = \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V)$ a representation with open kernel. Equivalently, ρ factors through a representation $\mathrm{Gal}(L/K) \to \mathrm{GL}(V)$ for some finite Galois extension L/K. If we equip G_K with the usual profinite topology and equip $\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C})$ with the natural topology coming from $\mathbb{C}$, then this assumption on ρ is also equivalent to asking that it is continuous. Here the point is that there exists an open neighborhood U of 1 in $\mathrm{GL}(V)$ such that any subgroup of $\mathrm{GL}(V)$ contained in U is trivial (Exercise). Since the open subgroups of G_K form a neighborhood basis of 1, one of them must be contained in the kernel of ρ.

In the following, we refer to such a ρ as a *continuous finite dimensional complex representation* of G_K.

We define the Artin L-function

$$L(s,\rho) = L_K(s,\rho) = \prod_{\mathfrak{p}} \det(1-(\mathrm{N}\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}}) \mid V^{I_{\mathfrak{p}}})^{-1}.$$

Here, $\mathfrak{p}$ runs over all primes of K. For each $\mathfrak{p}$ we choose a decomposition group $D_{\mathfrak{p}}$ in G_K, let $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$ be the inertia subgroup, and let $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ be an element lifting the Frobenius element of $D_{\mathfrak{p}}/I_{\mathfrak{p}}$. The term $\det(1-(\mathrm{N}\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}}) \mid V^{I_{\mathfrak{p}}})$ is then independent of the choices. More concretely, ρ factors through some finite $\mathrm{Gal}(L/K)$, and it suffices to choose the decomposition groups and the Frobenius elements with respect to the finite Galois extension L/K.

Fact 5.4.1. *For every $\delta > 0$, the series defining $L(s,\rho)$ converges absolutely and uniformly on $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1+\delta\}$. In particular $L(s,\rho)$ is an analytic function on $\mathrm{Re}(s) > 1$.*

Sketch of proof. Let S be the finite set of primes $\mathfrak{p}$ of K such that $I_{\mathfrak{p}}$ acts non-trivially on V. It suffices to analyze the convergence of the series obtained by deleting the Euler factors at S and formally taking logarithm:

$$\log \prod_{\mathfrak{p} \notin S} \det(1-(\mathrm{N}\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}}) \mid V)^{-1} = \sum_{\mathfrak{p}\notin S}\sum_{m\geq 1} \frac{(\mathrm{N}\mathfrak{p})^{-ms}}{m} \mathrm{Tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})^m \mid V).$$

But $|\mathrm{Tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})^m \mid V)| \leq \dim V$ since every eigenvalue of $\rho(\mathrm{Frob}_{\mathfrak{p}})^m$ is a root of unity. Hence the above series is majorized by

$$\sum_{\mathfrak{p}\notin S}\sum_{m\geq 1} \frac{(\mathrm{N}\mathfrak{p})^{-ms}}{m} = \log \prod_{\mathfrak{p}\notin S}(1-(\mathrm{N}\mathfrak{p})^{-s})^{-1}.$$

The convergence of the above series is equivalent to that of $\zeta_K(s)$. □

Fact 5.4.2. *The following relations hold.*

(1) *If ρ_1, ρ_2 are two continuous finite dimensional complex representations of G_K, then*
$$L(s, \rho_1 \oplus \rho_2) = L(s,\rho_1)L(s,\rho_2).$$

(2) *Let E/K be a finite extension, so $G_E = \mathrm{Gal}(\overline{K}/E)$ is a finite index subgroup of G_K. Let ρ be a continuous finite dimensional complex representation of G_E. Then $\mathrm{Ind}_{G_E}^{G_K}\rho$ is a continuous finite dimensional complex representation of G_K. We have*
$$L_K(s, \mathrm{Ind}_{G_E}^{G_K}\rho) = L_E(s,\rho).$$

These follow easily from the definition.

Example 5.4.3. Suppose ρ is one-dimensional. Then ρ must factor through $\rho : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ where L/K is a finite *abelian* extension. (In fact, we may also assume that $\mathrm{Gal}(L/K)$ is cyclic, since any finite subgroup of $\mathbb{C}^\times$ is cyclic.) Let $\mathfrak{m} = \mathfrak{f}_{L/K}$. Define χ to be the composition of the Artin map $\mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ with $\rho : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$. Then up to the finitely many Euler factors indexed by $\mathfrak{p}|\mathfrak{m}$, $L(s,\rho)$ is nothing but $L_{K,\mathfrak{m}}(s,\chi)$, the Weber L-function.

Conjecture 5.4.4 (Artin's Conjecture)**.** *Let ρ be a non-trivial irreducible finite dimensional continuous complex representation of G_K. Then $L(s,\rho)$ has analytic continuation to an entire function on $\mathbb{C}$.*

This conjecture is one of the starting points of the Langlands program. The one-dimensional case reduces to the analytic continuation of Weber L-functions Example 5.4.3. This is known, although we will not prove it in our course. (Nevertheless, recall that we proved that the Weber L-function is analytic at $s = 1$ for non-trivial χ, while it has a pole at $s = 1$ for trivial χ. This explains why in Artin's Conjecture ρ needs to be non-trivial.) In fact, Weber L-functions belong to a more general class of L-functions, called L-functions attached to Hecke characters (or *grossencharacters*), and their analytic continuation is known by the work of Hecke, while a more conceptual proof was given in Tate's thesis.

The two dimensional case of Artin's conjecture is known in many cases, but not all. This is closely related to Wiles' proof of Fermat's Last Theorem. The general case of the conjecture is widely open.

As an application of class field theory, we can prove the following result (admitting the meromorphic continuation to $\mathbb{C}$ of Weber L-functions).

Theorem 5.4.5. *Any Artin L-function $L(s,\rho)$ has a meromorphic continuation to $\mathbb{C}$.*

We need to use the following fact from representation theory of finite groups.

Fact 5.4.6 (Brauer's theorem)**.** *Let G be a finite group, and ρ a (finite dimensional complex) representation of G. Then there exist subgroups $H_1, \dots, H_k$ of G, a one-dimensional representation ρ_i of H_i for each i, and integers $n_1, \dots, n_k \in \mathbb{Z}$, such that as virtual representations we have*

$$\rho = \sum_{i=1}^{k} n_i \operatorname{Ind}_{H_i}^{G} \rho_i.$$

(Here an equality of virtual representations means that after we move the negative terms to the other side and understand addition as direct sum, we have an isomorphism of representations. Equivalently, it can be understood as an equality between linear combinations of characters.)

Proof of Theorem 5.4.5. Assume that ρ factors through $\mathrm{Gal}(L/K)$ for a finite Galois extension L/K. Then there exist intermediate extensions E_i/K in L/K $(1 \leq i \leq k)$, one-dimensional representations ρ_i of $\mathrm{Gal}(L/E_i)$, and integers n_i such that $\rho = \sum_i n_i \operatorname{Ind}_{G_{E_i}}^{G_K} \rho_i$. Then

$$L(s,\rho) = \prod_{i=1}^{k} L(s, \operatorname{Ind}_{G_{E_i}}^{G_K} \rho_i)^{n_i} = \prod_{i=1}^{k} L_{E_i}(s,\rho_i)^{n_i}.$$

Each $L_{E_i}(s,\rho_i)$ is essentially a Weber L-function, so it has meromorphic continuation to $\mathbb{C}$. It follows that the same holds for $L(s,\rho)$. □

Remark 5.4.7. The integers n_i can be negative, so in the above proof one cannot control the poles of $L(s,\rho)$.

5.5. **Chebotarev density theorem.** The Chebotarev density theorem generalizes the famous theorem of Dirichlet on primes in an arithmetic progression. Recall that the theorem states that for any pair of coprime integers a, m, there exist infinitely many primes in $\{a + mk \mid k \in \mathbb{Z}\}$. In other words, each class in $(\mathbb{Z}/m\mathbb{Z})^\times$ contains infinitely many primes. We shall generalize this to number fields, and also see that the set of primes in each class in $(\mathbb{Z}/m\mathbb{Z})^\times$ is of *density* $1/|(\mathbb{Z}/m\mathbb{Z})^\times|$, in a suitable sense.

Definition 5.5.1. Let f and g be two complex functions defined on $(1, 1+\epsilon)$ for some $\epsilon > 0$. We shall write $f \sim g$ if there exists a complex analytic function h defined on an open disk centered at 1 (with no pole at 1) such that $f - g = h$ on $(1, 1+\epsilon')$ for some $0 < \epsilon' < \epsilon$. Roughly speaking, we ask that $f - g$ extends to a complex analytic function near $s = 1$.

Example 5.5.2. For $s > 1$, we have

$$\log \zeta(s) = \sum_{p \text{ primes}} \sum_{m=1}^{\infty} \frac{1}{m} p^{-ms}.$$

We claim that

$$\sum_p \sum_{m=2}^{\infty} \frac{1}{m} p^{-ms}$$

converges absolutely and uniformly for the complex variable s with $\mathrm{Re}(s) \geq \frac{1}{2} + \delta$, for any $\delta > 0$. For each p, we have

$$\sum_{m\geq 2} \left| \frac{1}{m} p^{-ms} \right| \;\leq\; \frac{1}{2} \sum_{m \geq 2} p^{-m(\frac{1}{2}+\delta)} \;=\; \frac{1}{2} \frac{p^{-2(\frac{1}{2}+\delta)}}{1-p^{-(\frac{1}{2}+\delta)}} \;\leq\; \frac{1}{2} \frac{p^{-2(\frac{1}{2}+\delta)}}{1-2^{-(\frac{1}{2}+\delta)}} \;\leq\; C \cdot p^{-1-2\delta},$$

where the constant C depends only on δ, not on p. Hence

$$\sum_p \sum_{m=2}^{\infty} \left| \frac{1}{m} p^{-ms} \right| \leq C \sum_p p^{-1-2\delta} \leq C \sum_{n=1}^{\infty} n^{-1-2\delta} < \infty.$$

This proves the claim. By the claim, we have

$$\log \zeta(s) \sim \sum_p p^{-s}.$$

More generally, let K be a number field. Then for $s > 1$ we have

$$\log \zeta_K(s) = \sum_{\mathfrak{p} \text{ prime ideals}} \sum_{m=1}^{\infty} \frac{1}{m} (\mathrm{N}\mathfrak{p})^{-ms}.$$

For $\mathrm{Re}(s) > 0$, we have

$$\sum_{\mathfrak{p}} \sum_{m=2}^{\infty} \left| \frac{1}{m} (\mathrm{N}\mathfrak{p})^{-ms} \right| \leq [K:\mathbb{Q}] \sum_p \sum_{m=2}^{\infty} \left| \frac{1}{m} p^{-ms} \right|$$

because there are at most $[K : \mathbb{Q}]$ distinct primes of K above a fixed prime p of $\mathbb{Q}$, and when $\mathfrak{p}|p$ we have $\mathrm{N}\mathfrak{p} \geq p$. Thus by the above claim we have

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} (\mathrm{N}\mathfrak{p})^{-s}.$$

Now recall that $\zeta_K(s)$ has a simple pole at $s = 1$. Hence we can write $\zeta_K(s) = \frac{1}{s-1} g(s)$ for some $g(s)$ analytic and non-zero at $s = 1$. Then for sufficiently small $\epsilon > 0$, $g(s)$ is real and positive on $(1, 1+\epsilon)$ since $\zeta_K(s)$ is so. Thus on such interval we have

$$\log \zeta_K(s) = \log \frac{1}{s-1} + \log g(s).$$

Since g is analytic and non-zero at $s = 1$, this clearly implies that $\log \zeta_K(s) \sim \log \frac{1}{s-1}$. We conclude that

$$\log \zeta_K(s) \sim \log \frac{1}{s-1} \sim \sum_{\mathfrak{p}} (\mathrm{N}\mathfrak{p})^{-s}.$$

Exercise 5.5.3. Let K be a number field. Prove that

$$\sum_{\mathfrak{p}} (\mathrm{N}\mathfrak{p})^{-s} \sim \sum_{\mathfrak{p}, f(\mathfrak{p}/\mathbb{Q})=1} (\mathrm{N}\mathfrak{p})^{-s}$$

Here the extra condition means that the residue extension of $\mathfrak{p}$ over $(p) = \mathfrak{p} \cap \mathbb{Q}$ is trivial, i.e., $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$.

Remark 5.5.4. Since $\log\frac{1}{s-1} \to +\infty$ as $\mathbb{R} \ni s \to 1^+$, for any $f(s) \sim \log\frac{1}{s-1}$ we have

$$\lim_{\mathbb{R}\ni s\to 1^+} \frac{f(s)}{\log\frac{1}{s-1}} = 1.$$

In the following, fix K to be a number field.

Definition 5.5.5. Let S be a subset of the set of primes of K. Define the *Dirichlet density* of S to be

$$\delta(S) = \lim_{\mathbb{R}\ni s\to 1^+} \frac{\sum_{\mathfrak{p}\in S}(\mathrm{N}\mathfrak{p})^{-s}}{\sum_{\text{all }\mathfrak{p}}(\mathrm{N}\mathfrak{p})^{-s}} = \lim_{\mathbb{R}\ni s\to 1^+} \frac{\sum_{\mathfrak{p}\in S}(\mathrm{N}\mathfrak{p})^{-s}}{\log\frac{1}{s-1}},$$

if the limit exists.

Proposition 5.5.6. *The following statements hold.*

(1) *If $\delta(S)$ exists, then $0 \le \delta(S) \le 1$, and $\delta(S^c) = 1 - \delta(S)$.*
(2) *If S is finite, then $\delta(S) = 0$.*
(3) *If $S_1 \cap S_2 = \emptyset$, and if two of $\delta(S_1), \delta(S_2), \delta(S_1 \cup S_2)$ exist, then the third also exists, and we have $\delta(S_1) + \delta(S_2) = \delta(S_1 \cup S_2)$.*
(4) *If $\delta(S_1)$ and $\delta(S_2)$ exist, and $S_1 \subset S_2$, then $\delta(S_1) \le \delta(S_2)$.*
(5) *If $\delta(S) = 0$, then for any subset $T \subset S$ we have $\delta(T) = 0$.*
(6) *If $\delta(S_1)$ and $\delta(S_2)$ exist, and $\delta(S_2) = 1$, then $\delta(S_1 \cap S_2) = \delta(S_1)$.*
(7) *$\delta(\{\mathfrak{p} \mid f(\mathfrak{p}/\mathbb{Q}) = 1\}) = 1$.*
(8) *If $\delta(S)$ exists, and T is a subset of S containing all $\mathfrak{p} \in S$ such that $f(\mathfrak{p}/\mathbb{Q}) = 1$, then $\delta(T) = \delta(S)$.*

Proof. The first five statements follow from elementary properties of limits. For (6), we have $\delta(S_1 - S_2) = 0$ by (1) and (5). Then apply (3) to $S_1 = (S_1 - S_2) \cup (S_1 \cap S_2)$. (7) follows from Exercise 5.5.3. To prove (8), first note that $\delta(\{\mathfrak{p} \in S \mid f(\mathfrak{p}/\mathbb{Q}) = 1\}) = \delta(S)$ by (6) and (7). Then apply the sandwich theorem for limit. □

As an immediate application of our considerations so far, we can compute the density of the set of split primes. Let L/K be a finite extension. Recall that a prime $\mathfrak{p}$ of K is said to *split in* L, if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ with distinct primes $\mathfrak{P}_i$ of L, and moreover $e(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}_i/\mathfrak{p}) = 1$ for each i. (In particular $g = [L : K]$.) We write $\mathrm{Spl}(L/K)$ for the set of primes of K which split in L.

Proposition 5.5.7. *Let L/K be a finite Galois extension. Then $\delta(\mathrm{Spl}(L/K)) = [L : K]^{-1}$.*

Proof. A prime $\mathfrak{P}$ of L is above a prime in $\mathrm{Spl}(L/K)$ if and only if $f(\mathfrak{P}/K) = e(\mathfrak{P}/K) = 1$. In this case, $\mathrm{N}\mathfrak{P} = \mathrm{N}(\mathfrak{P} \cap K)$. Moreover, for each $\mathfrak{p} \in \mathrm{Spl}(L/K)$, there are exactly $[L : K]$ primes of L above $\mathfrak{p}$. Hence we have

$$\sum_{\mathfrak{p}\in\mathrm{Spl}(L/K)} (\mathrm{N}\mathfrak{p})^{-s} = [L:K]^{-1} \sum_{\mathfrak{P}, f(\mathfrak{P}/k)=e(\mathfrak{P}/K)=1} (\mathrm{N}\mathfrak{P})^{-s} \sim [L:K]^{-1} \sum_{\mathfrak{P}, f(\mathfrak{P}/k)=1} (\mathrm{N}\mathfrak{P})^{-s}.$$

Here the last $\sim$ is because there are only finitely many $\mathfrak{P}$ with $e(\mathfrak{P}/K) > 1$. By Proposition 5.5.6(8), the set of primes $\mathfrak{P}$ of K such that $f(\mathfrak{P}/K) = 1$ has Dirichlet density 1. Hence

$$\delta(\mathrm{Spl}(L/K)) = [L:K]^{-1} \lim_{s\to 1^+} \frac{\sum_{\mathfrak{P}, f(\mathfrak{P}/k)=1}(\mathrm{N}\mathfrak{P})^{-s}}{\log\frac{1}{s-1}} = [L:K]^{-1}.$$

□

Exercise 5.5.8. (1) Let L_1, L_2 be two finite extensions of K inside $\overline{K}$. Show that $\mathrm{Spl}(L_1L_2/K) = \mathrm{Spl}(L_1/K) \cap \mathrm{Spl}(L_2/K)$.

(2) Let L/K be a finite extension, and M/K its Galois closure. Then $\mathrm{Spl}(L/K) = \mathrm{Spl}(M/K)$. (Hint: use part (1).) In particular, we have $\delta(\mathrm{Spl}(L/K)) = [L : K]^{-1}$ if and only if L/K is Galois.

Corollary 5.5.9. *Let L_1, L_2 be two finite Galois extensions of K inside $\overline{K}$. Then the following are equivalent.*

(1) $L_1 \subset L_2$
(2) $\mathrm{Spl}(L_2/K) \subset \mathrm{Spl}(L_1/K)$
(3) *There exists a set S of primes of K with $\delta(S) = 0$ such that* $\mathrm{Spl}(L_2/K) - S \subset \mathrm{Spl}(L_1/K)$.

In particular, a finite Galois extension L/K is uniquely determined by the set $\mathrm{Spl}(L/K)$.

Proof. The implications (1) ⇒ (2) ⇒ (3) are clear. We show (3) ⇒ (1). For every $\mathfrak{p} \in \mathrm{Spl}(L_2/K) - S$, we have $\mathfrak{p} \in \mathrm{Spl}(L_1/K) \cap \mathrm{Spl}(L_2/K) = \mathrm{Spl}(L_1L_2/K)$ by Exercise 5.5.8(1). Thus

$$[L_2 : K]^{-1} = \delta(\mathrm{Spl}(L_2/K) - S) \leq \delta(\mathrm{Spl}(L_1L_2/K)) = [L_1L_2 : K]^{-1}.$$

Hence $L_2 = L_1L_2$, i.e., $L_1 \subset L_2$. □

Up to now we have not used class field theory. The following result generalizes Dirichlet's theorem on primes in an arithmetic progression, and its proof uses Theorem 5.2.9, which we proved using class field theory.

Theorem 5.5.10 (Generalized Dirichlet's theorem on primes in an arithmetic progression)**.** *Let $\mathfrak{m}$ be a modulus for K, and fix $\mathfrak{K}_0 \in \mathrm{Cl}_{\mathfrak{m}}(K)$. Let S be the set of primes of K which are coprime to $\mathfrak{m}$ and whose class in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is $\mathfrak{K}_0$. Then $\delta(S) = |\,\mathrm{Cl}_{\mathfrak{m}}(K)|^{-1}$.*

Remark 5.5.11. For $K = \mathbb{Q}$ and $\mathfrak{m} = \infty m$ with $m \in \mathbb{Z}_{\geq 2}$, we have $\mathrm{Cl}_{\mathfrak{m}}(K) = (\mathbb{Z}/m\mathbb{Z})^\times$, and the class of a prime coprime to m in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is just the usual mod m congruence class of that prime. Hence in this case the theorem implies that each congruence class in $(\mathbb{Z}/m\mathbb{Z})^\times$ contains infinitely many primes, i.e. the classical theorem of Dirichlet.

Proof. The proof is essentially the same as the usual proof of Dirichlet's theorem, which uses the non-vanishing of the Dirichlet L-function $L(s, \chi)$ at $s = 1$ for a non-trivial Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. This non-vanishing is of course a special case of Theorem 5.2.9, which we will use.

Let $\chi \in \mathrm{Cl}_{\mathfrak{m}}(K)^\vee$. For $s > 1$, we have

$$\log L_{K,\mathfrak{m}}(s, \chi) = \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{m=1}^{\infty} \frac{\chi(\mathfrak{p})^m}{m} (\mathrm{N}\mathfrak{p})^{-ms}.$$

The series

$$\sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{m=2}^{\infty} \frac{\chi(\mathfrak{p})^m}{m} (\mathrm{N}\mathfrak{p})^{-ms}$$

is majorized by

$$\sum_{\mathfrak{p}} \sum_{m=2}^{\infty} \frac{1}{m} (\mathrm{N}\mathfrak{p})^{-ms},$$

which converges absolutely and uniformly on $\mathrm{Re}(s) \geq \frac{1}{2} + \delta$ as shown in Example 5.5.2. Thus we have

$$\log L_{K,\mathfrak{m}}(s, \chi) \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s}.$$

On the other hand, by Theorem 5.2.9, we have $\log L_{K,\mathfrak{m}}(s,\chi) \sim 0$ if χ is non-trivial. Hence

$$\sum_{\chi \in \mathrm{Cl}_{\mathfrak{m}}(K)^\vee} \chi(\mathfrak{K}_0)^{-1} \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s} \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} (\mathrm{N}\mathfrak{p})^{-s} + \sum_{\chi\neq 1} 0 \sim \log\frac{1}{s-1}.$$

But the left hand side is equal to

$$|\mathrm{Cl}_{\mathfrak{m}}(K)| \sum_{\mathfrak{p}\in S} (\mathrm{N}\mathfrak{p})^{-s}$$

since for each $\mathfrak{p} \nmid \mathfrak{m}$ we have $\sum_\chi \chi(\mathfrak{K}_0^{-1}\mathfrak{p}) = 0$ unless $\mathfrak{p} \in \mathfrak{K}_0$. □

Theorem 5.5.12 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension of degree N. Fix a conjugacy class C in* $\mathrm{Gal}(L/K)$*. Let S be the set of primes $\mathfrak{p}$ of K which are unramified in L and such that the Frobenius conjugacy class* $\mathrm{Frob}(L/\mathfrak{p}) = \{\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \mid \mathfrak{P}$ *primes of L above* $\mathfrak{p}\}$ *is equal to C. Then*

$$\delta(S) = \frac{|C|}{N}.$$

Remark 5.5.13. The special cases when $C = 1$ and when L is the ray class field $K_{\mathfrak{m}}$ recover Proposition 5.5.7 and Theorem 5.5.10 respectively. Indeed, in the first case, for a prime $\mathfrak{p}$ of K unramified in L (the unramified condition excludes only finitely many primes), it splits in L if and only if $\mathrm{Frob}(L/\mathfrak{p}) = \{1\}$. In the second case, the set of primes of K coprime to $\mathfrak{m}$ and having a fixed class in $\mathrm{Cl}_{\mathfrak{m}}(K)$ is precisely the set of primes unramified in $K_{\mathfrak{m}}$ and whose Frobenius element in $\mathrm{Gal}(K_{\mathfrak{m}}/K)$ is a fixed element, in view of the Artin isomorphism $\mathrm{Cl}_{\mathfrak{m}}(K) \cong \mathrm{Gal}(K_{\mathfrak{m}}/K)$. In this case $\mathrm{Gal}(K_{\mathfrak{m}}/K)$ is abelian, so every conjugacy class is a singleton.

Proof. We first treat the case where L/K is abelian. Find a modulus $\mathfrak{m}$ of K admissible for L/K. Then we have the surjective Artin map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$. Let $\tilde{C}$ be the inverse image of C in $\mathrm{Cl}_{\mathfrak{m}}(K)$. For a prime of K coprime to $\mathfrak{m}$, it lies in S if and only if its class in $\mathrm{Cl}_{\mathfrak{m}}(K)$ lies in $\tilde{C}$. Therefore

$$\delta(S) = \frac{|\tilde{C}|}{|\mathrm{Cl}_{\mathfrak{m}}(K)|}$$

by Theorem 5.5.10. But this is equal to $|C|/N = 1/N$ since C is a singleton and $\tilde{C}$ has the same cardinality as the kernel of $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$.

We now treat the general case. Fix an element $\sigma \in C$, and let f be the order of σ. Let $K' = L^{\langle\sigma\rangle}$. Then L/K' is a cyclic extension of degree f. Let

$$S_L = \{\mathfrak{P} \text{ primes of } L \mid \mathfrak{P} \text{ is unramified over } K, \mathrm{Frob}(\mathfrak{P}/K) = \sigma\},$$

$$S_{K'} = \{\mathfrak{p}' \text{ primes of } K' \mid \mathfrak{p}' \cap K \text{ is unramified in } L, \mathrm{Frob}(L/\mathfrak{p}') = \sigma, f(\mathfrak{p}'/K) = 1\}.$$

Here $\mathrm{Frob}(L/\mathfrak{p}')$ is a well-defined element of $\mathrm{Gal}(L/K') = \langle\sigma\rangle$ since the latter is abelian.

Claim 1. For every $\mathfrak{p} \in S$, there are exactly $\frac{N}{|C|f}$ elements of S_L above $\mathfrak{p}$. Conversely, every element of S_L is above an element of S.

Indeed, the second statement is obvious. We prove the first. For $\mathfrak{p} \in S$, by definition the set $A = \{\mathfrak{P} \in S_L \mid \mathfrak{P}|\mathfrak{p}\}$ is non-empty. For $\mathfrak{P} \in A$ and $g \in \mathrm{Gal}(L/K)$, we have $\mathrm{Frob}(g\mathfrak{P}/\mathfrak{p}) = g\,\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})g^{-1} = g\sigma g^{-1}$. Hence $g\mathfrak{P}$ lies in A if and only if g centralizes σ. Let G_σ denote the centralizer of σ in $\mathrm{Gal}(L/K)$. Since $\mathrm{Gal}(L/K)$ acts transitively on the set of primes of L above $\mathfrak{p}$, we know that G_σ acts transitively on A. Moreover, for $\mathfrak{P} \in A$, its stabilizer in G_σ is the decomposition group $G_{\mathfrak{P}} \subset G_\sigma$. But $G_{\mathfrak{P}} = \langle \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})\rangle = \langle \sigma \rangle$. Hence

$$|A| = \frac{|G_\sigma|}{|G_{\mathfrak{P}}|} = \frac{N/|C|}{f}$$

as desired.

Claim 2. Let $\mathfrak{P} \in S_L$ and $\mathfrak{p}' = \mathfrak{P} \cap K'$. Then $\mathfrak{p}' \in S_{K'}$, and $\mathfrak{P}$ is the unique prime of L above $\mathfrak{p}'$. Conversely, for every $\mathfrak{p}' \in S_{K'}$, there is a unique prime $\mathfrak{P}$ of L above $\mathfrak{p}'$, and moreover $\mathfrak{P} \in S_L$.

For the first statement, note that $\mathrm{Frob}(\mathfrak{P}/K) = \sigma$ acts trivially on K'. It follows that $f(\mathfrak{p}'/K) = 1$ and that

$$\mathrm{Frob}(L/\mathfrak{p}') = \mathrm{Frob}(\mathfrak{P}/K') = \mathrm{Frob}(\mathfrak{P}/K)^{f(\mathfrak{p}'/K)} = \sigma.$$

Hence $\mathfrak{p}' \in S_{K'}$. Moreover, $\mathfrak{p}'$ is unramified in L, and $f(L/\mathfrak{p}')$ is equal to the order of $\mathrm{Frob}(L/\mathfrak{p}') = \sigma$, which is $f = [L : K']$. Hence there is a unique prime of L above $\mathfrak{p}'$. The first statement is proved. The second statement is proved similarly.

By the two claims, we have

$$\sum_{\mathfrak{p}\in S} (\mathrm{N}\mathfrak{p})^{-s} = \frac{|C|f}{N} \sum_{\mathfrak{P}\in S_L} \mathrm{N}(\mathfrak{P}\cap K)^{-s} = \frac{|C|f}{N} \sum_{\mathfrak{p}'\in S_{K'}} \mathrm{N}(\mathfrak{p}'\cap K)^{-s} = \frac{|C|f}{N} \sum_{\mathfrak{p}'\in S_{K'}} (\mathrm{N}\mathfrak{p}')^{-s},$$

where the last equality is because $f(\mathfrak{p}'/K) = 1$. Thus

$$\delta(S) = \frac{|C|f}{N}\delta(S_{K'})$$

(provided that $\delta(S_{K'})$ exists). Applying the abelian case of the theorem to L/K' and by Proposition 5.5.6 (8), we have $\delta(S_{K'}) = [L : K']^{-1} = f^{-1}$. □

As a simple application, we have the following:

Proposition 5.5.14. *Let f be a non-constant irreducible polynomial over K. Assume that f has a root in K_v for almost all places v. Then f is of degree 1, i.e., it has a root in K.*

Proof. Let $L \subset \overline{K}$ be the splitting field of f. Let S be the set of primes $\mathfrak{p}$ of K unramified in L and such that f has a root in $K_{\mathfrak{p}}$. Then there are only finitely many primes not in S, so $\delta(S) = 1$. Fix a root α of f in L. Let $\mathfrak{p} \in S$, and choose a K-embedding $\iota : L \hookrightarrow \overline{K_{\mathfrak{p}}}$. Let β be a root of f in $K_{\mathfrak{p}}$. Then β must lie in the image of ι, and by the irreducibility of f, there exists $g \in \mathrm{Gal}(L/K)$ such that $g(\alpha) = \beta$. Thus up to modifying ι we may assume that $\iota(\alpha) = \beta \in K_{\mathfrak{p}}$. On the other hand ι determines a prime $\mathfrak{P}$ of L above $\mathfrak{p}$, and the last condition on ι implies that $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})(\alpha) = \alpha$. Thus we have shown that for every $\mathfrak{p} \in S$, the conjugacy class $\mathrm{Frob}(L/\mathfrak{p})$ in $\mathrm{Gal}(L/K)$ has non-empty intersection with $H = \mathrm{Gal}(L/K(\alpha))$. If H is not equal to $\mathrm{Gal}(L/K)$, then by elementary group theory there is a conjugacy class C in $\mathrm{Gal}(L/K)$ disjoint from H. By Theorem 5.5.12, $\delta(S)$ is at most $1 - |C|/[L : K] < 1$, a contradiction. Hence $K(\alpha) = K$. □

5.6. **The Grunwald–Wang theorem.** Reference: [AT68, §X.1]

Let K be a number field and m a positive integer. Suppose an element c of K is an m-th power in K_v for almost all places v, does it follow that c is an m-th power in K? If the answer is yes for all c, then we say that K satisfies the local-global principle for m-th powers.

In 1928, Grunwald published a false theorem stating that K always satisfies the local-global principle for m-th powers, for all K and m. Wang found the following counterexample:

Exercise 5.6.1. Show that 16 is an 8-th power in $\mathbb{Q}_p$ for all odd primes p, but not an 8-th power in $\mathbb{Q}_2$ or $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{7})$. Then 16 is an 8-th power in K_v for all places v of K, but not an 8-th power in K.

The mistake in Grunwald's work arises from careless use of the notation $K(\sqrt[n]{c})$. When K does not contain a primitive n-th root of unity, adjoining different roots of $X^n - c$ to K can give rise to non-isomorphic extensions of K. For instance, related to the counter-example of Wang, adjoining different 8-th roots of 16 to $\mathbb{Q}$ can give rise to $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, and they are obviously non-isomorphic.

Lemma 5.6.2. *Assume that K contains a primitive m-th root of unity. Then K satisfies the local-global principle for m-th powers.*

Proof. Assume $c \in K^\times$ is an m-th power in K_v for almost all v. Let L/K be the splitting field of $X^m - c$. If $X^m - c$ has a root in $K_\mathfrak{p}$, then it splits in $K_\mathfrak{p}$, and in this case for every prime $\mathfrak{P}$ of L above $\mathfrak{p}$ we have $L_\mathfrak{P} = K_\mathfrak{p}$ since $L_\mathfrak{P}$ is the compositum of its subfields L and $K_\mathfrak{p}$. Thus $\delta(\mathrm{Spl}(L/K)) = 1$, and so $L = K$ by Proposition 5.5.7. □

Theorem 5.6.3 (Grunwald–Wang, rough version)**.** *Let $m = 2^t m'$ with m' odd. Assume that $K(\zeta_{2^t})/K$ is cyclic. Then K satisfies the local-global principle for m-th powers.*

Proof. **Step 1.** Reduce to the case where m is a prime power. For this it suffices to note that for two coprime integers m_1, m_2, we have $(K^\times)^{m_1} \cap (K^\times)^{m_2} = (K^\times)^{m_1 m_2}$.

Step 2. Assuming m is a prime power, and assuming that $K(\zeta_m)/K$ is cyclic of prime power degree, we show that K satisfies the local-global principle for m-th powers. For this, let $c \in K^\times$ be such that $c \in (K_v^\times)^m$ for almost all v. Then by Lemma 5.6.2 applied to the base field $K(\zeta_m)$, we have $c \in (K(\zeta_m)^\times)^m$. Let $f(X) = X^m - c \in K[X]$. Then $f(X)$ splits over $K(\zeta_m)$. Let $f(X) = f_1(X) \cdots f_k(X)$ with $f_i(X) \in K[X]$ irreducible. Let L_i/K be the splitting field of f_i inside $K(\zeta_m)$. By our assumption on $K(\zeta_m)/K$, all intermediate extensions in $K(\zeta_M)/K$ are totally ordered. Hence there exists i_0 such that $L_{i_0} \subset L_i$ for all i. Now if v is a place of K such that $c \in (K_v^\times)^m$, then some f_i has a root in K_v. Since L_i is actually generated by a single root of the irreducible f_i (as all roots are related by multiplying by an m-th root of unity), there exists a K-embedding $L_i \to K_v$. Hence there exists a K-embedding $L_{i_0} \to K_v$, which means that v splits in L_{i_0}. Thus for almost all places v of K, v splits in L_{i_0}. By Proposition 5.5.7 this implies that $L_{i_0} = K$, i.e., $c \in (K^\times)^m$.

Step 3. We prove the theorem assuming that $m = p^s$ for a prime p. If $p = 2$, then the assumption of the theorem states that $K(\zeta_m)/K$ is cyclic. It is also of prime power degree since the degree divides $|(\mathbb{Z}/m\mathbb{Z})^\times|$ which is a power of 2. Hence, by Step 2, K satisfies local-global principle for m-th powers. It remains to treat the case where p is odd. In view of the canonical injections $\mathrm{Gal}(K(\zeta_m)/K) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ and $\mathrm{Gal}(K(\zeta_p)/K) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$, we have an injection of $\mathrm{Gal}(K(\zeta_m)/K(\zeta_p))$ into the kernel of the natural map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order a power of p. Thus we can apply Step 2 to obtain that the field $K(\zeta_p)$ satisfies local-global principle for m-th powers. Now let $c \in K^\times$ be such that $c \in (K_v^\times)^m$ for almost all v. Then $c \in (K(\zeta_p)^\times)^m$. Write $c = y^m$ for $y \in K(\zeta_p)^\times$. Let $d = [K(\zeta_p) : K]$. Then $c^d = \mathrm{N}_{K(\zeta_p)/K}(c) = (\mathrm{N}_{K(\zeta_p)/K}(y))^m \in (K^\times)^m$. Since $d | p-1$, d is coprime to m. Hence there exist $a, b \in \mathbb{Z}$ such that $ad + bm = 1$. Then $c = (c^d)^a (c^b)^m$ lies in $(K^\times)^m$. □

To get a more precise version of the above theorem, we need to have a better understanding of when $K(\zeta_{2^r})/K$ can be non-cyclic. Recall that we have a canonical injection $\mathrm{Gal}(K(\zeta_{2^r})/K) \hookrightarrow (\mathbb{Z}/2^r\mathbb{Z})^\times$. The problem is that the right hand side is not a cyclic group unless $r \leq 2$ (e.g. $(\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Nevertheless, we have the canonical subgroup $\{\pm 1\} \subset (\mathbb{Z}/2^r\mathbb{Z})^\times$, and $(\mathbb{Z}/2^r\mathbb{Z})^\times/\{\pm 1\}$ is always cyclic. Correspondingly, inside $K(\zeta_{2^t})$ we have the subfield $K(\zeta_{2^t} + \zeta_{2^t}^{-1})$ of index at most 2, and the latter is cyclic over K. There is a maximal integer s such that $K(\zeta_{2^s} + \zeta_{2^s}^{-1}) = K$. Then $K(\zeta_{2^{s+1}} + \zeta_{2^{s+1}}^{-1})$ is a quadratic extension of K, and $K(\zeta_{2^{s+1}})$ is either a cyclic extension of K of degree 2 or 4, or a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension of K. The non-cyclicity of (any) $K(\zeta_{2^r})/K$ is essentially caused by the latter possibility.

To make these ideas more precise, we first introduce some notations. Inside $\overline{K}$ we fix a primitive 2^r-th root of unity ξ_r for each $r \in \mathbb{Z}_{\geq 1}$ in a compatible way, i.e., $\xi_{r+1}^2 = \xi_r$. Let

$$\eta_r = \xi_r + \xi_r^{-1}.$$

For instance, we may fix an embedding $\overline{K} \to \mathbb{C}$ and choose $\xi_r = e^{2\pi i/2^r}$. Then $\eta_r = 2\cos(2\pi/2^r)$. Note that ξ_2 is a primitive 4-th root of unity, namely "$\xi_2 = i = \sqrt{-1}$", and it is of degree at most 2 over K (depending whether -1 is a square in K).

Let $K_r = K(\xi_r)$. Thus

$$K \subset K_1 \subset K_2 \subset K_3 \subset \cdots.$$

Since $\eta_{r+1}^2 = \eta_r + 1$, we have

$$K(\eta_1) \subset K(\eta_2) \subset K(\eta_3) \subset \cdots.$$

Of course each $K(\eta_r)$ is contained in K_r. Since K_r/K is an abelian extension, so is $K(\eta_r)/K$. We have $\eta_1 = -2, \eta_2 = 0, \eta_r \neq 0, \ \forall r \geq 3$.

Note that $\xi_r\eta_r = 1+\xi_r^2 = 1+\xi_{r-1}$, so $\xi_r = \eta_r^{-1}(1+\xi_{r-1})$ for $r \geq 3$. Thus $K_r \subset K(\eta_r, \xi_{r-1})$ for $r \geq 3$, and then by induction

$$K_r = K(\xi_2, \eta_r) = K_2(\eta_r).$$

For instance,

$$\mathbb{Q}(e^{2\pi i/2^r}) = \mathbb{Q}(i, \cos(2\pi i/2^r)).$$

Lemma 5.6.4. *Each $K(\eta_r)/K$ is a cyclic extension.*

Proof. Consider the canonical injection $\alpha : \mathrm{Gal}(K_r/K) \hookrightarrow (\mathbb{Z}/2^r\mathbb{Z})^\times$. If -1 is not in the image of α, then α induces an injection of $\mathrm{Gal}(K_r/K)$ into $(\mathbb{Z}/2^r\mathbb{Z})^\times/\{\pm 1\}$, which is a cyclic group. Then K_r/K is cyclic, and in particular $K(\eta_r)/K$ is cyclic.

If -1 is in the image of α, say $-1 = \alpha(\tau)$. Then $\tau(\xi_r) = \xi_r^{-1}$ by the definition of α. Hence $\eta_r \in K_r^{\langle\tau\rangle}$. But $[K_r : K(\eta_r)] \leq 2$ since $K_r = K_2(\eta_r)$. Hence $K(\eta_r) = K_r^{\langle\tau\rangle}$, and $\mathrm{Gal}(K(\eta_r)/K)$ injects into $(\mathbb{Z}/2^r\mathbb{Z})^\times/\{\pm 1\}$, which is a cyclic group. □

Definition 5.6.5. Let $s \in \mathbb{Z}_{\geq 1}$ be the largest such that $\eta_s \in K$.

Note that such s exists, since otherwise we have $K_2 = K_2(\eta_r) = K_r$ for all r, which is impossible.

Lemma 5.6.6. *The following conditions are equivalent.*

(1) $\mathrm{Gal}(K_{s+1}/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(2) *There exists r such that K_r/K is not cyclic.*
(3) $\xi_2 \notin K(\eta_{s+1})$.
(4) *All of $-1, \pm(\eta_s + 2)$ are non-squares in K.*

Proof. (1) ⇒ (2) is trivial. For (2) ⇒ (3), assume that $\xi_2 \in K(\eta_{s+1})$. Then for every $r \geq s+1$, we have $K_r = K_2(\eta_r) = K(\eta_r)$. By Lemma 5.6.4 this is cyclic over K. It follows that K_r/K is cyclic for every $r \geq 1$. For the equivalence of (1), (3), and (4), note that

$K_{s+1} = K(\xi_2, \eta_{s+1})$ where $\xi_2^2 = -1$ and $\eta_{s+1}^2 = \eta_s + 2$ are in K. Thus K_{s+1} is of the form $K(\sqrt{a}, \sqrt{b})$ with $a, b \in K$. Such an extension is a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension if and only if a, b, ab are all non-squares in K. □

We now come back to the local-global principle for m-th powers. Let S be a finite set of places of K. Denote

$$P(m, S) = \{c \in K^\times \mid \forall v \in V_K - S, c \in (K_v^\times)^m\}.$$

Corollary 5.6.7. *If $P(m, S) \neq (K^\times)^m$, then the following conditions hold:*

(1) *All of $-1, \pm(\eta_s + 2)$ are non-squares in K.*
(2) *We have $m = 2^t m'$ with m' odd and $t > s$.*

Proof. By Theorem 5.6.3, K_t/K must be non-cyclic. By Lemma 5.6.6, (1) holds. If $t \leq s$, then $K_t = K_2(\eta_t) = K_2$ is quadratic over K, a contradiction. Hence $t > s$. □

Proposition 5.6.8. *Assume (1) (2) in Corollary 5.6.7. Then*

$$P(m, S) \subset (K^\times)^m \sqcup x_m (K^\times)^m,$$

where

$$x_m = (1 + \xi_s)^m = \eta_{s+1}^m \in K^\times - (K^\times)^m.$$

Proof. Firstly, since $1+\xi_s = \xi_{s+1}\eta_{s+1}$, and since $m = 2^t m'$ with $t \geq s+1$, we have $(1+\xi_s)^m = \xi_{s+1}^m \eta_{s+1}^m = \eta_{s+1}^m$. Now if x_m were in $(K^\times)^m$, then using $x_m = \eta_{s+1}^m = (\eta_s + 2)^{2^{t-1}m'}$, we know that $(\eta_s + 2)^{2^{t-1}} \in (K^\times)^{2^t}$. Thus there exists a 2^{t-1}-th root of unity $\xi \in K$ such that $\xi(\eta_s + 2) \in (K^\times)^2$. By condition (1), -1 is not a square in K, so we must have $\xi \in \{\pm 1\}$. Thus one of $\pm(\eta_s + 2)$ is a square in K, a contradiction with (1).

We now prove the containment. By (1), K_2/K is quadratic. We write $\mathrm{Gal}(K_2/K) = \{1, \sigma\}$. We have $K_2 = K_2(\eta_s) = K_s = K(\xi_s)$. We check that $\sigma(\xi_s) = \xi_s^{-1}$: For this it suffices to note that $\xi_s \xi_s^{-1}$ and $\xi_s + \xi_s^{-1}$ are both in K.

Let $x \in P(m, S)$. Since -1 is a square in K_2, by Corollary 5.6.7 applied to the field K_2 we have $x \in (K_2^\times)^m$. In particular there exists $y \in K_2$ such that $x = y^{2^t}$. Then $(y\sigma(y)^{-1})^{2^t} = (x\sigma(x)^{-1})^{2^t} = 1$, so $y\sigma(y)^{-1}$ is a 2^t-th root of unity in K_2. By condition (1), we have $\eta_{s+1} \notin K_2$ in view of Lemma 5.6.6. In particular $\xi_{s+1} \notin K_2$. Since $t > s$ (condition (2)), $y\sigma(y)^{-1}$ is a 2^s-th root of unity in K_2, i.e.,

$$y\sigma(y)^{-1} = \xi_s^\mu$$

for some $\mu \in \mathbb{Z}$. We shall see that μ being even or odd correspond to $x \in (K^\times)^m$ or $x \in x_m(K^\times)^m$ respectively.

Let $y_1 = y\xi_s^\lambda \in K_2$, where $\lambda \in \mathbb{Z}$ is to be determined. Then $y_1^{2^t} = x$ as well, i.e., y_1 is another candidate for y. We have

$$y_1\sigma(y_1)^{-1} = y\sigma(y)^{-1}(\xi_s\sigma(\xi_s)^{-1})^\lambda = \xi_s^{\mu+2\lambda}.$$

If μ is even, then we can choose $\lambda = -\mu/2$. In other words we can choose $y \in K_2$ such that $y^{2^t} = x$ and $y = \sigma(y)$, i.e., $y \in K$. In this case, $x \in (K^\times)^{2^t}$. By Theorem 5.6.3, we also have $x \in (K^\times)^{m'}$. Hence $x \in (K^\times)^m$. (Find integers a, b such that $a2^t + bm' = 1$. Then $x = (x^a)^{2^t}(x^b)^{m'}$. Then use $x^a \in (K^\times)^{m'}$ and $x^b \in (K^\times)^{2^t}$.)

If μ is odd, then we can choose λ such that $\mu + 2\lambda = m'$. In other words we can choose $y \in K_2$ such that $y^{2^t} = x$ and $y\sigma(y)^{-1} = \xi_s^{m'}$. Let $z = y(1+\xi_s)^{-m'} \in K_2$. Then $z\sigma(z)^{-1} = 1$, i.e., $z \in K$. We have $z^{2^t} = xx_m^{-1}$. Thus $xx_m^{-1} \in (K^\times)^{2^t}$. Since $x_m = (\eta_s + 2)^{m/2}$ with $\eta_s \in K$, we have $x_m \in (K^\times)^{m'}$. By Theorem 5.6.3, we have $x \in (K^\times)^{m'}$. Hence $xx_m^{-1} \in (K^\times)^{m'}$. As before, it follows that $xx_m^{-1} \in (K^\times)^m$. □

Definition 5.6.9. Let S_0 be the set of places v of K such that -1 and $\pm(\eta_s + 2)$ are non-squares in K_v.

Remark 5.6.10. The condition in the definition of S_0 is equivalent to that $K_v(\xi_2, \eta_{s+1})$ is a $\mathbb{Z}/2 \times \mathbb{Z}/2$-extension of K_v. If v is archimedean, this is impossible. If v divides an odd prime in $\mathbb{Q}$, this is again impossible because $K_v(\xi_2, \eta_{s+1}) = K_v(\xi_{s+1})$ is unramified over K_v and hence cyclic over K_v. Hence all places in S_0 divide 2.

Lemma 5.6.11. *Assume (1) (2) in Corollary 5.6.7. Then S_0 consists precisely of those places v such that $x_m \notin (K_v^\times)^m$.*

Proof. If $v \in S_0$, then the same argument as in the proof of Proposition 5.6.8 showing that $x_m \notin (K^\times)^m$ shows that $x_m \notin (K_v^\times)^m$. Now let $v \in V_K - S_0$. We need to prove that $x_m \in (K_v^\times)^m$. If -1 is a square in K_v, then $\xi_2 \in K_v$, and so $\xi_s \in K_v(\xi_2, \eta_s) \subset K_v$. Then $x_m = (1 + \xi_s)^m \in (K_v^\times)^m$, as desired. If one of $\pm(\eta_s + 2)$ is a square in K_v, then either $\sqrt{\eta_s + 2} = \pm\eta_{s+1} \in K_v$ or $\sqrt{-(\eta_s + 2)} = \pm\xi_2\eta_{s+1} \in K_v$. In either case we have $x_m = \eta_{s+1}^m = (\xi_2\eta_{s+1})^m$ lies in $(K_v^\times)^m$. (The second equality is because $4|m$.) □

Theorem 5.6.12 (Grunwald–Wang, refined version)**.** *We have $P(m, S) = (K^\times)^m$, except in the so-called* special case*, where all the following three conditions are satisfied:*

(1) *All of $-1, \pm(\eta_s + 2)$ are non-squares in K.*
(2) *We have $m = 2^t m'$ with m' odd and $t > s$.*
(3) *$S \supset S_0$.*

Moreover, in the special case, we have $P(m, S) = (K^\times)^m \sqcup x_m(K^\times)^m$.

Proof. By Lemma 5.6.11, condition (3) is equivalent to the condition that $x_m \in P(m, S)$. In view of this, the theorem follows from Corollary 5.6.7 and Proposition 5.6.8. □

5.7. Approximating local abelian extensions by global ones.

Reference: [AT68, §X.2]

Theorem 5.7.1. *Let K be a number field and S a finite subset of V_K. Suppose that for each $v \in S$ we are given a finite abelian extension K^v/K_v. Then there exists a finite abelian extension L/K such that for each $v \in S$ and each place w of L above v, we have $L_w \cong K^v$ as extensions of K_v.*

Remark 5.7.2. If L/K is a finite Galois extension of global fields and w_1, w_2 are places of L over a place v of K, then $L_{w_1} \cong L_{w_2}$ as extensions of K_v, by the transitivity of the $\mathrm{Gal}(L/K)$-action on the set of places of L above v. Indeed, if $\tau \in \mathrm{Gal}(L/K)$ takes w_1 to w_2, then the isomorphism $\tau : L \xrightarrow{\sim} L$ induces an isomorphism $\tau : L_{w_1} \xrightarrow{\sim} L_{w_2}$ after completion, and the latter isomorphism restricts to the identity map on K_v.

Remark 5.7.3. If we are given one non-archimedean place v of K and a finite extension K^v/K_v, then it is easy to find a finite extension L/K such that there is exactly one place w of L over K and moreover $L_w \cong K^v$ as extensions of K_v. Indeed, write $K^v = K_v(\alpha)$ and let $f(X) \in K_v[X]$ be the minimal polynomial of α over K_v. By Krasner's lemma and by the density of K in K_v, there exists an irreducible $g(X) \in K[X]$ such that $K_v[X]/(g(X))$ is isomorphic to K^v as extensions of K_v. Take L to be $K[X]/(g(X))$.

By the classification of finite abelian extensions of global and local fields (Corollaries 4.2.8, 4.5.4) and by the local-global compatibility (Theorem 4.5.9), in order to prove Theorem 5.7.1 it suffices to show that there is an open (and finite index, which is automatic) subgroup N of C_K such that

$$\prod_{v\in S} \mathrm{N}_{K^v/K_v}(K^{v,\times}) = (\prod_{v\in S} K_v^\times) \cap N.$$

Here the intersection is inside C_K, and we embed $\prod_{v\in S} K_v^\times$ into C_K by

$$(x_v)_{v\in S} \mapsto ((x_v)_{v\in S}, (1)_{v\notin S}) \in \mathbb{A}_K^\times/K^\times.$$

The left hand is an open subgroup of finite index of $\prod_{v\in S} K_v^\times$ (equipped with the product topology). Hence Theorem 5.7.1 follows from the following theorem.

Theorem 5.7.4. *Every open finite index subgroup of $\prod_{v\in S} K_v^\times$ is of the form $(\prod_{v\in S} K_v^\times)\cap N$ for some open subgroup N of C_K.*

We will see that the proof crucially depends on the Grunwald–Wang theorem.

One subtlety is that when S has more than one element, the product topology on $\prod_{v\in S} K_v^\times$ is finer than the subspace topology inherited from C_K. We write $\tilde{P}$ for $\prod_{v\in S} K_v^\times$ with the product topology, and write P for $\prod_{v\in S} K_v^\times$ with the subspace topology inherited from C_K. Thus the identity map is a continuous map

$$\tilde{P} \to P \subset C_K.$$

Theorem 5.7.5. *If $\tilde{P}_0$ is an open finite index subgroup of $\tilde{P}$, then its image P_0 is P is also open.*

For the proof we need two lemmas.

Lemma 5.7.6. *If the triple (K, m, S) does not belong to the special case in Theorem 5.6.12, then $P \cap C_K^m = P^m$. If (K, m, S) belongs to the special case, then*

$$P \cap C_K^m = P^m \cup c_m P^m,$$

where $c_m = (c_{m,v})_{v\in S} \in P$ is defined by $c_{m,v} = 1$ for $v \notin S_0$ and $c_{m,v} = x_m$ for $v \in S_0$.

Proof. Let $a = (a_v)_{v\in S} \in P$ such that it lies in C_K^m. Then there exists $\alpha \in K^\times$ and $b \in \mathbb{A}_K^\times$ such that $a = \alpha b^m$. In particular $\alpha \in P(m, S)$. If we are not in the special case of Theorem 5.6.12, then it follows that $\alpha \in (K^\times)^m$. Then clearly $a \in P^m$.

Suppose we are in the special case and that $\alpha \notin (K^\times)^m$. Then $\alpha \in x_m(K^\times)^m$. Hence

$$a = x_m e^m$$

for some $e \in \mathbb{A}_K^\times$. Thus the component of $ac_m^{-1} \in P$ at $v \in S$ is e_v^m for $v \in S_0$ and $x_m e_v^m$ for $v \in S - S_0$. By Lemma 5.6.11, we have $ac_m^{-1} \in P^m$. □

Lemma 5.7.7. *For every $m \in \mathbb{Z}_{\geq 1}$, P^m is closed in P. Moreover, $\tilde{P}/\tilde{P}^m$ and P/P^m are compact.*

Proof. Using $C_K \cong \mathbb{R}_{>0} \times C_K^1$ and the compactness of C_K^1, it is easy to see that C_K^m is closed in C_K. If (K, m, S) does not belong to the special case in Theorem 5.6.12, then by Lemma 5.7.6 we have $P^m = P \cap C_K^m$ and this is closed in P. Suppose we are in the special case. Note that $x_{2m} = \eta_{s+1}^{2m} = (\eta_s + 2)^m$ and $\eta_s + 2 \in K$. Hence $x_{2m} \in (K^\times)^m$, and $c_{2m} \in P^m$. By Lemma 5.7.6 applied to $(K, S, 2m)$ (which still belongs to the special case), we have

$$P \cap C_K^{2m} = P^{2m} \cup c_{2m} P^{2m} \subset P^m.$$

Thus we have

$$P^{2m} \subset P \cap C_K^{2m} \subset P^m \subset P.$$

Clearly $[P : P^{2m}] < \infty$. Hence P^m is a finite union of the cosets of $P \cap C_K^{2m}$ in P. It follows that P^m is closed in P.

The compactness of $\tilde{P}/\tilde{P}^m \cong \prod_{v\in S} K_v^\times / K_v^{\times,m}$ is directly checked. The compactness of P/P^m follows since there is a bijective continuous map $\tilde{P}/\tilde{P}^m \to P/P^m$. □

Proof of Theorem 5.7.5. Since $\tilde{P}_0$ is of finite index in $\tilde{P}$, there exists $m \in \mathbb{Z}_{\geq 1}$ such that $\tilde{P}^m \subset \tilde{P}_0$. Then $\tilde{P}_0/\tilde{P}^m$ is open, and hence closed, in $\tilde{P}/\tilde{P}^m$. Since $\tilde{P}/\tilde{P}^m$ is compact, so is $\tilde{P}_0/\tilde{P}^m$. It follows that P_0/P^m is compact. But by Lemma 5.7.7, P/P^m is Hausdorff. Hence P_0/P^m is closed in P/P^m, and so P_0 is closed in P. Since P_0 is of finite index in P, it follows that it is open in P. □

By Theorem 5.7.5, in order to prove Theorem 5.7.4 it suffices to prove the following theorem.

Theorem 5.7.8. *Every open finite index subgroup of P is of the form $P \cap N$ for some open subgroup N of C_K.*

To prove the above theorem we prove two more lemmas.

Lemma 5.7.9. *Let P_0 be an open finite index subgroup of P. For every $m \in \mathbb{Z}_{\geq 1}$, $P_0 C_K^m$ is closed in C_K^m.*

Proof. We will use the following general fact ([AT68, §X.2, Lem. 1]): In a topological group, if A is a compact subset and B is a closed subset, then $A \cdot B$ is closed.

Let $\tilde{P}_0$ be the inverse image of P_0 in $\tilde{P}$. Then $\tilde{P}_0$ is open. Let $\tilde{W}$ be a compact neighborhood of 1 in $\tilde{P}$ contained in $\tilde{P}_0$ (since each $K_v^\times$ contains arbitrarily small compact neighborhoods of 1). By finite index, there exists $N \in \mathbb{Z}_{\geq 1}$ divisible by m and such that $\tilde{P}^N \subset \tilde{P}_0$. By the compactness of $\tilde{P}_0/\tilde{P}^N$ (which is closed in the compact $\tilde{P}/\tilde{P}^N$), there exists $\tilde{p}_1, \cdots, \tilde{p}_k$ such that $\tilde{P}_0 = \bigcup_{i=1}^k \tilde{p}_i \tilde{P}^N \tilde{W}$. Let W (resp. p_i) be the image of $\tilde{W}$ (resp. p_i) in P. Then

$$P_0 C_K^m = \bigcup_{i=1}^k p_i P^N W C_K^m.$$

But $P^N \subset C_K^m$, so

$$P_0 C_K^m = \bigcup_{i=1}^k p_i W C_K^m.$$

Now each $p_i W C_K^m$ is of the form a compact set $(p_i W)$ times a closed set (C_K^m), and hence closed. □

Lemma 5.7.10. *Let P_0 be an open finite index subgroup of P. For each $m \in \mathbb{Z}_{\geq 1}$, there exists an open subgroup $N \subset C_K$ such that $P \cap N = P_0(P \cap C_K^m)$ and $N \supset C_K^m$.*

Proof. By Lemma 5.7.9, $P_0 C_K^m$ and PC_K^m are closed in C_K. Since $P_0 C_K^m$ is a subgroup of finite index and closed in PC_K^m, it is open in the latter. Therefore there exists a neighborhood V of 1 in C_K such that

$$PC_K^m \cap V \subset P_0 C_K^m.$$

Up to shrinking V, we may assume that $C_K^m V$ is a subgroup of C_K^m. (The point is that for each place v, there exist arbitrarily small open neighborhoods V_v of 1 in $K_v^\times$ such that $(K_v^\times)^m V_v$ is a subgroup: If v is non-archimedean we can take V_v to be open subgroups; if v is archimedean we can take V_v to be arbitrary contained in the identity connected component since $(K_v^\times)^m = K_v^\times$ or $(K_v^\times)^m = \mathbb{R}_{>0} \subset K_v^\times = \mathbb{R}^\times$.)

Then we set $N = P_0 C_K^m V$. This is an open subgroup of C_K containing C_K^m. To check that $P \cap N = P_0(P_0 \cap C_K^m)$, we use that for any subsets A, B, C of a group we have $B \cap (AC) = A \cdot (B \cap C)$. Applying this to $A = P_0 C_K^m, B = PC_K^m, C = V$, we get

$$(PC_K^m) \cap N = P_0 C_K^m \cdot (PC_K^m \cap V) = P_0 C_K^m.$$

Hence

$$P \cap N = P \cap PC_K^m \cap N = P \cap (P_0 C_K^m) = P_0(P \cap C_K^m),$$

as desired. □

Proof of Theorem 5.7.8. By Lemma 5.7.10, it suffices to find $m \in \mathbb{Z}_{\geq 1}$ such that $P \cap C_K^m \subset P_0$. First find n such that $P^n \subset P_0$. As in the proof of Lemma 5.7.7, by the Grunwald-Wang theorem we either have $P \cap C_K^n = P^n$ or $P \cap C_K^{2n} \subset P^n$. In all cases taking $m = 2n$ we have $P \cap C_K^m \subset P^n \subset P_0$. □

References

[AT68] Emil Artin and John Torrence Tate. *Class field theory*, volume 366. American Mathematical Soc., 1968. 86, 90, 92

[Bou87] N. Bourbaki. *Topological vector spaces. Chapters 1–5*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1987. Translated from the French by H. G. Eggleston and S. Madan. 8

[CF+67] John William Scott Cassels, Albrecht Fröhlich, et al. Algebraic number theory: Proceedings of an instructional conference organized by the london mathematical society (a nato advanced study institute) with the support of the international mathematical union. 1967. 2

[GW20] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry I: schemes*. Springer, 2020. 6

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994. 77

[Mil20] J.S. Milne. Class field theory (v4.03). pages 287+viii, 2020. Available at `www.jmilne.org/math/`. 2, 71

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. 2, 6, 11, 14

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 2, 11, 12, 14, 19, 21, 63

[Wei40] André Weil. *L'intégration dans les groupes topologiques et ses applications*, volume No. 869 of *Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics]*. Hermann & Cie, Paris, 1940. [This book has been republished by the author at Princeton, N. J., 1941.]. 27

[Wei95] André Weil. *Basic number theory*, volume 144. Springer Science & Business Media, 1995. 24