# Lectures on Algebraic Number Theory

Weizhe Zheng

Morningside Center of Mathematics
Academy of Mathematics and Systems Science, Chinese Academy of Sciences
Beijing 100190, China
Email: wzheng@math.ac.cn

# Contents

# Chapter 1

# Adèles, Idèles

## 1.1 Topological groups

**Definition 1.1.1.** A *topological group* is a group $G$ equipped with a topology such that the maps

$$\begin{aligned} G \times G \to G \quad & (x, y) \mapsto xy \text{ (multiplication)} \\ G \to G \quad & x \mapsto x^{-1} \text{ (inversion)} \end{aligned}$$

are continuous.

**Remark 1.1.2.** The continuity of the multiplication and inversion maps is equivalent to the continuity of the map $G \times G \to G$ given by $(x, y) \mapsto x^{-1}y$.

**Example 1.1.3.**

(1) Any group equipped with the discrete topology is a topological group.

(2) The additive groups $\mathbb{R}$, $\mathbb{C}$ equipped with the Euclidean topology are topological groups. More generally, a finite-dimensional real vector space equipped with the Euclidean topology is a topological group.

(3) The multiplicative groups $\mathbb{R}^\times$, $\mathbb{C}^\times$ equipped with the Euclidean topology are topological groups. More generally, the general linear groups $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$, equipped with the Euclidean topology are topological groups.

(4) The additive group $\mathbb{Q}_p$ and the multiplicative group $\mathbb{Q}_p^\times$ equipped with the topology defined by the $p$-adic absolute value are topological groups.

**Remark 1.1.4.** For $x \in G$, the map $l_x \colon G \to G$ given by $y \mapsto xy$, called *left translation by* $x$, is continuous. Moreover, $l_x$ has a continuous inverse $l_{x^{-1}}$, so $l_x$ is a homeomorphism. Similarly, the map $r_x \colon G \to G$ given by $y \mapsto yx$ (right translation by $x$) is a homeomorphism. It follows that $G$ is a *homogeneous space*, in the sense that given $x, y \in G$, there exists a homeomorphism $G \to G$ sending $x$ to $y$ (for example, $l_{yx^{-1}}$ or $r_{x^{-1}y}$ or $r_y l_x^{-1}$). Thus $G$ looks topologically the same at all points. We can use translations to transfer topological properties from one point to another.

**Lemma 1.1.5.** *For a topological group $G$, the following conditions are equivalent:*

*(1) $G$ is Hausdorff;*

*(2) every point of $G$ is closed;*

*(3) the identity element $e \in G$ is closed.*

Recall that a topological space $X$ is Hausdorff if and only if the diagonal $\Delta_X \subseteq X \times X$ is closed.

*Proof.* (1) ⇒ (2). Clear. (This holds in fact for any topological space.)

(2) ⇒ (3). Trivial.

(3) ⇒ (1). Indeed, (3) implies that $\Delta_G = \phi^{-1}(e)$ is closed in $G \times G$, where

$$\phi \colon G \times G \to G \quad (x, y) \mapsto x^{-1}y.$$

□

Recall that a topological space is *locally compact* if every point admits a compact neighborhood. Every closed subspace of a locally compact space is locally compact. Recall the following fact from general topology:

- Every open subspace of a locally compact Hausdorff space is locally compact ([B1, I.9.7], [H, page 59]). Equivalently, for each point $x$ of a locally compact Hausdorff space, compact neighborhoods of $x$ form a basis of neighborhoods of $x$.

**Definition 1.1.6.** A *locally compact group* is a locally compact Hausdorff topological group.

All the topological groups in Example 1.1.3 are locally compact groups. In (4), $\mathbb{Z}_p$ is a compact neighborhood of 0. Indeed, as the finite discrete spaces $\mathbb{Z}/p^n\mathbb{Z}$ are compact, the compactness of $\mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ follows from the following fact from general topology.

**Lemma 1.1.7.** *Let $(X_i)_{i\in I}$ be a system of compact Hausdorff spaces indexed by a partially ordered set $I$. Then the limit $\varprojlim_{i\in I} X_i$ is compact Hausdorff.*

*Proof.* (1) (Tychonoff's Theorem) The product of a (possibly infinite) family of compact spaces is compact.

(2) The product of a (possibly infinite) family of Hausdorff spaces is Hausdorff.

(3) The limit $V = \varprojlim_{i\in I} X_i$ of a system of Hausdorff spaces is a closed subspace of the product $X = \prod_{i\in I} X_i$. Indeed, $V$ is the intersection of the closed subspaces $V_{ij} \subseteq X$ defined by $\alpha_{ij}(x_i) = x_j$ (inverse image of the graph in $X_i \times X_j$ of the transition map $\alpha_{ij} \colon X_i \to X_j$) for $i \leq j$.

□

## Subgroups

**Lemma 1.1.8.** *Let $G$ be topological group and let $H \subseteq G$ be a subgroup. Then the closure $\bar{H}$ is a subgroup.*

*Proof.* Indeed, we have $\phi^{-1}(H) \supseteq H \times H$, which implies $\phi^{-1}(\bar{H}) \supseteq \overline{H \times H} = \bar{H} \times \bar{H}$ by continuity. □

**Lemma 1.1.9.** *Every open subgroup $H$ of a topological group $G$ is closed.*

*Proof.* Indeed, every left coset $gH$ is open, and $H = G - \bigcup_{gH\neq H} gH$. □

**Proposition 1.1.10.** *Every locally closed subgroup $H$ of a topological group $G$ is closed.*

*Proof.* By the preceding lemmas, $H$ is an open subgroup of $\bar{H}$, hence is closed in $\bar{H}$, thus closed in $G$. □

**Corollary 1.1.11.** *Every locally compact subgroup of a Hausdorff topological group is closed. In particular, every discrete subgroup of a Hausdorff topological group is closed.*

*Proof.* Indeed, every locally compact subset of a Hausdorff space is locally closed, because every compact subset of a Hausdorff space is closed. □

**Corollary 1.1.12.** *A subgroup $H$ of a locally compact group is closed if and only if $H$ is locally compact.*

**Example 1.1.13.** $\mathbb{Z} \subseteq \mathbb{R}$ is a discrete (hence closed) subgroup. $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is an open (hence closed) subgroup.

## Locally profinite groups

This subsection will not be used in the sequel of this chapter or in the next chapter.

The *identity component* of a topological group $G$ is defined to be the connected component containing the identity $e$. It is a normal closed subgroup.

Recall that a topological space $X$ is called *totally disconnected* if the connected components of $X$ are one-point sets. Every subspace of a totally disconnected space is totally disconnected. Every limit of totally disconnected spaces is totally disconnected. A topological group $G$ is totally disconnected if and only if its identity component is $\{e\}$. Totally disconnected groups are Hausdorff.

**Proposition 1.1.14.** *Let $G$ be a locally compact group. The following conditions are equivalent:*

*(1) $G$ is totally disconnected.*
*(2) Every neighborhood of $e$ contains an open subgroup of $G$.*
*(3) The intersection of open subgroups of $G$ is $\{e\}$.*

*Proof.* (1) ⇒ (2). This is [B1, Section III.4, Proposition 14, Corollaire 1].

(2) ⇒ (3). Since $G$ is Hausdorff, the intersection of neighborhoods of $e$ is $\{e\}$.

(3) ⇒ (1). Since open subgroups are closed, the identity component is contained in every open subgroup. □

**Corollary 1.1.15.** *Let $G$ be a topological group. The following conditions are equivalent:*

*(1) $G$ is compact and totally disconnected.*
*(2) $G$ is a filtered limit of discrete finite groups.*
*(3) $G$ is a limit of discrete finite groups.*

*Proof.* (1) $\Rightarrow$ (2). By the proposition, open subgroups of $G$ form a basis of neighborhoods of $e$. Since $G$ is compact, each open subgroup has finite index, hence only a finite number of conjugates. The intersection of the conjugates is a normal open subgroup of $G$. Thus normal open subgroups $V$ of $G$ form a basis of neighborhoods of $e$. The continuous homomorphism $f\colon G \to \varprojlim_V G/V$ has dense image. For every $e \neq g \in G$, there exists $V$ such that $g \notin V$. Thus $f$ is injective. Since $G$ is compact and the target is Hausdorff, $f$ is closed. Therefore, $f$ is an isomorphism of topological groups.

(2) $\Rightarrow$ (3) $\Rightarrow$ (1). Clear. □

**Definition 1.1.16.** A topological group is *locally profinite* (resp. *profinite*) if it is locally compact (resp. compact) and totally disconnected.

**Example 1.1.17.** $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ are profinite groups. $\mathbb{Q}_p$ and $\mathbb{Q}_p^\times$ are locally profinite groups.

**Example 1.1.18.** Let $L/K$ be a (possibly infinite) Galois field extension. Then $\mathrm{Gal}(L/K) \simeq \varprojlim_F \mathrm{Gal}(F/K)$ is a profinite group, where $F$ runs through intermediate fields such that $F/K$ is a finite Galois extension. Conversely, for every profinite group $G$ and every field $k$, there exists an extension $K/k$ and a Galois extension $L/K$ such that $G \simeq \mathrm{Gal}(L/K)$ (Exercise, due to Waterhouse).

## Quotients

Let $H$ be subgroup of a topological group $G$. The left coset space $G/H$ is equipped with the quotient topology. This is the finest topology on $G/H$ such that the quotient map $q\colon G \to G/H$ is continuous. A subset $V \subseteq G/H$ is open if and only if $q^{-1}(V)$ is open.

**Proposition 1.1.19.** *(1) The quotient map $q\colon G \to G/H$ is open.*

*(2) If $H$ is a normal subgroup of $G$, then $G/H$ is a topological group.*

*Proof.* (1) Indeed, for any open subset $U \subseteq G$, $q^{-1}(q(U)) = \bigcup_{h\in H} Uh \subseteq G$ is open, so $q(U) \subseteq G/H$ is open by the definition of quotient topology.

(2) We need to show that the map $\phi'\colon G/H \times G/H \to G/H$ given by $(x,y) \mapsto x^{-1}y$ is continuous. The map sits in the commutative diagram

$$\begin{tikzcd}
G \times G \arrow[r, "\phi"] \arrow[d, "q\times q"'] & G \arrow[d, "q"] \\
G/H \times G/H \arrow[r, "\phi'"] & G/H,
\end{tikzcd}$$

where $\phi\colon (x,y) \mapsto x^{-1}y$. The map $q\times q$ is open and surjective, hence a quotient map. The continuity of $\phi$ and $q$ then implies the continuity of $\phi'$.

□

**Remark 1.1.20.** The product of two quotient maps of topological spaces is not a quotient map in general. For example, if we equip $\mathbb{Q} \subseteq \mathbb{R}$ with the subspace topology and take $q\colon \mathbb{Q} \to X$ to be the quotient map identifying $\mathbb{Z} \subseteq \mathbb{Q}$ to a point, then $q \times q$ is not a quotient map. Indeed, if $U \subseteq \mathbb{R} \times \mathbb{R}$ is an open subset such that $\bar{U} \cap ((\mathbb{Z} \times \mathbb{Q}) \cup (\mathbb{Q} \times \mathbb{Z})) = \emptyset$ and the closure of $p_2(\bar{U} \cap (\mathbb{Z} \times \mathbb{R}))$ contains some $a \in \mathbb{Q}$, then $V = \bar{U} \cap (\mathbb{Q} \times \mathbb{Q}) = (q \times q)^{-1}((q \times q)(V))$ is closed in $\mathbb{Q} \times \mathbb{Q}$ but $(q \times q)(V)$ is not closed because its closure contains $(q \times q)(0, a)$.

**Proposition 1.1.21.** *(1) $H$ is closed if and only if $G/H$ is Hausdorff.*
*(2) $H$ is open if and only if $G/H$ is discrete.*
*(3) If $G$ is locally compact, then $G/H$ is locally compact.*

*Proof.* (1) We use the notation in the proof of the previous proposition. If $G/H$ is Hausdorff, then $\{H\} \subseteq G/H$ is closed, so $H = q^{-1}(\{H\}) \subseteq G$ is closed. Conversely, if $H \subseteq G$ is closed, then $(q \times q)^{-1}(\Delta_{G/H}) = \phi^{-1}(H) \subseteq G \times G$ is closed, so that $\Delta_{G/H} \subseteq G/H \times G/H$ is closed, that is, $G/H$ is Hausdorff.
(2) Indeed, $H$ is open ⇔ the cosets $gH$ are open ⇔ all points of $G/H$ are discrete.
(3) Since $q$ is open, it sends a compact neighborhood of $x \in G$ onto a compact neighborhood of $q(x) \in G/H$.

□

**Proposition 1.1.22** (First isomorphism Theorem)**.** *Let $G$ and $H$ be topological groups and let $f\colon G \to H$ be a continuous homomorphism. Then $f = jf'q$:*

$$G \xrightarrow{q} G/\mathrm{Ker}(f) \xrightarrow{f'} \mathrm{Im}(f) \xrightarrow{j} H,$$

*where $q$ is the quotient map, $j$ is the inclusion, and $f'$ is a continuous group isomorphism. If $f$ is open or closed, then $f'$ is an isomorphism of topological groups (namely, a group isomorphism that is also a homeomorphism).*

*Proof.* The first assertion is clear. If $f$ is open or closed, then the same holds for $f'$, which implies that $f'$ is a homeomorphism. □

**Example 1.1.23** (Second isomorphism theorem)**.** Let $G$ be a topological group, let $H \subseteq G$ be a normal subgroup and let $L \subseteq G$ be a subgroup. Then the map $L \to LH/H$ induces a continuous group isomorphism $L/L \cap H \to LH/H$. This is not an isomorphism of topological groups in general. For example, if $G = \mathbb{R}$, $H = \mathbb{Z}$, $L = \lambda\mathbb{Z}$, $\lambda$ irrational, then $L/L \cap H = L$ is discrete, but $(L + H)/H$ is dense in $\mathbb{R}/\mathbb{Z}$.

**Remark 1.1.24** (Third isomorphism theorem)**.** Let $G$ be a topological group and let $H \subseteq L \subseteq G$ be subgroups such that $H$ is a normal subgroup of $G$. Then the map $f\colon G/L \to (G/H)/(L/H)$ is a homeomorphism. In particular, if $L$ is a normal subgroup of $G$, then $f$ is an isomorphism of topological groups.

We refer to [H] for a more detailed account of topological groups. See also [B1], which discusses completeness [B1, Section III.3] and metrizability [B1, IX.3.1] among other things.

## 1.2 Global fields, Local fields

### Valued fields

**Definition 1.2.1.** A *topological ring* is a ring $R$ equipped with a topology such that the maps

$$\begin{aligned} R \times R \to R &\quad (x, y) \mapsto x + y \\ R \times R \to R &\quad (x, y) \mapsto xy \end{aligned}$$

are continuous. A *topological field* is a field $K$ equipped with a topology such that the maps

$$\begin{aligned} K \times K \to K &\qquad (x, y) \mapsto x + y \\ K \times K \to K &\qquad (x, y) \mapsto xy \\ K^\times \to K^\times &\qquad x \mapsto x^{-1} \end{aligned}$$

are continuous.

**Remark 1.2.2.** The additive group of a topological ring is a topological group. The additive group $K$ and the multiplicative group $K^\times$ of a topological field $K$ are topological groups.

**Definition 1.2.3.** An *absolute value* on a field $K$ is a group homomorphism

$$K^\times \to \mathbb{R}^\times_{>0} \quad x \mapsto |x|,$$

extended by $|0| = 0$, satisfying the triangle inequality

$$|x + y| \leq |x| + |y|$$

for $x, y \in K$. An absolute value on $K$ is *ultrametric* (or *non-Archimedean*) if it satisfies the stronger inequality

$$|x + y| \leq \max\{|x|, |y|\}$$

for $x, y \in K$. A *valued field* (resp. *ultrametric valued field*) is a field equipped with an absolute value (resp. ultrametric absolute value).

An absolute value on $K$ defines a metric on $K$ by $d(x, y) = |x - y|$. The topology induced by this metric makes $K$ a topological field.

**Example 1.2.4.** The *trivial* absolute value

$$|x| = \begin{cases} 1 & x \in K^\times \\ 0 & x = 0 \end{cases}$$

defines the discrete topology on $K$.

**Remark 1.2.5.** Let $x \mapsto |x|$ be an absolute value on $K$. For $0 < r \leq 1$, $x \mapsto |x|^r$ is an absolute value. This follows from the inequality $(a+b)^r \leq a^r + b^r$ for real numbers $a, b \geq 0$. Moreover, if $|-|$ is ultrametric, then for all $r > 0$, $|-|^r$ is an ultrametric absolute value.

**Definition 1.2.6.** Two absolute values on $K$ are *equivalent* if they define the same topology on $K$.

**Proposition 1.2.7.** *Let $x \mapsto |x|_1$, $x \mapsto |x|_2$ be absolute values on a field $K$. The following conditions are equivalent:*

*(1) There exists a real number $r > 0$ such that $|x|_1 = |x|_2^r$.*
*(2) The two absolute values are equivalent.*
*(3) $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$.*

*Moreover, if $x \mapsto |x|_1$ is nontrivial, then the following conditions are both equivalent to the above conditions:*

*(4) The topology defined by $x \mapsto |x|_1$ is finer than the topology defined by $x \mapsto |x|_2$.*
*(5) $|x|_1 < 1 \Rightarrow |x|_2 < 1$.*

*Proof.* We have

$$\begin{tikzcd}
(1) \arrow[r, Rightarrow] & (2) \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (4) \arrow[d, Rightarrow] \\
 & (3) \arrow[r, Rightarrow] & (5).
\end{tikzcd}$$

Indeed, the horizontal implications are trivial. For the vertical ones, it suffices to note that $|x|_i < 1 \Leftrightarrow \lim_{n\to+\infty} x^n = 0$ in the topology defined by $|-|_i$. If $|-|_1$ is trivial, clearly (3) $\Rightarrow$ (1). It remains to show (5) $\Rightarrow$ (1), in the case when $|-|_1$ is nontrivial. In this case, there exists $y \in K^\times$ such that $|y|_1 > 1$. It follows by (5) that $|y|_1 = |y|_2^r$ for some $r > 0$. Let $x \in K^\times$. Then $|x|_1 = |y|_1^a$ for some real number $a$. We need to show $|x|_2 = |y|_2^a$. The idea is to approximate $a$ by rationals. For integers $m, n$ satisfying $n > 0$ and $a < m/n$, we have $|x|_1 < |y|_1^{m/n}$, namely, $|x^n/y^m|_1 < 1$, which implies by (5) that $|x^n/y^m|_2 < 1$, namely $|x|_2 < |y|_2^{m/n}$. Similarly, for $a > m/n$, $|x|_2 > |y|_2^{m/n}$. Thus $|x|_2 = |y|_2^a$. □

For a valued field $K$ and $a \in K$, $r \geq 0$, we consider the closed ball $B_{\leq r}(a) = \{x \mid |x - a| \leq r\}$ and the open ball $B_{<r}(a) = \{x \mid |x - a| \leq r\}$ of center $a$ and radius $r$.

## Ultrametric absolute values

**Proposition 1.2.8.** *An absolute value $|-|$ on $K$ is ultrametric if and only if $|-|$ is bounded on the image of $\mathbb{N}$ in $K$. In particular, every absolute value on a field of characteristic $> 0$ is ultrametric.*

*Proof.* If the absolute value is ultrametric, then

$$|n \cdot 1| = |1 + \cdots + 1| \leq |1| = 1.$$

Conversely, assume $|n| \leq C$ for $n \in \mathbb{N}$. Then for $a, b \in K$,

$$|a+b|^n = |(a+b)^n| = \left|\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\right| \leq \sum_{i=0}^{n} C|a|^i|b|^{n-i} \leq C(n+1)\max\{|a|, |b|\}^n.$$

Thus $|a+b| \leq C^{1/n}(n+1)^{1/n}\max\{|a|,|b|\}$. Taking limit as $n \to +\infty$, we get $|a+b| \leq \max\{|a|,|b|\}$. For the second assertion, it suffices to note that the image of $\mathbb{N}$ in a field of characteristic $> 0$ is a finite set. □

The ultrametric inequality implies that for $|x| \neq |y|$, we have $|x+y| = \max\{|x|,|y|\}$. Indeed, $|y| = |(x+y)-x| \leq \max\{|x|,|x+y|\}$ implies $|x+y| \geq |x|$ and similarly $|x+y| \geq |y|$.

**Remark 1.2.9.** Let $K$ be an ultrametric valued field. Open balls are closed and closed balls of positive radius are open. Any point of a ball is a center: $b \in B_{\leq r}(a)$ implies $B_{\leq r}(a) = B_{\leq r}(b)$ and the same holds for open balls. The *valuation ring* $\mathcal{O}_K = B_{\leq 1}(0)$ is an open subring of $K$ and balls containing 0 are precisely the sub-$\mathcal{O}_K$-modules of $K$. In particular, $\mathfrak{p}_K = B_{<1}(0)$ is the unique maximal ideal of $\mathcal{O}_K$. Balls containing 1 of radius $< 1$ and $B_{<1}(1)$ are subgroups of $\mathcal{O}_K^\times$.

An (additive) *valuation* on a field $K$ is a homomorphism $v\colon K^\times \to \mathbb{R}$, extended by $v(0) = +\infty$, such that $v(x+y) \geq \min\{v(x), v(y)\}$. For any real number $q > 1$, if we put $|x| = q^{-v(x)}$, then $v$ is a valuation if and only if $x \mapsto |x|$ is an ultrametric absolute value. A *discrete valuation* is a valuation $v$ such that $v(K^\times) \subseteq \mathbb{R}$ is a nontrivial discrete subgroup. We usually normalize discrete valuations by $v(K^\times) = \mathbb{Z}$. Elements $\pi \in K$ such that $v(\pi) = 1$ are called *uniformizers* of $K$.

**Example 1.2.10.** Let $K$ be the fraction field of a Dedekind domain $\mathcal{O}_K$. We define a normalized discrete valuation $v_\mathfrak{p}$ on $K$ for every maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ by $x\mathcal{O}_K = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(x)}$. Every nontrivial valuation on $K$, nonnegative on $\mathcal{O}_K$, is of the form $rv_\mathfrak{p}$ for some $r > 0$ and some maximal ideal $\mathfrak{p}$.

## Global fields

The ring of rational integers $\mathbb{Z}$ and the ring of polynomials $k[T]$ over a field $k$ are both principal ideal domains. Maximal ideals of $\mathbb{Z}$ are in bijection with rational primes. There are infinitely many of them. Euclid gave the following proof in *Elements*: for a nonempty finite set of primes $S$, $1 + \prod_{p \in S} p$ has prime factors outside $S$. Maximal ideals of $k[T]$ are in bijection with monic irreducible polynomials. Euclid's argument shows that there are infinitely many of them (trivial for $k$ infinite). There are many other analogies between $\mathbb{Z}$ and $k[T]$, as well as between their fraction fields $\mathbb{Q}$ and $k(T)$, especially when $k$ is a finite field.

**Definition 1.2.11.** A *global field* is either

(1) a *number field*, that is, a finite extension of $\mathbb{Q}$, or
(2) a *function field* (of one variable over a finite field), that is, a finite extension of $\mathbb{F}_p(T)$.

**Definition 1.2.12.** A *place* of a global field $K$ is an equivalence class of nontrivial absolute values on $K$.

**Remark 1.2.13.** Let $k$ be a field. The nontrivial valuations of $k(T)$, trivial on $k$, are multiples of the following:

(1) $v_P\colon k(T)^\times \to \mathbb{Z}$ for monic irreducible polynomials $P$, given by $Q = c\prod_P P^{v_P(Q)}$ for $c \in k^\times$.

(2) $v_\infty\colon k(T)^\times \to \mathbb{Z}$ given by $v_\infty(A/B) = \deg(B) - \deg(A)$, where $A, B \in \mathbb{F}_q[T]$.

Indeed, if $v(T) \geq 0$, then $v$ is nonnegative on $\mathbb{F}_q[T]$ and we get (1) by Example 1.2.10. If $v(T) < 0$, we get (2).

In particular, the places of $\mathbb{F}_q(T)$ are given by the above valuations, since any valuation on $\mathbb{F}_q$ is trivial. More generally, for any smooth projective curve $C$ over a finite field, the places of its function field are in bijection with closed points of $C$.

**Remark 1.2.14.** By Ostrowski's theorem [B3, VI.6.3] or [N, Proposition II.3.7], the places of $\mathbb{Q}$ are the following:

(1) Ultrametric places: given by the $p$-adic absolute values $|{-}|_p$ for rational primes $p$.

(2) Archimedean place: given by the usual absolute value $|{-}|_\infty$.

More generally, the places of any number field $K$ can be described as follows:

(1) Ultrametric places: given by $v_\mathfrak{p}$ for maximal ideals $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of $K$.

(2) Archimedean places: given by $|{-}|_\sigma$ for embeddings $\sigma\colon K \to \mathbb{C}$. Here $|x|_\sigma = |\sigma(x)|_\mathbb{C}$, where $|{-}|_\mathbb{C}$ denotes the usual absolute value on $\mathbb{C}$. Two embeddings $\sigma$ and $\sigma'$ give the same place if and only if $\sigma' = \bar{\sigma}$.

The ultrametric case follows from Example 1.2.10 and let us sketch a proof in the Archimedean case (2). For the first assertion, by Ostrowski's theorem, it suffices to show that any extension $|{-}|$ of $|{-}|_\infty$ to $K$ is given by $|{-}|_\sigma$ for some embedding $\sigma$. For this let $\sigma_1 = \bar{\sigma}_1, \dots, \sigma_{r_1} = \bar{\sigma}_{r_1}, \sigma_{r_1+1} \neq \bar{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2} \neq \bar{\sigma}_{r_1+r_2}\colon K \to \mathbb{C}$ be the embeddings. Consider the isomorphism $K \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ induced by $\sigma_1, \dots, \sigma_{r_1+r_2}$. By the universal property of tensor product, the inclusion of $K$ into its completion $\hat{K}$ with respect to $|{-}|$ induce a homomorphism $K \otimes_Q \mathbb{R} \to \hat{K}$, which must factorize through, the projection from $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ onto, say, its $i$-th factor. Then $|{-}| = |{-}|_{\sigma_i}$. The last assertion follows from the fact that the inclusion $K \to K \otimes_\mathbb{Q} \mathbb{R}$ has dense image.

## Classification of complete Archimedean valued fields

**Theorem 1.2.15** (Ostrowski)**.** *Every complete Archimedean valued field* $(K, |{-}|)$ *is isomorphic to* $(\mathbb{R}, |{-}|_\mathbb{R}^r)$ *or* $(\mathbb{C}, |{-}|_\mathbb{C}^r)$ *for some* $0 < r \leq 1$*, where* $|{-}|_\mathbb{R}$ *and* $|{-}|_\mathbb{C}$ *denote the usual absolute values.*

More generally every complete Archimedean valued division ring $(K, |{-}|)$ is isomorphic to $(\mathbb{R}, |{-}|_\mathbb{R}^r)$, $(\mathbb{C}, |{-}|_\mathbb{C}^r)$, or $(\mathbb{H}, |{-}|_\mathbb{H}^r)$ for some $0 < r \leq 1$.

**Corollary 1.2.16.** *Every Archimedean valued field* $(K, |{-}|)$ *is isomorphic to a subfield of* $(\mathbb{C}, |{-}|_\mathbb{C}^r)$ *for some* $0 < r \leq 1$.

*Proof.* Indeed, it suffices to apply the theorem to the completion of $(K, |{-}|)$. □

We will deduce Theorem 1.2.15 from the following theorem of Stanisław Mazur.

**Theorem 1.2.17** (Mazur)**.** *The underlying algebra of a real normed division algebra is isomorphic to* $\mathbb{R}$, $\mathbb{C}$, *or* $\mathbb{H}$.

**Corollary 1.2.18** (Gelfand-Mazur). *A complex normed division algebra is isomorphic to $\mathbb{C}$.*

For a proof of Mazur's theorem, see [B3, VI.6.4].

*Proof of Theorem 1.2.15.* Since the absolute value is Archimedean, we have $\operatorname{char}(K) = 0$, namely, $\mathbb{Q} \subseteq K$. By the classification of absolute values on $\mathbb{Q}$, the restriction of $|-|$ to $\mathbb{Q}$ is $|-|_\infty^r$ for $r > 0$. By triangle inequality, $2^r = (1+1)^r \leq 1^r + 1^r = 2$, so that $r \leq 1$. We claim that $|-|^{1/r}$ is an absolute value of $K$. The claim follows from a general criterion for absolute values (Proposition 1.6.4). We give a more direct proof of the claim as follows. It suffices to check the triangle inequality. For $a, b \in K$, and $n \geq 1$,

$$|a+b|^n = |(a+b)^n| \leq \sum_{i=0}^{n} \binom{n}{i}^r |a|^i |b|^{n-i} \leq \left(\sum_{i=0}^{n} \binom{n}{i} |a|^{i/r} |b|^{(n-i)/r}\right)^r (n+1)^{1-r}$$
$$= (|a|^{1/r} + |b|^{1/r})^{nr} (n+1)^{1-r}$$

by Hölder's inequality, so that

$$|a+b|^{1/r} \leq (|a|^{1/r} + |b|^{1/r})(n+1)^{(1-r)/nr}.$$

Taking limit as $n \to +\infty$, we get $|a+b|^{1/r} \leq |a|^{1/r} + |b|^{1/r}$, as claimed.

Then, by the completeness of $K$, $(K, |-|^{1/r})$ is an extension of $(\mathbb{R}, |-|_{\mathbb{R}})$. Thus, by Mazur's theorem, $K$ is isomorphic as a real algebra to $\mathbb{R}$ or $\mathbb{C}$. Since $K$ is a finite-dimensional real vector space, the topology induced by $|-|$ must be the Euclidean topology, that is, $|-|$ is equivalent to the usual absolute value. Since the two absolute values coincide on $\mathbb{R}$, they are equal. □

Historically Theorem 1.2.15 predates Mazur's theorem. We refer the reader to [N, Theorem II.4.2] or [I, Section II.3.1] for a more direct proof of Theorem 1.2.15, without using Mazur's theorem.

## Extension of absolute values

**Theorem 1.2.19.** *Let $L/K$ be a field extension of degree $n$ and let $|-|_K$ be an absolute value on $K$. Then there exists an absolute value $|-|_L$ extending $|-|_K$. Moreover, if $|-|_K$ is complete, then the extension is unique, complete, and given by $|x|_L = |\mathrm{Nm}_{L/K} x|_K^{1/n}$.*

Note that the existence and uniqueness extend to the case of algebraic extensions.

*Proof.* We give some indications. In the Archimedean case, by Mazur's Theorem $(K, |-|_K)$ is a subfield of $(\mathbb{C}, |-|_{\mathbb{C}})$ and any $K$-embedding $L \to \mathbb{C}$ provides the desired extension. In the ultrametric case, we may either argue using general valuation rings [B3, VI.8.7], or reduce to the complete case and verify, using Hensel's Lemma, that $|\mathrm{Nm}_{L/K} -|_K^{1/n}$ is an ultrametric absolute value [I, Theorem I.4.4]. The uniqueness and completeness follows from the lemma below. For the last assertion, let $|-|$ be the unique extension of $|-|_K$ to an algebraic closure of $K$. The norm $\mathrm{Nm}_{L/K} x$ is a product of conjugates $x'$ of $x$. By the uniqueness of $|-|$, we have $|x'| = |x|$. Thus $|\mathrm{Nm}_{L/K} x| = |x|^n$. □

**Lemma 1.2.20.** *Any pair of norms on a finite-dimensional vector space over a complete valued field are equivalent and complete.*

See [N, Proposition II.4.9] or [T2, Lemma 8.5.3] for a proof.

Let $(K, v_K)$ be a complete *discrete* valuation field and let $(L, v_L)$ be a finite extension. The ramification index is defined to be the cardinality of $v_L(L^\times)/v_K(K^\times)$. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the valuation rings of $K$ and $L$, respectively. Let $k_K$ and $k_L$ be the residue fields of $K$ and $L$, respectively.

**Proposition 1.2.21.** *$\mathcal{O}_L$ is a free $\mathcal{O}_K$-module with a basis given by $\alpha_i\pi_L^j$, $1 \leq i \leq f$, $0 \leq j \leq e-1$, where $\alpha_1, \dots, \alpha_f \in \mathcal{O}_L$ are elements such that their images in $k_L$ form a basis over $k_K$ (so that $f = [k_L : k_K]$). In particular, $[L : K] = ef$.*

See [T2, Proposition 9.1.4] for a proof.

**Theorem 1.2.22.** *Let $(K, v)$ be a valued field and let $L$ be a finite separable extension of $K$. Then the diagonal embedding $L \to \prod_{w|v} L_w$ induces an isomorphism $L \otimes_K K_v \simeq \prod_{w|v} L_w$.*

Here $w$ runs through extensions of $v$ to $L$ and $K_v$ denotes the completion of $K$ with respect to $v$ and similarly for $L_w$.

*Proof.* Since $L/K$ is a separable extension, we have $L \otimes_K K_v \simeq \prod L_i$, where each $L_i$ is a finite extension of $K_v$, hence a complete valued field by Theorem 1.2.19. Moreover, $L$ is dense in $L \otimes_K K_v$, and hence in $L_i$, so that $L_i = L_w$ for some $w \mid v$. Similarly to the argument at the end of 1.2.14, the universal property of tensor product implies that each $L_w$ appears in the product and the density of $L$ in $L \otimes K_v$ implies that the $L_w$'s appearing in the product are pairwise distinct. □

**Corollary 1.2.23.** *For all $x \in L$, we have*

$$\operatorname{tr}_{L/K}(x) = \sum_{w|v} \operatorname{tr}_{L_w/K_v}(x), \quad \operatorname{Nm}_{L/K}(x) = \prod_{w|v} \operatorname{Nm}_{L_w/K_v}(x).$$

The theorem implies that the diagonal embedding $L \to \prod_{w|v} L_w$ has dense image. More generally, we have the following.

**Theorem 1.2.24** (Approximation)**.** *Let $K$ be a field and let $|-|_1, \dots, |-|_n$ be pairwise nonequivalent nontrivial absolute values. Then the diagonal embedding $K \to \prod_i K_i$, where $K_i$ denotes the completion of $K$ with respect to $|-|_i$, has dense image.*

We refer the reader to [B3, VI.7.3] or [N, II.3.4] for a proof. We will later prove a stronger result in the case of a number field.

## Local fields

**Definition 1.2.25.** A *local field* is a locally compact Hausdorff topological field whose topology is not discrete.

**Example 1.2.26.** $\mathbb{R}$ and $\mathbb{C}$ are local fields.

**Example 1.2.27.** A non trivial valuation field $K$ is a local field if and only if it is a complete discrete valuation field with finite residue field is a local field. Indeed, local compactness implies completeness, which implies that the canonical map $\mathcal{O}_K \to \varprojlim_{r\to 0} \mathcal{O}_K/B_{\le r}(0)$ is an isomorphism. Note that $K$ is locally compact if and only if $\mathcal{O}_K$ is compact. Since the quotient rings $\mathcal{O}_K/B_{\le r}(0)$ are discrete, this is further equivalent to the finiteness of $\mathcal{O}_K/B_{\le r}(0)$, which is equivalent to the conditions that the valuation is discrete and the residue field is finite.

The following are complete discrete valuation fields with finite residue field.

(1) The field of $p$-adic numbers $\mathbb{Q}_p$, equipped with the $p$-adic valuation $v_p$, and more generally finite extensions $K$ of $\mathbb{Q}_p$, equipped with the valuation $x \mapsto v_p(\mathrm{Nm}_{K/\mathbb{Q}_p}(x))$.

(2) The field of formal Laurent series $\mathbb{F}_q((T)) = \{\sum_{i\gg -\infty} a_iT^i \mid a_i \in \mathbb{F}_q\}$ over a finite field $\mathbb{F}_q$, equipped with the valuation $v(\sum a_iT^i) = \min\{i \mid a_i \neq 0\}$.

In particular, the completion of a global field at a place is a local field.

**Theorem 1.2.28.** *A local field is isomorphic to either $\mathbb{R}$, $\mathbb{C}$, a finite extension of $\mathbb{Q}_p$, or $\mathbb{F}_q((T))$.*

More generally, a local division ring is isomorphic to either $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, a division ring of finite rank over $\mathbb{Q}_p$, or a division ring of finite rank over its center $\mathbb{F}_q((T))$. We refer to [B3, Section VI.9] or [W, Chapter I] for a proof in this generality. We will give a proof of the theorem in the characteristic 0 case later.

**Corollary 1.2.29.** *Every local field is the completion of a global field at one place.*

*Proof.* Indeed, $\mathbb{R}$ is a completion of $\mathbb{Q}$, $\mathbb{C}$ is a completion of $\mathbb{Q}(i)$, and $\mathbb{F}_q((T))$ is a completion of $\mathbb{F}_q(T)$. That every finite extension of $\mathbb{Q}_p$ is a completion of a number field is a consequence of Krasner's lemma [T2, Corollary 8.6.3]. □

## Product formula

**Definition 1.2.30.** For an ultrametric local field of residue field $\mathbb{F}_q$, we define the *normalized absolute value* by $|x|_v = q^{-v(x)}$, where $v$ is the normalized valuation. For $\mathbb{R}$, we define the normalized absolute value to be $|-|_{\mathbb{R}}$. For $\mathbb{C}$, we define the normalized absolute value to be $|-|_{\mathbb{C}}^2$ (which is not an absolute value).

**Remark 1.2.31.** Given a finite extension of local fields $L_w/K_v$ of degree $n$, $|-|_w$ extends $|-|_v^n$. This follows from the definition in the Archimedean case and from $n = ef$ in the ultrametric case. Thus, by Theorem 1.2.19, for all $x \in L_w$, we have $|x|_w = |\mathrm{Nm}_{L_w/K_v} x|_v$.

**Theorem 1.2.32.** *Let $K$ be a global field. For $x \in K^\times$, we have $\prod_v |x|_v = 1$. Here $v$ runs through all places of $K$, and $|-|_v$ denotes the normalized absolute value on $K_v$.*

Note that $|x|_v = 1$ for all but finitely many $v$.

*Proof.* The case of $\mathbb{Q}$ and $\mathbb{F}_q(T)$ follows from the explicit description of the absolute values. In general, $K$ is a finite separable extension of $K_0 = \mathbb{Q}$ or $K_0 = \mathbb{F}_q(T)$. We have $\prod_v |x|_v = \prod_{v_0} \prod_{v|v_0} |\mathrm{Nm}_{K_v/(K_0)_{v_0}} x|_{v_0} = \prod_{v_0} |\mathrm{Nm}_{K/K_0} x|_{v_0} = 1$. □

## 1.3 Adèles

Note that infinite products of locally compact groups is not locally compact in general. However, we can construct a locally compact group in the following case. Let $(G_v)_{v\in V}$ be a family of locally compact groups. Assume that for all $v \in V_f = V - V_\infty$, where $V_\infty \subseteq V$ is a finite subset, we are given a compact open (hence closed) subgroup $H_v \subseteq G_v$.

**Definition 1.3.1.** The *restricted product* of the $G_v$ with respect to the $H_v$ is the subgroup $\prod'_{v\in V} G_v \to \prod_{v\in V} G_v$ consisting of elements $(x_v)_{v\in V}$, $x_v \in G_v$ such that $x_v \in H_v$ for all but finitely many $v$. (Note that $H_v$ is concealed in the notation.)

For a finite subset $S \subseteq V$ containing $V_\infty$, we equip

$$G_S = \prod_{v\in S} G_v \times \prod_{v\in V-S} H_v \subseteq \prod{}' G_v$$

with the product topology. We equip $\prod' G_v$ with the finest topology such that the inclusions $G_S \subseteq \prod' G_v$ are continuous.

Note that $\prod' G_v = \bigcup_S G_S$. A fundamental system of neighborhoods of 1 is given by $\prod_{v\in V} N_v$, where $N_v \subseteq G_v$ is a neighborhood of 1, and $N_v = H_v$ for all but finitely many $v$. For any $S$, $G_S$ is a locally compact group, and is an open subgroup of $\prod' G_v$. Moreover, $\prod' G_v$ is a locally compact group.

Note that the inclusion $\prod' G_v \subseteq \prod G_v$ is continuous, but not a homeomorphism onto its image in general. Moreover, replacing $V_\infty$ by a finite subset of $V$ containing $V_\infty$, or changing $H_v$ for finitely many $v$, does not change the restricted product.

**Remark 1.3.2.** If the $G_v$ are topological rings and the $H_v$ are subrings, then $G_S$ and the restricted product are topological rings.

Now let $K$ be a number field. Let $V$ be the set of places of $K$. Let $V_\infty$ be the set of Archimedean places and let $V_f$ be the set of ultrametric places. For $v \in V$, we let $K_v$ denote the completion of $K$ at $v$. For $v \in V_f$, we let $\mathcal{O}_v$ denote the valuation ring of $K_v$.

**Definition 1.3.3.** The adèle ring of $K$ is the restricted product $\mathbb{A}_K = \prod'_{v\in V} K_v$ with respect to the $\mathcal{O}_v$, $v \in V_f$. Elements of $\mathbb{A}_K$ are called adèles (short for "additive idèles") of $K$.

Thus $\mathbb{A}_K$ is a locally compact topological ring. For $x \in K$, the image of $x$ in $K_v$ belongs to the valuation ring $\mathcal{O}_v$ for all but finitely many $v$. We thus get a diagonal embedding of rings $K \to \mathbb{A}_K$.

**Theorem 1.3.4.**

*(1) $K \subseteq \mathbb{A}_K$ is a discrete (hence closed) subring.*

*(2) The quotient group $\mathbb{A}_K/K$ is compact.*

*Proof of (1).* Consider the neighborhood $U = \prod_{v\in V_\infty} U_v \times \prod_{v\in V_f} \mathcal{O}_v$, where $U_v = B_{<1}(0) \subseteq K_v$. For $x \in U$, $\prod_{x\in V} |x|_v < 1$. By product formula, this implies $x \notin K^\times$. Thus $U \cap K = \{0\}$ and consequently $K$ is discrete. □

We will show later that conversely (1) implies the product formula.

To prove (2), we need the following results on approximation. We let $\mathcal{O}_K$ denote the ring of integers of $K$.

**Lemma 1.3.5.** *The subring $\mathcal{O}_K \subseteq \prod_{v\in V_f} \mathcal{O}_v$ is dense.*

Indeed, this follows from the Chinese remainder theorem.

**Proposition 1.3.6.** *Let $K_\infty = \prod_{v\in V_\infty} K_v$. Then*

$$\mathbb{A}_K = K + K_\infty \times \prod_{v\in V_f} \mathcal{O}_v.$$

*Proof.* Let $x \in \mathbb{A}_K$. There exists $a \in \mathcal{O}_K$, $a \neq 0$ such that $ax \in \mathcal{O}_v$ for all $v \in V_f$. Let $S \subseteq V_f$ be the finite set of ultrametric places such that $a \notin \mathcal{O}_v^\times$. By the lemma, for any $\epsilon > 0$, there exists $b \in \mathcal{O}_K$ such that $|b - ax|_v < \epsilon$ for all $v \in S$. Note that $|b - ax|_v \leq 1$ for all $v \in V_f$. For $\epsilon$ small enough, we then have $|\frac{b}{a} - x|_v \leq 1$ for all $v \in V_f$. Thus $x = \frac{b}{a} + (x - \frac{b}{a}) \in K + K_\infty \times \prod_{v\in V_f} \mathcal{O}_v$. □

**Corollary 1.3.7.** *We have an isomorphism of topological groups*

$$\mathbb{A}_K/K \simeq (K_\infty \times \prod_{v\in V_f} \mathcal{O}_v)/\mathcal{O}_K.$$

*Proof.* By the proposition, the homomorphism $K_\infty \times \prod_{v\in V_f} \mathcal{O}_v \to \mathbb{A}_K/K$ is surjective. Moreover, it is open. The kernel $K \cap (K_\infty \times \prod_{v\in V_f} \mathcal{O}_v) = \mathcal{O}_K$, because $\bigcap_{v\in V_f} \mathcal{O}_v = \mathcal{O}_K$. The assertion then follows from the isomorphism theorem. □

Recall that $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R} \simeq K \otimes_{\mathbb{Q}} \mathbb{R} \simeq K_\infty$ and equivalently $\mathcal{O}_K$ is a lattice in $K_\infty$.

For a group $G$ and a subgroup $H$, we say that a subset $D \subseteq G$ is a *fundamental domain* for $H$ if the quotient map $G \to G/H$ induces a bijection $D \simeq G/H$.

*Proof of Theorem 1.3.4 (2).* For a basis $(a_1, \dots, a_n)$ of $\mathcal{O}_K$, $D = \sum_{i=1}^n [-\frac{1}{2}, \frac{1}{2})a_i \subseteq K_\infty$ is a fundamental domain for $\mathcal{O}_K$. Thus $D \times \prod_{v\in V_f} \mathcal{O}_v \subseteq \mathbb{A}_K$ is a fundamental domain for $K$. The map $\bar{D} \times \prod_{v\in V_f} \mathcal{O}_v \to \mathbb{A}_K/K$ is a continuous surjection, and $\bar{D} \times \prod_{v\in V_f} \mathcal{O}_v$ is compact. Therefore, $\mathbb{A}_K/K$ is compact. □

Note that by Corollary 1.3.7, we have a short exact sequence of topological groups

$$0 \to \prod_{v\in V_f} \mathcal{O}_v \to \mathbb{A}_K/K \to K_\infty/\mathcal{O}_K \to 0, \tag{1.3.1}$$

where $K_\infty/\mathcal{O}_K$ and $\prod_{v\in V_f} \mathcal{O}_v$ are compact. Thus the compactness of $\mathbb{A}_K/K$ also follows from the following general fact about topological groups.

**Proposition 1.3.8.** *Let $G$ be a topological group and let $H$ be a subgroup. If $H$ and $G/H$ are compact, then $G$ is compact.*

For a proof, see, for example, [H, p. 48].

**Remark 1.3.9.** Via the diagonal embedding, $\mathbb{A}_K$ becomes a $K$-vector space. Thus $\mathbb{A}_K/K$ is a $K$-vector space, hence a torsion-free abelian group. As $K_\infty/\mathcal{O}_K$ has nonzero torsion elements, the extension (of abelian groups) (1.3.1) is non split.

## 1.4 Haar measures

For a locally compact Hausdorff topological space $X$, we let $C_c(X,\mathbb{R})$ denote the vector space of continuous functions $X \to \mathbb{R}$ with compact support.

**Definition 1.4.1.** A *positive Radon measure* on $X$ is a positive linear functional $\Lambda\colon C_c(X,\mathbb{R}) \to \mathbb{R}$, namely a linear functional such that $\Lambda(f) \geq 0$ for all $f \geq 0$ (here $f \geq 0$ means $f(x) \geq 0$ for all $x \in X$).

**Remark 1.4.2.** We have $C_c(X,\mathbb{R}) = \bigcup_K C_K(X,\mathbb{R})$, where $K$ runs through compact subsets of $X$ and $C_K(X,\mathbb{R})$ denotes continuous functions $X \to \mathbb{R}$ with support in $K$. We equip $C_K(X,\mathbb{R}) \subseteq C(K,\mathbb{R})$ with the topology given by the maximum norm, and we equip $C_c(X,\mathbb{R})$ with the finest topology such that the inclusions $C_K(X,\mathbb{R}) \subseteq C_c(X,\mathbb{R})$ are continuous. Then a positive Radon measure on $X$ is a continuous linear functional $C_c(X,\mathbb{R}) \to \mathbb{R}$ (real Radon measure) by Urysohn's lemma.

**Remark 1.4.3.** Positive Radon measures on $X$ are stable under addition. Moreover, if $\Lambda$ is a positive Radon measure on $X$, and $g\colon X \to \mathbb{R}$ is a continuous function (not necessarily with compact support), $g \geq 0$, we define a positive Radon measure $g\Lambda$ by $(g\Lambda)(f) = \Lambda(gf)$.

**Remark 1.4.4.** For any $\sigma$-algebra $\mathfrak{M}$ in $X$ containing all Borel subsets, and any positive measure $\mu$ (namely, countably additive function $\mathfrak{M} \to [0,\infty]$) satisfying

(1) $\mu(K) < \infty$ for every compact set $K \subseteq X$,

the linear functional $f \mapsto \int_X f\,d\mu$ is a positive Radon measure. Conversely, the Riesz representation theorem (see, for example, [R, 2.14]) states that for any positive Radon measure $\Lambda$ there exists a $\sigma$-algebra $\mathfrak{M}$ in $X$ containing all Borel subsets, and a unique positive measure $\mu$ satisfying (1) above and such that:

- $\Lambda(f) = \int_X f\,d\mu$ for every $f \in C_c(X,\mathbb{R})$.
- $\mu$ is *outer regular*: $\mu(E) = \inf\{\mu(V) \mid E \subseteq V,\ V \text{ open}\}$ for every $E \in \mathfrak{M}$.
- $\mu$ is *inner regular* on open sets: $\mu(E) = \sup\{\mu(K) \mid K \subseteq E,\ K \text{ compact}\}$ for every open subset $E \subseteq X$.

Moreover, $\mu$ satisfies condition (1) above, and is inner regular on $\sigma$-finite sets (countable union of sets $E_i \in \mathfrak{M}$ with $\mu(E_i) < \infty$). (In particular, $\mu$ is inner regular if $X$ is $\sigma$-compact, namely, a countable union of compact subsets.) Furthermore, there exists a biggest $\mathfrak{M}$ characterized by the following additional properties:

- $\mu$ is *complete*: if $\mu(E) = 0$ for $E \in \mathfrak{M}$ and if $A \subseteq E$, then $A \in \mathfrak{M}$.
- If $E \subseteq X$ is such that $E \cap K \in \mathfrak{M}$ for every compact subset $K \subseteq X$, then $E \in \mathfrak{M}$.

We sometimes identify $\mu$ and $\Lambda$ via the above correspondence. $\mu(X) \in [0,\infty]$ is sometimes called the *volume* of $X$.

Let $G$ be locally compact group, let $f \in C_c(X,\mathbb{R})$, and let $\Lambda$ be a positive Radon measure. For $g \in G$, we define the *left translation of $f$ by $g$*, $L_g f$, by $(L_g f)(x) = f(g^{-1}x)$ and the *left translation of* $\Lambda$ *by* $g$, $L_g\Lambda$, by $(L_g\Lambda)(f) = \Lambda(L_{g^{-1}}f)$. Correspondingly, $L_g\mathfrak{M} = \{gE \mid E \in \mathfrak{M}\}$ and $(L_g\mu)(E) = \mu(g^{-1}E)$.

**Definition 1.4.5.** A *left Haar measure* on $G$ is a nonzero positive Radon measure $\mu$ that is left-invariant, namely, $L_g\Lambda = \Lambda$ for all $g \in G$.

Similarly one defines right Haar measures. For abelian groups, left Haar measures and right Haar measures are the same and are simply called Haar measures.

A positive scalar multiple of a left Haar measure is a left Haar measure.

**Theorem 1.4.6** (Haar)**.** *For any locally compact group, there exists a left Haar measure, unique up to scalar multiple.*

See [B2, VII.1.2] or [H, Chapter III] for a proof. We will sketch a proof below in the case of the additive group of a local field (assuming Theorem 1.2.28).

**Proposition 1.4.7.** *Let $\mu$ be a left Haar measure on a locally compact group $G$.*

*(1) For any nonempty open subset $U \subseteq G$, $\mu(U) > 0$ (may be $\infty$).*

*(2) For any function $f \in C_c(G, \mathbb{R})$, $f \geq 0$, $f \neq 0$ ($f$ not identically zero), we have $\int f \, d\mu > 0$.*

*Proof.* (1) Since $\mu \neq 0$ is inner regular on open sets, there exists a compact subset $K \subseteq G$ such that $\mu(K) > 0$. Since $K \subseteq \bigcup_{g \in G} gU$, $K$ is covered by finitely many left-translates $g_i U$ of $U$. It follows that $\mu(g_i U) > 0$ for some $i$. We conclude by $\mu(U) = \mu(g_i U)$.

(2) Indeed, there exists $\epsilon > 0$ such that the open subset $U = f^{-1}((\epsilon, \infty)) \subseteq G$ is nonempty. Then $\int f \, d\mu \geq \epsilon \mu(U) > 0$.

□

**Example 1.4.8.** For a discrete group $G$, the counting measure $\mu(E) = \#E$, $E \subseteq G$ is a left Haar measure (and a right Haar measure). We have $\int f \, d\mu = \sum_{g \in G} f(g)$. In this case, the left Haar measure is clearly unique up to scalar.

**Example 1.4.9.** For $G = \mathbb{R}^n$ or $G = K$ an ultrametric local field, let us sketch a proof for the existence and uniqueness of Haar measure. For $G = \mathbb{R}^n$, let $Q_0 = [0,1)^n$ and let $\Omega_m = \{A^{-m}(Q_0 + a) \mid a \in \mathbb{Z}^n\}$, where $A \geq 2$ is an integer. For $G = K$, let $Q_0 = \mathcal{O}_K$ and let $\Omega_m$ be the collection of translates of $\pi^m \mathcal{O}_K$. Then for each $m$, $\Omega_m$ is a partition of $G$. Moreover, $Q_0$ is the disjoint union of $q^m$ elements of $\Omega_m$, where $q = A^n$ for $G = \mathbb{R}^n$ and $q = \#k$ for $G = K$ of residue field $k$. Choose $x_Q \in Q$ for each $Q \in \Omega_m$. For $f \in C_c(G, \mathbb{R})$, consider the Riemann sum $\Lambda_m f = q^{-m} \sum_{Q \in \Omega_m} f(x_Q)$ associated to the step function $f_m = \sum_{Q \in \Omega_m} f(x_Q) \mathbf{1}_Q$, where $\mathbf{1}_Q$ denotes the characteristic function of $Q$. By uniform continuity, $\Lambda_m f$ is a Cauchy sequence. Let $\Lambda f = \lim_{m \to \infty} \Lambda_m f$. It follows from the construction that $\Lambda$ is a Haar measure on $G$. For $G = \mathbb{R}^n$, $\Lambda$ is the Lebesgue measure.

Conversely, let $\mu$ is a Haar measure on $G$. Then $\mu(Q) = q^{-m}\mu(Q_0)$ for each $Q \in \Omega_m$. For $f \in C_c(G, \mathbb{R})$, by uniform continuity,

$$\int f \, d\mu = \lim_{m \to \infty} \int f_m \, d\mu = \lim_{m \to \infty} \mu(Q_0) \Lambda_m f = \mu(Q_0) \Lambda f,$$

which proves the uniqueness up to scalar multiple.

Note that for $G = K$ in the previous example, the step functions $f_m$ are locally constant and compactly-supported. Note also that locally constant functions on $K$ are continuous.

**Definition 1.4.10.** Let $K$ be an ultrametric local field. A *Schwartz-Bruhat function* on $K$ is a locally constant compactly-supported function on $K$.

**Lemma 1.4.11.** *Let $K$ be an ultrametric local field. A function is a Schwartz-Bruhat function if and only if it is a finite sum $\sum_i c_i \mathbf{1}_{B_i}$, where each $c_i$ is a constant and each $B_i$ is an open ball.*

*Proof.* A finite sum of the above form is obviously a Schwartz-Bruhat function. Conversely, let $f$ be a Schwartz-Bruhat function. Each point $a \in K$ admits an open ball containing $a$ on which $f$ is constant. The support is covered by a finite family of such balls $(B_i)$. We may assume that there are no inclusions among the family. Then the family is disjoint and $f = \sum_i f(x_i)\mathbf{1}_{B_i}$, where $x_i \in B_i$. □

## Modulus

Let $G$ be a locally compact group, and let $\phi$ be an automorphism of $G$ (as topological group). For any left Haar measure $\mu$ on $G$, $\phi^{-1}\mu$ defined by $(\phi^{-1}\mu)(E) = \mu(\phi(E))$ is a left Haar measure on $G$, and thus is a scalar multiple of $\mu$.

**Definition 1.4.12.** The real number $c > 0$ such that $\phi^{-1}\mu = c\mu$ is called the modulus of $\phi$ and is denoted $\mathrm{mod}(\phi)$.

In other words,

$$\mu(\phi(E)) = \mathrm{mod}(\phi)\mu(E), \quad \int f(\phi^{-1}(x))\, d\mu(x) = \mathrm{mod}(\phi) \int f(x)\, d\mu(x).$$

Note that $\mathrm{mod}(\phi)$ does not depend on the choice of $\mu$. If $\psi$ is another automorphism of $G$, then $\mathrm{mod}(\phi\psi) = \mathrm{mod}(\phi)\mathrm{mod}(\psi)$.

**Proposition 1.4.13.** *If $G$ is compact or discrete, then* $\mathrm{mod}(\phi) = 1$.

*Proof.* We have

$$\mu(G) = \mu(\phi(G)) = \mathrm{mod}(\phi)\mu(G), \quad \mu(\{e\}) = \mu(\phi(\{e\})) = \mathrm{mod}(\phi)\mu(\{e\}).$$

For $G$ compact, $0 < \mu(G) < \infty$. For $G$ discrete, $0 < \mu(\{e\}) < \infty$. □

**Example 1.4.14.** For $G = \mathbb{R}^n$, $\phi$ is a linear transformation $\mathrm{mod}(\phi) = |\det(\phi)|$.

**Example 1.4.15.** For $G = K$ a local field, $a \in K^\times$, multiplication by $a$ provides an automorphism $\phi_a \colon K \to K$. We write $\mathrm{mod}(a)$ for $\mathrm{mod}(\phi_a)$, so that $\mu(aE) = \mathrm{mod}(a)\mu(E)$. We obtain thus a homomorphism $\mathrm{mod}\colon K^\times \to \mathbb{R}^\times_{>0}$, which can be extended by $\mathrm{mod}(0) = 0$. If $K$ is ultrametric with residue field $\mathbb{F}_q$, $\mathrm{mod}(a) = q^{-v(a)}$, where $v$ is the normalized valuation. If $K = \mathbb{R}$, $\mathrm{mod}(a) = |a|_\mathbb{R}$. If $K = \mathbb{C}$, $\mathrm{mod}(a) = |a|^2_\mathbb{C}$. In other words, mod is the normalized absolute value on $K$. Note that for $K = \mathbb{C}$, mod is not an absolute value.

For $f \in C_c(K^\times, \mathbb{R})$, $\frac{f}{\mathrm{mod}}$ extended by $0 \mapsto 0$ belongs to $C_c(K, \mathbb{R})$. We define a positive Radon measure $\mu/\mathrm{mod}$ on $K^\times$ by $f \mapsto \int \frac{f}{\mathrm{mod}}\, d\mu$. We have

$$\int \frac{f(ax)}{\mathrm{mod}(x)}\, d\mu(x) = \mathrm{mod}(a) \int \frac{f(ax)}{\mathrm{mod}(ax)}\, d\mu(x) = \int \frac{f(x)}{\mathrm{mod}(x)}\, d\mu.$$

Thus $\mu/\mathrm{mod}$ is a Haar measure on $K^\times$.

## Products

Let $X$ and $Y$ be locally compact Hausdorff spaces. Let $\mu$ be a positive Radon measure on $X$ and let $\nu$ be a positive Radon measure on $Y$.

**Proposition 1.4.16** (Fubini's Theorem)**.** *For $f \in C_c(X \times Y, \mathbb{R})$, we have $y \mapsto \int f(x,y)\,d\mu(x) \in C_c(Y,\mathbb{R})$, $x \mapsto \int f(x,y)\,d\nu(y) \in C_c(X,\mathbb{R})$, and*

$$\int d\mu(x) \int f(x,y)\,d\nu(y) = \int d\nu(x) \int f(x,y)\,d\mu(y).$$

We thus obtain a positive Radon measure on $\mu \times \nu$, which we denote by $\mu \times \nu$.

The first two assertions follows from uniform continuity of continuous functions on compact spaces. The last assertion holds trivially for functions of the form $f \otimes g$ given by $(x,y) \mapsto f(x)g(y)$, where $f \in C_c(X,\mathbb{R})$ and $g \in C_c(Y,\mathbb{R})$. The general case follows from the fact that such functions form a dense subspace of $C_c(X \times Y, \mathbb{R})$. We refer to [B2, III.4.1] (or [H, Section III.6] for details.

**Remark 1.4.17.** If $X$ and $Y$ are locally compact groups and $\mu$ and $\nu$ are left Haar measures, then $\mu \times \nu$ is a left Haar measure on $X \times Y$. In this case, the last assertion of the proposition also follows from the fact that both sides of the equation define left Haar measures on $X \times Y$.

The above extends trivially to products of finitely many measures. For infinite products, consider a family of *compact* Hausdorff spaces $(X_i)_{i\in I}$, and for each $i \in I$, a positive Radon measure $\mu_i$ on $X_i$. Then $X = \prod_{i\in I} X_i$ is a compact Hausdorff space. For any finite subset $J \subseteq I$, let $X_J = \prod_{j\in J} X_j$ and let $\mathrm{pr}_J \colon X \to X_J$ be the projection. We let $\mu_J$ denote the positive Radon measure $\prod_{j\in J}\mu_j$ defined above.

**Proposition 1.4.18.** *Assume that $\prod_{i\in I}\mu_i(X_i)$ converges (to a positive real number). Then there exists a unique positive Radon measure $\mu$ on $X$ such that for every finite subset $J \subseteq I$ and every $f_J \in C(X_J,\mathbb{R})$,*

$$\int f_J \circ \mathrm{pr}_J\, d\mu = \prod_{i\in I-J} \mu_i(X_i) \int f_J\, d\mu_J.$$

We let $\prod_{i\in I}\mu_i$ denote the measure $\mu$ in the proposition. If the $X_i$'s are compact groups and the $\mu_i$'s are left Haar measures, then $\prod_{i\in I}\mu$ is a left Haar measure on $X$.

*Proof.* Let $F \subseteq C(X,\mathbb{R})$ be the space of functions of the form $f_J \circ \mathrm{pr}_J$ for some finite subset $J \subseteq I$. Note that $F$ is stable under addition. Indeed,

$$f_J \circ \mathrm{pr}_J + f_{J'} \circ \mathrm{pr}_{J'} = f_{J\cup J'} \circ \mathrm{pr}_{J\cup J'},$$

where $f_{J\cup J'} = f_J \circ p + f_{J'} \circ p'$, and $p\colon X_{J\cup J'} \to X_J$, $p'\colon X_{J\cup J'} \to X_{J'}$ are projections. Similarly, $F$ is stable under multiplication. Thus $F$ is a real subalgebra of $C(X,\mathbb{R})$. Let $x \neq y$ be distinct points in $X$. Then there exists $i \in I$ such that $x_i \neq y_i$. For any $f_i \in C(X_i,\mathbb{R})$ such that $f_i(x_i) \neq f_i(y_i)$, $f_i \circ \mathrm{pr}_i$ separates $x$ and $y$, where $\mathrm{pr}_i = \mathrm{pr}_{\{i\}}\colon X \to X_i$. Therefore, by the theorem below, $F$ is dense in $C(X,\mathbb{R})$. The equation in the proposition defines a positive linear functional $\Lambda$ on $F$. The assumption assures that $\Lambda$ is continuous. Thus $\Lambda$ extends uniquely to a positive linear functional on $C(X,\mathbb{R})$. □

**Theorem 1.4.19** (Stone-Weierstrass). *Let $X$ be a compact Hausdorff space. Then any real subalgebra of $C(X,\mathbb{R})$ that separates points is dense.*

For a proof, see [B1, X.4.2].

**Remark 1.4.20.** Let $(G_v)_{v\in V}$, $H_v \subseteq G_v$, $v \in V_f$ be as in the beginning of Section 1.3. Recall that the restricted product $G = \prod' G_v = \bigcup G_S$, where $G_S = \prod_{v\in S} G_v \times \prod_{v\in V-S} H_v$, $S$ runs through finite subsets of $V$ containing $V_\infty$. Since $G_S \subseteq G$ is open, extension by zero provides an inclusion $C_c(G_S,\mathbb{R}) \subseteq C_c(G,\mathbb{R})$. We have $C_c(G,\mathbb{R}) = \bigcup C_c(G_S,\mathbb{R})$. For each $v \in V$, let $\mu_v$ be a positive Radon measure on $G_v$. Assume that $\prod_{v\in V-V_\infty} \mu_v(H_v)$ converges. Then we have product measures $\mu_S$ on $G_S$, compatible with the inclusions $C_c(G_S,\mathbb{R}) \subseteq C_c(G_{S'},\mathbb{R})$ for $S \subseteq S'$. Thus we obtain a positive Radon measure $\mu = \prod'_{v\in V} \mu_v$ on $G$. Functions of the form $f_S \otimes \mathbf{1}_{H^S}$, where $f_S \in C_c(\prod_{v\in S} G_v,\mathbb{R})$ and $H^S = \prod_{v\in V-S} H_v$, form a dense subset of $C_c(G,\mathbb{R})$.

If the $\mu_v$'s are left Haar measures, then $\mu$ is a left Haar measure.

**Example 1.4.21.** Let $K$ be an number field. For $v$ ultrametric, we take the Haar measure $\mu_{K_v}$ normalized by $\mu_{K_v}(\mathcal{O}_v) = 1$. We take $\mu_\mathbb{R}$ to be the Lebesgue measure, and $\mu_\mathbb{C}$ to be twice the Lebesgue measure (via the isomorphism $\mathbb{R}\times\mathbb{R} \simeq \mathbb{C}$ given by $(x,y) \mapsto x+yi$). We obtain a Haar measure $\prod'_{v\in V} \mu_{K_v}$ on $\mathbb{A}_K$.

## Quotients

Let $G$ be a locally compact group and let $H$ be a closed subgroup. Let $\nu$ be a left Haar measure on $H$. For $f \in C_c(G,\mathbb{R})$, the function $x \mapsto \int f(xh)\,dh$ on $G$ defines a function of $G/H$, that we denote by $f^\flat$.

**Lemma 1.4.22.** *We have $f^\flat \in C_c(G/H,\mathbb{R})$ and the map $C_c(G,\mathbb{R}) \to C_c(G/H,\mathbb{R})$ given by $f \mapsto f^\flat$ is surjective.*

*Proof.* The first assertion follows from uniform continuity. For the second assertion, let $g \in C_c(G/H,\mathbb{R})$ and let $K \subseteq G$ be a compact subset such that the support of $g$ is contained in $KH$. Let $u \in C_c(G,\mathbb{R})$ be such that $u \geq 0$ and $u(x) > 0$ for $x \in K$. Then $u^\flat(y) > 0$ for $y \in KH/H$. The function $h = g/u^\flat$, extended by zero outside $KH/H$, belongs to $C_c(G/H)$. Let $\pi\colon G \to G/H$ be the projection. Then $f = u(h\circ\pi) \in C_c(G,\mathbb{R})$ and $f^\flat = g$. □

The following is an immediate consequence of the lemma.

**Proposition 1.4.23.** *For a positive Radon measure $\lambda$ on $G/H$,*

$$\int f\,d\lambda^\sharp = \int f^\flat\,d\lambda$$

*defines a positive Radon measure $\lambda^\sharp$ on $G$. Conversely, given a positive Radon measure $\mu$ on $G$, there exists at most one positive Radon measure $\lambda$ on $G/H$ such that $\mu = \lambda^\sharp$.*

In the situation of the proposition, $\lambda$ is called the quotient measure of $\mu = \lambda^\sharp$ by $\nu$, and is denoted by $\mu/\nu$.

**Remark 1.4.24.** Assume that $H$ is a normal subgroup of $G$. If $\lambda$ is a left Haar measure on $G/H$, then $\mu$ in the above proposition is a left Haar measure on $G$. Conversely, if $\mu$ is a Haar measure on $G$, then $\mu/\nu$ exists and is a Haar measure on $G/H$.

**Example 1.4.25.** If $H'$ is a locally compact group such that $G = H \times H'$, and $\nu'$ is a positive Radon measure on $H'$, then $(\nu \times \nu')/\nu = \nu'$.

**Proposition 1.4.26.** *Let $H$ be a normal subgroup of a locally compact group $G$. Let $\phi$ be an automorphism of $G$ (as topological group) such that $\phi(H) = H$ and let $\phi_H$, $\phi_{G/H}$ be the induced automorphisms of $H$ and of $G/H$. Then* $\mathrm{mod}(\phi) = \mathrm{mod}(\phi_H)\mathrm{mod}(\phi_{G/H})$.

*Proof.* Let $\mu$, $\nu$, $\lambda$ be left Haar measures on $G$, $H$, $G/H$, respectively. Then

$$\begin{aligned}\int f(\phi^{-1}(x))\, d\mu(x) &= \int d\lambda(\dot{x}) \int f(\phi^{-1}(xh))\, d\nu(h)\\ &= \mathrm{mod}(\phi_H) \int d\lambda(\dot{x}) \int f(\phi^{-1}(x)h)\, d\nu(h) = \mathrm{mod}(\phi_H)\mathrm{mod}(\phi_{G/H}) \int f(x)\, d\mu(x),\end{aligned}$$

where $\dot{x} = xH$. □

**Corollary 1.4.27.** *Let $H$ be a discrete normal subgroup of a locally compact group $G$ such that $G/H$ is compact. For any automorphism $\phi$ of $G$ such that $\phi(H) = H$,* $\mathrm{mod}(\phi) = 1$.

*Proof.* This follows from the above proposition and Proposition 1.4.13. □

**Definition 1.4.28.** The *content* of an adèle $x \in \mathbb{A}_K$ is defined to be $|x| = \prod_{v\in V} |x_v|_v \geq 0$, where $|-|_v$ denotes the normalized absolute value on $K_v$.

For $x, y \in \mathbb{A}_K$, we have $|xy| = |x||y|$. Note however that triangle inequality does not hold. The function $x \mapsto |x|$ on $\mathbb{A}_K$ is *not* continuous, since every neighborhood of $1 \in \mathbb{A}_K$ contains an adèle of content 0.

**Remark 1.4.29.** For $x \in \mathbb{A}_K^\times$, $|x|$ is the modulus of the automorphism $\mathbb{A}_K \to \mathbb{A}_K$ given by $y \mapsto xy$. Since $\mathbb{A}_K/K$ is compact, Corollary 1.4.27 implies the product formula: for $x \in K^\times$, $|x| = 1$. In other words, the product formula is equivalent to the discreteness of $K \subseteq \mathbb{A}_K$.

**Example 1.4.30.** Let $L = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n \subseteq \mathbb{R}^n$ be a lattice and let $\mu$ be the quotient of the Lebesgue measure on $\mathbb{R}^n$ by the counting measure on $L$. Then $\mu(\mathbb{R}^n/L) = |\det(e_1, \dots, e_n)|$.

**Example 1.4.31.** Let $K$ be a number field. We consider the quotient of the Haar measure on $\mathbb{A}_K$ in Example 1.4.21 by the counting measure on $K$. We have

$$\mathrm{vol}(\mathbb{A}_K/K) = \mathrm{vol}(K_\infty/\mathcal{O}_K)\mathrm{vol}(\prod_{v\in V_f} \mathcal{O}_v) = \mathrm{vol}(K_\infty/\mathcal{O}_K) = \sqrt{|\Delta_K|},$$

where $\Delta_K$ is the discriminant of $K$. For the last identity, recall that $\Delta_K = \det(\sigma_i(\alpha_j))^2$, where $(\alpha_1, \dots, \alpha_n)$ is an integral basis of $\mathcal{O}_K$ and $\sigma_1, \dots, \sigma_n$ are the embeddings of

$K$ into $\mathbb{C}$. Let $\lambda\colon K \to K_\infty = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ be the embedding induced by the isomorphism $\mathbb{C} \simeq \mathbb{R}^2$ given by taking real and imaginary parts. Under a suitable ordering of the $\sigma_i$, we have

$$(\sigma_i(\alpha_j)_{ij} = \begin{pmatrix} I_{r_1} & 0 & 0 & 0 \\ 0 & \begin{smallmatrix} 1 & -i \\ 1 & i \end{smallmatrix} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \begin{smallmatrix} 1 & -i \\ 1 & i \end{smallmatrix} \end{pmatrix} = (\lambda(\alpha_1), \dots, \lambda(\alpha_n)),$$

so that $\det(\sigma_i(\alpha_j)) = (2i)^{r_2} \det(\lambda(\alpha_1), \dots, \lambda(\alpha_n))$. Thus

$$\mathrm{vol}(K_\infty/\mathcal{O}_K) = 2^{r_2}\mathrm{vol}(\mathbb{R}^n/\lambda(\mathcal{O}_K)) = |\det(\sigma_i(\alpha_j))| = \sqrt{|\Delta_K|},$$

where $\mathbb{R}^n$ is equipped with the Lebesgue measure.

## Application: Strong approximation

Let $K$ be a number field.

**Theorem 1.4.32** (Minkowski). *For constants $(c_v)_{v\in V}$, $c_v \in |K_v^\times|_v$, $c_v \leq 1$ for all but finitely many $v$, satisfying*

$$\prod_{v\in V} c_v > (2/\pi)^{r_2}\sqrt{|\Delta_K|},$$

*there exists $a \in K^\times$ such that $|a|_v \leq c_v$ for all $v \in V$. Here $|-|_v$ denotes the normalized absolute value on $K_v$, and $r_2$ is the number of complex places.*

*Proof.* Let $B_v = B_{\leq c_v}(0) \subseteq K_v$ for $v \in V_f$, let $B_v = B_{\leq c_v/2}(0) \subseteq \mathbb{R}$ for $v$ real and let $B_v = \{z \in \mathbb{C} \mid |z| \leq \sqrt{c_v}/2\}$ (where $|-|$ denotes the usual absolute value) for $v$ complex. Let $X = \prod_{v\in V} B_v \subseteq \mathbb{A}_K$. Let $\mu_v$ be the normalized Haar measure on $K_v$ and let $\mu = \prod'_{v\in V} \mu_v$. Then $\mu_v(B_v) = c_v$ for $v \in V_f$ or $v$ real, and $\mu_v(B_v) = \frac{\pi}{2}c_v$ for $v$ complex. Thus $\mu(X) = (\pi/2)^{r_2}\prod_{v\in V} c_v > \mathrm{vol}(\mathbb{A}_K/K)$. It follows that there exist $x, y \in X$, $x \neq y$ such that $x - y \in K$. It then suffices to take $a = x - y$. □

Minkowski's theorem is more frequently stated in the following form.

**Corollary 1.4.33.** *Let $I$ be a fractional ideal of $\mathcal{O}_K$. For constants $(c_v)_{v\in V_\infty}$ satisfying*

$$\prod_{v\in V} c_v > (2/\pi)^{r_2}\sqrt{|\Delta_K|}\mathrm{Nm}(I),$$

*there exists $a \in I$, $a \neq 0$ such that $|a|_v \leq c_v$ for all $v \in V_\infty$.*

Here the norm of an ideal is defined to be $\mathrm{Nm}(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$ and this definition extends to fractional ideals by multiplicativity.

The corollary is equivalent to the theorem. Indeed, for $I = \prod_v \mathfrak{p}_v^{m_v}$ it suffices to take $c_v = q_v^{-m_v}$ for $v \in V_f$.

We refer the reader to [N, Theorem I.5.3] for a more direct proof of Corollary 1.4.33.

**Corollary 1.4.34.** *Let $v_0 \in V$. For positive constants $(c_v)_{v\in V-\{v_0\}}$, $c_v = 1$ for all but finitely many 1, there exists $a \in K^\times$ such that $|a|_v \leq c_v$ for all $v \neq v_0$.*

*Proof.* Indeed, we may assume that $c_v \in |K_v^\times|_v$ for all $v \neq v_0$. In this case, we apply the proposition by taking $c_{v_0}$ large enough. □

**Theorem 1.4.35** (Strong approximation)**.** *Let $v_0 \in V$. Then the diagonal embedding $K \to \prod'_{v\in V-\{v_0\}} K_v$ has dense image. In other words, $K + K_{v_0}$ is dense in $\mathbb{A}_K$.*

**Corollary 1.4.36.** *$\mathbb{A}_K/K$ is connected.*

*Proof.* For $v_0 \in V_\infty$, the theorem implies that the image of $K_{v_0}$ in $\mathbb{A}_K/K$ is dense. □

*Proof of Theorem 1.4.35.* The assertion is equivalent to saying that for all $x \in \mathbb{A}_K$, and positive constants $(\epsilon_v)_{v\in V-\{v_0\}}$ such that $\epsilon_v = 1$ for all but finitely many $v$, there exists $a \in K$ such that $|a - x_v|_v \leq \epsilon_v$ for all $v \in V - \{v_0\}$. We have seen in the construction of fundamental domain (proof of Theorem 1.3.4) that there exist positive constants $(c_v)_{v\in V}$, $c_v = 1$ for all $v \in V_f$ such that every $y \in \mathbb{A}_K$ is of the form $y = b + y'$ with $b \in K$ and $|y'_v|_v \leq c_v$ for all $v \in V$. By Corollary 1.4.34, there exist $\alpha \in K^\times$ such that $|\alpha|_v \leq \epsilon_v/c_v$ for all $v \neq v_0$. Taking $y = \alpha^{-1}x$ (extended to an element of $\mathbb{A}_K$), we get $x = \alpha b + \alpha y'$, with $\alpha b \in K$ and $|\alpha y'|_v \leq \epsilon_v$. □

## 1.5 Idèles

Idèles were introduced by Chevalley first under the name "élément idéal" (ideal element), then abbreviated by him to "idèle".

Let $K$ be a number field. We use the notation of 1.3. Note that $\mathcal{O}_v^\times$ is compact for $v \in V_f$.

**Definition 1.5.1.** The *idèle group* of $K$ is the restricted product $\mathbb{I}_K = \prod'_{v\in V} K_v^\times$ with respect to $\mathcal{O}_v^\times$ for $v \in V_f$. Elements of $\mathbb{I}_K$ are called *idèles* of $K$.

**Remark 1.5.2.** As groups $\mathbb{I}_K = \mathbb{A}_K^\times$. The inclusion map $\mathbb{I}_K \to \mathbb{A}_K$ is continuous, but not a homeomorphism onto its image. The map $\mathbb{I}_K \to \mathbb{A}_K \times \mathbb{A}_K$ carrying $x$ to $(x, x^{-1})$ identifies $\mathbb{I}_K$ with a subspace of $\mathbb{A}_K \times \mathbb{A}_K$. In other words, the topology on $\mathbb{I}_K$ is the coarsest topology such that the inclusion $\mathbb{I}_K \to \mathbb{A}_K$ and the inversion $\mathbb{I}_K \to \mathbb{I}_K$ are continuous.

The diagonal embedding $K \to \mathbb{A}_K$ induces the diagonal embedding $K^\times \to \mathbb{I}_K$.

**Lemma 1.5.3.** *$K^\times \subseteq \mathbb{I}_K$ is a discrete subgroup.*

*Proof.* This follows from the facts that $K \subseteq \mathbb{A}_K$ is discrete and the topology of $\mathbb{I}_K$ is finer than the subspace topology induced from the topology of $\mathbb{A}_K$. □

Images of the embedding $K^\times \to \mathbb{I}_K$ are called *principal idèles* of $K$ and the (locally compact) quotient group $\mathbb{I}_K/K^\times$ is called the *idèle class group.*

Recall the content of $x \in \mathbb{A}_K$ is defined to be $|x| = \prod_v |x_v|_v$. Note that $x \in \mathbb{I}_K$ if and only if $x_v \in K_v^\times$ for all $v$ and $|x_v|_v = 1$ for all but finitely many $v$. In this case $|x|$ is essentially a finite product.

**Lemma 1.5.4.** *For $x \in \mathbb{A}_K$, $|x| > 0$ if and only if $x \in \mathbb{I}_K$.*

*Proof.* The "if" part is clear. Conversely, $|x| > 0$ trivially implies $x_v \in K_v^\times$. Moreover, for $v \in V_f$, $|x_v|_v \notin (1/2, 1)$, so $|x| > 0$ also implies that $|x_v|_v = 1$ for all but finitely many $v$. □

**Lemma 1.5.5.** *The map $\mathbb{I}_K \to \mathbb{R}_{>0}$ carrying $x$ to $|x|$, is an open homomorphism admitting continuous sections.*

*Proof.* The map is clearly a continuous homomorphism. The map $\mathbb{R}_{>0} \to K_\infty^\times \subseteq \mathbb{I}_K$ carrying $t$ to $(\sqrt[n]{t}, \dots, \sqrt[n]{t})$, where $n = [K\colon \mathbb{Q}]$, is a continuous section. For $v$ real (resp. complex), the map $\mathbb{R}_{>0} \to K_v^\times \subseteq \mathbb{I}_K$ carrying $t$ to $t$ (resp. $\sqrt{t}$) is also a continuous section. The openness follows from this. □

We let $\mathbb{I}_K^1$ denote the kernel of the homomorphism $|-|$ and equip it with the subspace topology induced from the topology of $\mathbb{I}_K$. We thus obtain an isomorphism of topological groups $\mathbb{I}_K/\mathbb{I}_K^1 \simeq \mathbb{R}_{>0}$. Moreover the continuous sections of $|-|$ (not unique for $n > 1$) induce isomorphisms of topological groups $\mathbb{I}_K \simeq \mathbb{I}_K^1 \times \mathbb{R}_{>0}$.

By product formula, the image of the diagonal embedding $K^\times \to \mathbb{I}_K$ is contained in $\mathbb{I}_K^1$.

**Theorem 1.5.6.** *The quotient $\mathbb{I}_K^1/K^\times$ is compact.*

**Lemma 1.5.7.** *Let $c > 1$. For all but finitely many $v \in V$, $|K_v^\times| \cap (1, c) = \emptyset$.*

*Proof.* Indeed, the equality holds for all $v \in V_f$ with residue field of cardinality $q \geq c$, and in particular, for $v \in V_f$ above a rational prime $p \geq c$. □

**Proposition 1.5.8.** *$\mathbb{I}_K^1 \subseteq \mathbb{A}_K$ is a closed subset and the topology on $\mathbb{I}_K^1$ coincides with the subspace topology induced from $\mathbb{A}_K$.*

*Proof.* For $x \in \mathbb{A}_K$, consider the neighborhood $U_{S,\epsilon}(x) \subseteq \mathbb{A}_K$, set of adèles $y$ such that $|y_v - x_v|_v \leq \epsilon$ for $v \in S$ and $|y_v|_v \leq 1$ for $v \in V - S$. Here $\epsilon > 0$ and $S \subseteq V$ is a finite subset containing $V_\infty$ and such that $|x_v|_v \leq 1$ for all $v \in V - S$.

For the first assertion, we need to show that for $x \notin \mathbb{I}_K^1$, there exists such a neighborhood that does not meet $\mathbb{I}_K^1$. There are two cases.

(1) $|x| < 1$ (may be zero). Then there exists $S$ satisfying the above and such that $\prod_{v\in S}|x_v|_v < 1$. It then suffices to take $\epsilon$ sufficiently small such that for $y \in U_{S,\epsilon}(x)$, we have $|y| = \prod_{v\in S}|y_v|_v < 1$.
(2) $|x| > 1$. By Lemma 1.5.4, $x \in \mathbb{I}_K$. By Lemma 1.5.7, there exists a finite subset $S \subseteq V$ containing $V_\infty$ such that $|x_v|_v = 1$ for $v \in V - S$ and such that $|K_v^\times|_v \cap (\frac{1}{2|x|}, 1) = \emptyset$ for $v \in V - S$. It then suffices to take $\epsilon$ sufficiently small such that for $y \in U_{S,\epsilon}(x)$, we have $1 < \prod_{v\in S}|y_v|_v < 2\prod_{v\in S}|x_v|_v = 2|x|$. It follows that either $|y| = \prod_{v\in S}|y_v|_v > 1$, or $|y| \leq \frac{1}{2}\prod_{v\in S}|y_v|_v < 1$.

The topology on $\mathbb{I}_K^1$ is clearly finer than the topology induced from $\mathbb{A}_K$. To show the converse, let $x \in \mathbb{I}_K^1$ and let $W$ be a neighborhood of $x$ in $\mathbb{I}_K$. We need to find a neighborhood $U$ of $x$ in $\mathbb{A}_K$ such that $U \cap \mathbb{I}_K^1 \subseteq W \cap \mathbb{I}_K^1$. We may assume that $W$ is the set of idèles $y$ such that $|y_v - x_v|_v < \epsilon$ for $v \in S$ and $|y_v|_v = 1$ for $v \in V - S$, where $S \subseteq V$ is a finite subset containing $V_\infty$ and such that $|x_v|_v = 1$ for $v \in V - S$. We may further assume that $\epsilon$ is sufficiently small such that for $z \in U_{S,\epsilon}(x)$, we have $\prod_{v\in S}|z_v|_v < 2\prod_{v\in S}|x_v|_v = 2$. If, moreover, $|z| = 1$, then $|z_v|_v > 1/2$ for all $v \in V_f - S$, so that $|z_v|_v = 1$ for such $v$. Thus $U_{S,\epsilon}(x) \cap \mathbb{I}_K^1 = V \cap \mathbb{I}_K^1$. □

*Proof of Theorem 1.5.6.* By the proposition, it suffices to find a compact $B \subseteq \mathbb{A}_K$ such that the map $B \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$ is surjective. By Theorem 1.4.32, there exists a constant $C$ such that for every idèle $x \in \mathbb{I}_K$ satisfying $|x| > C$, there exists $a \in K^\times$ such that $|a|_v \leq |x_v|_v$ for all $v \in V$. Choose such an $x$ and let $B$ be the set of adèles $y$ such that $|y_v|_v \leq |x_v|_v$ for all $v \in V$. Let $z \in \mathbb{I}_K^1$. Then $|z^{-1}x| > C$, so that there exists $a \in K^\times$ such that $|a|_v \leq |z_v^{-1}x_v|_v$ for all $v \in V$. Thus $z = a^{-1}(az)$, with $az \in B \cap \mathbb{I}_K^1$, as required. □

## Idèles and ideals

Recall that every fractional ideal of $\mathcal{O}_K$ can be uniquely factorized as a finite product $\prod_i \mathfrak{p}_i^{m_i}$, where the $\mathfrak{p}_i$ are distinct maximal ideals of $\mathcal{O}_K$. Fractional ideals of $\mathcal{O}_K$ form a free abelian group $\mathcal{I}_K$ with basis given by the set of maximal ideals of $\mathcal{O}_K$. We let $\mathcal{P}_K$ denote the set of principal fractional ideals of $\mathcal{O}_K$, namely, fractional ideals of the form $x\mathcal{O}_K$, where $x \in K^\times$. We let $\mathcal{C}l_K = \mathcal{I}_K/\mathcal{P}_K$ denote the ideal class group of $K$.

For every idèle $(x_v)_{v\in V} \in \mathbb{I}_K$, $m_v = v(x_v)$ equals 0 for all but finitely many $v \in V_f$, so that $\prod_{v\in V_f} \mathfrak{p}_v^{m_v}$ is a fractional ideal. Here $\mathfrak{p}_v$ denotes the maximal ideal corresponding to $v$. This defines a homomorphism $\mathbb{I}_K \to \mathcal{I}_K$, which is clearly surjective, and the kernel is an open subgroup $U_K = K_\infty^\times \times \prod_{v\in V_f} \mathcal{O}_v^\times \subseteq \mathbb{I}_K$. Thus we get an isomorphism

$$\mathbb{I}_K/U_K \simeq \mathcal{I}_K,$$

which induces an isomorphism

$$\mathbb{I}_K/K^\times U_K \simeq \mathcal{C}l_K.$$

Restricting to idèles of content 1, we get

$$\mathbb{I}_K^1/K^\times U_K^1 \simeq \mathcal{C}l_K,$$

where $U_K^1 = U_K \cap \mathbb{I}_K^1 = K_\infty^1 \times \prod_{v\in V_f} \mathcal{O}_v^\times$, and $K_\infty^1$ is the kernel of the homomorphism $K_\infty^\times \to \mathbb{R}_{>0}^\times$ carrying $(x_v)_{v\in V_\infty}$ to $\prod_{v\in V_\infty} |x_v|_v$. Here we have used $\mathbb{I}_K^1 U_K = \mathbb{I}_K$.

**Theorem 1.5.9.** *The ideal class group $\mathcal{C}l_K$ of any number field is a finite abelian group.*

*Proof.* Since $U_K^1$ is an open subgroup of $\mathbb{I}_K^1$, the quotient is discrete. Since $\mathbb{I}_K^1/K^\times$ is compact (Theorem 1.5.6), $\mathbb{I}_K^1/K^\times U_K^1$ is also compact, hence finite. □

The theorem holds more generally for ray class groups, defined as follows.

**Definition 1.5.10.** A *modulus* for $K$ is a function $m \colon V \to \mathbb{N}$ carrying $v$ to $m_v$ satisfying the following conditions:

- $m_v = 0$ for $v$ complex.
- $m_v = 0$ or 1 for $v$ real.
- $m_v = 0$ for all but finitely many $v$.

We can identify moduli with pairs $(I,(m_v)_{v\in V_\mathbb{R}})$, where $I=\prod_{v\in V_f}\mathfrak{p}_v^{m_v}$ is an ideal of $\mathcal{O}_K$. Here $V_\mathbb{R}$ denotes the set of real places of $K$.

For a modulus $m$, we let $\mathcal{I}_K(m)\subseteq\mathcal{I}_K$ denote the subgroup of fractional ideals generated by $\mathfrak{p}_v$ with $m_v=0$. We let $\mathcal{P}_K(m)\subseteq\mathcal{P}_K$ denote the group of principal fractional ideals $x\mathcal{O}_K$, $x\in K^\times$ such that $v(x-1)\geq m_v$ for $v\in V_f$ with $m_v>0$ and $\sigma_v(x)>0$ for real places $v$ with $m_v=1$. Here $\sigma_v$ denotes the embedding $K\to\mathbb{R}$ corresponding to $v\in V_\mathbb{R}$.

**Definition 1.5.11.** The *ray class group* of $K$ for $m$ is $\mathcal{C}l_K(m)=\mathcal{I}_K(m)/\mathcal{P}_K(m)$.

**Example 1.5.12.** If $m$ is constant of value 0, then $\mathcal{C}l_K(m)=\mathcal{C}l_K$.

**Example 1.5.13.** If $m$ is the characteristic function of $V_\mathbb{R}$, then $\mathcal{P}_K(m)=\mathcal{P}_K^+$ is the set of principal fractional ideals generated by totally positive elements, namely $x\in K^\times$ such that $\sigma(x)>0$ for all real embeddings $\sigma\colon K\to\mathbb{R}$. In this case, $\mathcal{C}l_K(m)=\mathcal{I}_K/\mathcal{P}_K^+$ is called the *narrow class group* of $K$.

**Example 1.5.14.** Let $n>1$ be an integer. Then $m=((n),1)$ is a modulus for $K=\mathbb{Q}$. In other words, $m_p=v_p(n)$ and $m_\infty=1$. The map $\mathcal{I}_\mathbb{Q}(m)\to(\mathbb{Z}/n\mathbb{Z})^\times$ carrying $\frac{a}{b}\mathbb{Z}$, $a,b\in\mathbb{N}_{>0}$, $(a,n)=(b,n)=1$, to $\bar{a}/\bar{b}$, where $\bar{a}$ and $\bar{b}$ denote the images of $a$ and $b$ in $\mathbb{Z}/n\mathbb{Z}$, respectively, induces an isomorphism $\mathcal{C}l_\mathbb{Q}(m)\simeq(\mathbb{Z}/n\mathbb{Z})^\times$.

For a modulus $m$ of $K$, we let $\mathbb{I}_{K,m}\subseteq\mathbb{I}_K$ denote the open subgroup of idèles $(x_v)_{v\in V}$ such that $v(x_v-1)\geq m_v$ for $v\in V_f$ with $m_v\geq 1$ and $x_v>0$ for $v\in V_\mathbb{R}$ with $m_v=1$. Note that $\mathcal{P}_K(m)$ is the group of principal fractional ideals $x\mathcal{O}_K$, $x\in\mathbb{I}_{K,m}\cap K^\times$. The homomorphism $\mathbb{I}_{K,m}\to\mathcal{I}_K(m)$ carrying $(x_v)_{v\in V}$ to $\prod_{v\in V_f}\mathfrak{p}_v^{m_v}$ is surjective, and the kernel is $U_{K,m}=U_K\cap\mathbb{I}_{K,m}$. In other words $U_{F,m}=\prod_v U_v^{(m_v)}$, where $U_v^{(0)}=F_v^\times$ for $v$ Archimedean, $U_v^{(1)}=\mathbb{R}_{>0}^\times$ for $v$ real, $U_v^{(0)}=U_v=\mathcal{O}_v^\times$ for $v$ finite, and $U_v^{(n)}=1+\pi_v^n\mathcal{O}_v$ for $v$ finite and $n\geq 1$. We get an isomorphism

$$\mathbb{I}_{K,m}/U_{K,m}\simeq\mathcal{I}_K(m),$$

which induces an isomorphism

$$\mathbb{I}_K/K^\times U_{K,m}\simeq\mathbb{I}_{K,m}/(\mathbb{I}_{K,m}\cap K^\times)U_{K,m}\simeq\mathcal{C}l_K(m). \tag{1.5.1}$$

Here we have used the equality $K^\times\mathbb{I}_{K,m}=\mathbb{I}_K$, which follows from the approximation theorem. Restricting to idèles of content 1, we get an isomorphism

$$\mathbb{I}_K^1/K^\times U_{K,m}^1\simeq\mathcal{C}l_K(m),$$

where $U_{K,m}^1=U_{K,m}\cap\mathbb{I}_K^1$. By the compactness of $\mathbb{I}_K^1/K^\times$, we get the following.

**Theorem 1.5.15.** *The ray class group $\mathcal{C}l_K(m)$ of any number field $K$ for any modulus $m$ is a finite abelian group.*

## Dirichlet unit theorem

We let $\mu_K$ denote the group of roots of unity of $K$.

**Lemma 1.5.16.** *Let $C = \prod_{v\in V} C_v \subseteq \mathbb{I}_K$, where $C_v = \{x \in K_v^\times \mid |x|_v = 1\}$. Then $\mu_K = K^\times \cap C$ is a finite cyclic group.*

*Proof.* It is clear that $\mu_K \subseteq K^\times \cap C$. Since $C \subseteq \mathbb{I}_K$ is compact and $K^\times \subseteq \mathbb{I}_K$ is discrete, $K^\times \cap C$ is finite. Thus every element of $K^\times \cap C$ has finite order, so that $K^\times \cap C \subseteq \mu_K$. We have shown that $\mu_K = K^\times \cap C$ is a finite group. Since there are at most $n$ roots of unity of order $n$, the exponent of $\mu_K$ is necessarily equal to the order of $\mu_K$, so that $\mu_K$ is a finite cyclic group. □

We refer the reader to [T2, Lemma 4.2.1] for a proof without using idèles.

**Definition 1.5.17.** Let $S \subset V$ be a finite set of places of $K$ containing $V_\infty$. We say that $x \in K$ is an *$S$-integer* (resp. *$S$-unit*) if $|x|_v \leq 1$ (resp. $|x|_v = 1$) for all $v \in V - S$. We let $\mathcal{O}_{K,S}$ denote the ring of $S$-integers of $K$. The group $\mathcal{O}_{K,S}^\times$ is the group of $S$-units of $K$.

**Theorem 1.5.18.** *We have $\mathcal{O}_{K,S}^\times = \mu_K \times L$, where $L$ is a free Abelian group of rank $\#S - 1$.*

Since $\mathcal{O}_K^\times = \mathcal{O}_{K,V_\infty}^\times$, we obtain the following.

**Corollary 1.5.19.** *We have $\mathcal{O}_K^\times = \mu_K \times L$, where $L$ is a free Abelian group of rank $r_1 + r_2 - 1$, $r_1$ and $r_2$ being the number of real and complex places of $K$, respectively.*

Let $\mathbb{A}_{K,S} = \prod_{v\in S} K_v \times \prod_{v\in V-S} \mathcal{O}_v$, $\mathbb{I}_{K,S} = \mathbb{A}_{K,S}^\times = \prod_{v\in S} K_v^\times \times \prod_{v\in V-S} \mathcal{O}_v^\times$. Recall that $\mathbb{A}_{K,S}$ is an open subring of $\mathbb{A}_K$ and $\mathbb{I}_{K,S}$ is an open subgroup of $\mathbb{I}_K$. We have $\mathcal{O}_{K,S} = K \cap \mathbb{A}_{K,S}$, $\mathcal{O}_{K,S}^\times = K^\times \cap \mathbb{I}_{K,S}$.

*Proof of Theorem 1.5.18.* Consider the continuous homomorphism $\lambda\colon \mathbb{I}_{K,S} \to \mathbb{R}^S$ carrying $(x_v)_{v\in V}$ to $(\log|x_v|_v)_{v\in S}$. We have $\operatorname{Ker}(\lambda) = C$, $\lambda(\mathbb{I}_{K,S}) = \mathbb{R}^{V_\infty} \times \prod_{v\in V_f} \log(q_v)\mathbb{Z}$, and $\lambda$ induces an isomorphism of topological groups $\mathbb{I}_{K,S}/C \simeq \lambda(\mathbb{I}_{K,S})$. Let $\mathbb{I}_{K,S}^1 = \mathbb{I}_{K,S} \cap \mathbb{I}_K^1$. Then $\lambda(\mathbb{I}_{K,S}^1) = \lambda(\mathbb{I}_{K,S}) \cap H$, where $H$ is the kernel of the map $\mathbb{R}^S \to \mathbb{R}$ carrying $(x_v)_{v\in S}$ to $\sum_{v\in S} x_v$. Note that $H$ is a Euclidean space of dimension $\#S - 1$. Moreover $\lambda(\mathcal{O}_{K,S}^\times)$ is discrete by the properness of $\lambda$. Indeed, $\lambda^{-1}([\frac{1}{2}, 2]^S)$ is compact, hence has finite intersection with the discrete subgroup $\mathcal{O}_{K,S}^\times$ of $\mathbb{I}_{K,S}$. Now $\mu_K = \mathbb{I}_{K,S} \cap \mathcal{O}_{K,S}^\times$, so $L = \lambda(\mathcal{O}_{K,S}^\times) \simeq \mathcal{O}_{K,S}^\times/\mu_K$. We get a short exact sequence

$$1 \to C/\mu_K \to \mathbb{I}_{K,S}^1/\mathcal{O}_{K,S}^\times \to \lambda(\mathbb{I}_{K,S}^1)/L \to 0.$$

Note that $\mathbb{I}_{K,S}^1/\mathcal{O}_{K,S}^\times = \mathbb{I}_{K,S}^1/K^\times \cap \mathbb{I}_{K,S}^1$ is isomorphic to an open subgroup of $\mathbb{I}_K^1/K^\times$, hence is compact. It follows that $\lambda(\mathbb{I}_{K,S}^1)/L$ is compact. Since $H/\lambda(\mathbb{I}_{K,S}^1) \simeq \mathbb{R}^S/\lambda(\mathbb{I}_{K,S}^\times) \simeq (\mathbb{R}/\mathbb{Z})^{S-V_\infty}$ is compact, so is $H/L$. Therefore, $L$ is a lattice in $H$, hence a free Abelian group of rank $\#S - 1$. It follows that the extension $1 \to \mu_K \to \mathcal{O}_{K,S}^\times \to L \to 1$ splits. □

## Haar measures

Recall that for any Haar measure $dx$ on $K_v$, $dx/|x|_v$ is a Haar measure on $K_v^\times$. For $v \in V_f$, the volume of $\mathcal{O}_v^\times$ under $dx/|x|_v$ is $1 - \frac{1}{q_v}$ times the volume of $\mathcal{O}_v$ under $dx$. Note that $\prod_{v \in V_f}(1 - \frac{1}{q_v}) = 0$.

For $v \in V_f$, we take the Haar measure $\mu_{K_v^\times}$ normalized by $\mu_{K_v^\times}(\mathcal{O}_v^\times) = 1$. For $v \in V_\infty$, we take $\mu_{K_v^\times} = d^\times x = dx/|x|_v$, where $dx$ is the Haar measure on $K_v$ normalized as in Example 1.4.21. We obtain a Haar measure $\prod'_{v \in V} \mu_v$ on $\mathbb{I}_K$. This, combined with the Haar measure $dx/|x|$ on $\mathbb{R}_{>0}^\times$, induces a Haar measure $\mathbb{I}_K^1 = \operatorname{Ker}(\mathbb{I}_K \xrightarrow{|-|} \mathbb{R}_{>0}^\times)$. We equip $K^\times$ with the counting measure.

We equip $H = \operatorname{Ker}(\mathbb{R}^{V_\infty} \xrightarrow{\Sigma} \mathbb{R})$ with the Haar measure induced by the Lebesgue measures on $\mathbb{R}^{V_\infty}$ and $\mathbb{R}$. We have seen in the proof of the Dirichlet unit theorem that $L = \{(\log(x_v))_{v \in V_\infty} \mid x \in \mathcal{O}_K^\times\}$ is a lattice in $H$. We equip $L$ with the counting measure.

**Definition 1.5.20.** The *regulator* $R$ of $K$ is the volume of $H/L$.

**Remark 1.5.21.** (1) The Haar measure on $H$ is $1/\sqrt{r+1}$ times the usual measure, where $r + 1 = \#V_\infty = r_1 + r_2$. It is also the measure induced via the isomorphism $H \subseteq \mathbb{R}^{V_\infty} \to \mathbb{R}^r$ given by any of the $r+1$ projections from the Lebesgue measure on $\mathbb{R}^r$.

(2) Let $(u_i)_{1 \le i \le r}$ be a basis of $\mathcal{O}_K^\times/\mu_K$. Consider the $r \times (r+1)$ matrix $M = (|u_i|_{v_j})$, where $v_1, \dots, v_{r+1}$ is an enumeration of $V_\infty$. Then $R$ is the absolute value of any $r \times r$ minor of $M$.

**Proposition 1.5.22.** *We have*

$$\operatorname{vol}(\mathbb{I}_K^1/K^\times) = 2^{r_1}(2\pi)^{r_2} hR/w,$$

*where $r_1$, $r_2$ are the number of real and complex places of $K$, respectively, $h$ is the class number of $K$, $R$ is the regulator of $K$, and $w$ is the number of roots of unity of $K$.*

*Proof.* We have exact sequences

$$\begin{gathered} 1 \to U_K^1/\mathcal{O}_K^\times \to \mathbb{I}_K^1/K^\times \to \mathcal{C}l_K \to 1, \\ 1 \to C/\mu_K \to U_K^1/\mathcal{O}_K^\times \to H/L \to 0. \end{gathered}$$

Thus

$$\begin{aligned} \operatorname{vol}(\mathbb{I}_K^1/K^\times) = \operatorname{vol}(U_K^1/\mathcal{O}_K^\times)\operatorname{vol}(\mathcal{C}l_K) &= \operatorname{vol}(C/\mu_K)\operatorname{vol}(H/L)\operatorname{vol}(\mathcal{C}l_K) \\ &= \operatorname{vol}(C)hR/w = \prod_{v \in V_\infty} \operatorname{vol}(C_v)hR/w. \end{aligned}$$

Consider the short exact sequence

$$1 \to C_v \to K_v^\times \xrightarrow{\log(|-|_v)} \mathbb{R} \to 0.$$

For $v$ real, $C_v = \{\pm 1\}$, $dx/|x| = \pm d\log|x|$ is compatible with the counting measure on $C_v$ and the Lebesgue measure on $\mathbb{R}$, so that $\mathrm{vol}(C_v) = 2$. For $v$ complex, $C_v = S^1$,

$$d^\times z = \frac{2dx \wedge dy}{|z|^2} = \frac{d(r^2)}{r^2} \wedge d\theta = d\log(r^2) \wedge d\theta$$

for $z = x + iy = re^{i\theta}$, compatible with the measure $d\theta$ on $C_v$ and the Lebesgue measure on $\mathbb{R}$, so that $\mathrm{vol}(C_v) = 2\pi$. □

## 1.6 Appendix: Classification of local fields of characteristic 0

The goal of this section is to prove the following case of Theorem 1.2.28 (assuming the existence of a Haar measure on $K$).

**Theorem 1.6.1.** *A local field $K$ of characteristic $0$ is isomorphic to either $\mathbb{R}$, $\mathbb{C}$, or a finite extension of $\mathbb{Q}_p$.*

### Generalized absolute values

Let $|-|$ be an absolute value on a field $K$. For $0 < r \leq 1$, $|-|^r$ is an absolute value. However, for $r > 1$, $|-|^r$ does not satisfy the triangle inequality in general. For example, the normalized absolute value $|-|_{\mathbb{C}}$ does not satisfy the triangle inequality.

**Definition 1.6.2.** A *generalized absolute value* on a field $K$ is a homomorphism $f\colon K^\times \to \mathbb{R}^\times_{>0}$, extended by $f(0) = 0$, satisfying the inequality $(U_C)$:

$$f(x+y) \leq C\max\{f(x), f(y)\},$$

$x, y \in K$, for some constant $C > 0$.

Taking $x = 1$, $y = 0$, we get $C \geq 1$. For $C = 1$, $(U_1)$ is the ultrametric inequality. If $f$ is a generalized absolute value satisfying $(U_C)$, then $f^r$ is a generalized absolute value satisfying $(U_{C^r})$.

**Proposition 1.6.3.** *Let $f\colon K^\times \to \mathbb{R}^\times_{>0}$ be a homomorphism extended by $f(0) = 0$. Then $f$ is a generalized absolute value on $K$ if and only if $f(1+x)$ is bounded on the set $B_{\leq 1} = \{x \in K \mid f(x) \leq 1\}$. More precisely, $f$ satisfies $(U_C)$ if and only if $f(1+x) \leq C$ for all $x \in B_{\leq 1}$.*

*Proof.* Taking $y = 1$ in $(U_C)$, we get $f(1+x) \leq C\max\{f(1), f(x)\} \leq C$ for $x \in B_{\leq 1}$. Conversely, assume $f(1+x) \leq C$ for all $x \in B_{\leq 1}$. To show $(U_C)$, we may assume $f(x) \leq f(y)$, and $y \neq 0$, so that $f(x+y) = f(y)f(1+\frac{x}{y}) \leq Cf(y) = C\max\{f(x), f(y)\}$. □

**Proposition 1.6.4.** *Let $f\colon K^\times \to \mathbb{R}^\times_{>0}$ be a homomorphism extended by $f(0) = 0$. The following conditions are equivalent.*

*(1) $f$ is an absolute value on $K$.*

*(2) $f$ satisfies $(U_2)$.*

*(3) $f$ is a generalized absolute value on $K$ and there exists a constant $A$ such that $f(n \cdot 1) \leq An$ for all $n \in \mathbb{N}$.*

*Proof.* (1) $\Rightarrow$ (2). Indeed, $f(x+y) \leq f(x) + f(y) \leq 2\max\{f(x), f(y)\}$.

(2) $\Rightarrow$ (3). By induction, $(U_2)$ implies $f(x_1 + \cdots + x_{2^m}) \leq 2^m \max_{1\leq i \leq 2^m}\{f(x_i)\}$. For $n > 0$, let $m$ be the smallest integer such that $2^m \geq n$. Then $f(n\cdot 1) \leq 2^m < 2n$.

(3) $\Rightarrow$ (1). By induction, $(U_C)$ implies $f(x_1 + \cdots + x_{2^m}) \leq C^m \max_{frm[o]--lei\leq 2^m}\{f(x_i)\}$. Let $n = 2^m - 1$. Then

$$\begin{aligned} f(x+y)^n = f((x+y)^n) = f\left(\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}\right) &\leq C^m \max_{0\leq i\leq n}\left\{f\left(\binom{n}{i}x^i y^{n-i}\right)\right\} \\ &\leq AC^m \sum_{i=0}^{n}\binom{n}{i} f(x)^i f(y)^{n-i} = AC^m (f(x)+f(y))^n, \end{aligned}$$

so that $f(x+y) \leq \sqrt[n]{AC^m}(f(x)+f(y))$. Let $m \to +\infty$. We get $\leq f(x) + f(y)$. □

**Corollary 1.6.5.** *Every generalized absolute value $f$ on $K$ has the form $f(x) = |x|^r$, where $|-|$ is an absolute value on $K$ and $r > 0$.*

*Proof.* Indeed, for $s > 0$ sufficiently small, $f^s$ satisfies $(U_2)$, hence is an absolute value by the proposition. □

## Modulus of a local field

Let $K$ be a local field. For the moment we make no assumption on the characteristic of $K$. Let $\mathrm{mod}\colon K \to \mathbb{R}_{\geq 0}$ be the modulus of $K$. By definition, for any Haar measure $\mu$ on $K$, any measurable set $E \subseteq K$, and any $a \in K$, $\mu(aE) = \mathrm{mod}(a)\mu(E)$ (here $0 \cdot \infty = 0$). The function mod induces a group homomorphism $K^\times \to \mathbb{R}^\times_{>0}$.

**Proposition 1.6.6.** *The function* $\mathrm{mod}\colon K \to \mathbb{R}_{\geq 0}$ *is continuous.*

*Proof.* Let $V$ be a compact neighborhood of 0 in $K$. Then $\mu(V) \in \mathbb{R}_{>0}$. Let $a \in K$. By the outer regularity of $\mu$, for any $\epsilon > 0$, there exists an open subset $U \supseteq aV$ such that $\mu(U) \leq \mu(aV) + \epsilon$. By the continuity of multiplication in $K$, there exists a neighborhood $W$ of $a$ such that $WV \subseteq U$. For $x \in W$, $\mu(xV) \leq \mu(U) \leq \mu(aV) + \epsilon$. Thus $\mathrm{mod}(x) \leq \mathrm{mod}(a) + \epsilon/\mu(V)$. This inequality shows that mod is upper continuous, hence continuous at 0. For $a \in K^\times$, $\mathrm{mod}(a) = 1/\mathrm{mod}(1/a)$. It follows that mod is also lower continuous at any $a \in K^\times$. □

**Proposition 1.6.7.** *For $r \geq 0$, $B_{\leq r} = \{x \in K \mid \mathrm{mod}(x) \leq r\}$ is compact.*

Let $V$ be a compact neighborhood of 0 in $K$. By the continuity of mod, $B_{\leq r}$ is closed in $K$, so it suffices to show that $B_{\leq r}$ is contained in a compact set of the form $aV$, $a \in K$.

**Lemma 1.6.8.** *There exists $\pi \in K^\times$ such that $\pi^n \to 0$ as $n \to +\infty$ and $\pi V \subseteq V$.*

*Proof.* Since $0 \cdot V \subseteq V$, there exists a neighborhood $U$ of $0$ such that $UV \subseteq V$. By the continuity of mod, since $K$ is not discrete, there exists $\pi \in U \cap V$ such that $0 < \mathrm{mod}(\pi) < 1$. Thus $\pi V \subseteq V$. By induction, $\pi^n V \subseteq V$ for $n \geq 0$, so that $\pi^n \in \pi^{n-1}V \subseteq V$ for $n \geq 1$. Since $V$ is compact, the sequence $\pi^n$ has a cluster point. For any cluster point $x$ of the sequence, $\mathrm{mod}(x)$ is a cluster point of $\mathrm{mod}(\pi^n) = \mathrm{mod}(\pi)^n$ by the continuity of mod, hence $\mathrm{mod}(x) = 0$, which implies $x = 0$. Thus $0$ is the only cluster point of $\pi^n$. In other words, $\pi^n \to 0$ as $n \to +\infty$. □

*Proof of Proposition 1.6.7.* Let $\pi$ be as in the lemma. Let $X$ be the closure of $V - \pi V$ in $K$. We have $0 \notin X$, so that $\rho = \min_{x \in X}\{\mathrm{mod}(x)\} > 0$. Choose $N \geq 0$ such that $\mathrm{mod}(\pi)^N r \leq \rho$. We claim that $B_{\leq r} \subseteq \pi^{-N}V$. To see this, let $a \in B_{\leq r}$. To show $a \in \pi^{-N}V$, we may assume $a \notin V$. Since $\pi^n a \to 0$, there exists $n \geq 1$ such that $\pi^n a \in V$, but $\pi^{n-1}a \notin V$. In other words, $\pi^n a \in V - \pi V$. Thus

$$\mathrm{mod}(\pi)^N r \leq \rho \leq \mathrm{mod}(\pi^n a) \leq \mathrm{mod}(\pi)^n r,$$

so that $n \leq N$. Thus $a \in \pi^{-n}V \subseteq \pi^{-N}V$. □

**Corollary 1.6.9.** *The subsets $B_{\leq r} \subseteq K$, $r > 0$ form a fundamental system of neighborhoods of $0$ in $K$. In particular, for $a \in K$, $a^n \to 0$ as $n \to +\infty$ if and only if $\mathrm{mod}(a) < 1$.*

*Proof.* Let $V$ be any neighborhood of $0$ in $K$. We show that $B_{\leq r} \subseteq V$ for some $r > 0$. We may assume that $V$ does not contain $B_{\leq R}$ for some $R > 0$. Let $X$ be the closure of $B_{\leq R}\backslash V$ in $K$. We have $0 \notin X$, so that $\rho = \min_{x \in X}\{\mathrm{mod}(x)\} > 0$. For $0 < r < \rho$, $B_{\leq r} \subseteq V$. □

**Corollary 1.6.10.** *Any discrete subfield $F$ of $K$ is finite.*

*Proof.* For any $a \in F^\times$, as $a^{-n} \not\to 0$, we have $\mathrm{mod}(a) \leq 1$. Thus $F \subseteq B_{\leq 1}$ is compact and discrete, hence finite. □

*Proof of Theorem 1.6.1.* By Propositions 1.6.6 and 1.6.7, $x \mapsto \mathrm{mod}(1+x)$ is bounded on $B_{\leq 1}$. By Proposition 1.6.3, mod is a generalized absolute value. By Corollary 1.6.5, we obtain an absolute value on $K$, which defines the topology on $K$ by Corollary 1.6.9. By Corollary 1.6.10, the restriction of this absolute value to $\mathbb{Q}$ is nontrivial, thus is equivalent to either $|-|_\infty$ or $|-|_p$. Thus there exists an absolute value on $K$ extending $|-|_\infty$ or $|-|_p$. Since $K$ is complete, $K$ as a valued field contains either $\mathbb{R}$ or $\mathbb{Q}_p$. We conclude by the following. □

**Proposition 1.6.11.** *Let $W$ be a locally compact normed vector space over a complete valued field $K$ with nontrivial absolute value $|-|$. Then the dimension of $W$ is finite.*

*Proof.* Let $V$ be a compact neighborhood of $0$ in $W$. Let $\pi \in K$ with $0 < |\pi| < 1$. Then there exist $x_1, \dots, x_n \in W$ such that $V \subseteq \bigcup(x_i + \pi V)$. Let $L = \sum K x_i \subseteq W$. Then $L$ is a finite-dimensional $K$-vector subspace of $W$, hence complete (Lemma 1.2.20), therefore closed. Let $A$ be the image of $V$ in $W/L$, which is a compact neighborhood of $0$ in $W/L$. We have $A \subseteq \pi A$. For any $y \in W/L$, $\pi^n y \to 0$ as $n \to +\infty$. Thus $W/L \subseteq \bigcup \pi^{-n}A = A$, so that $W/L = A$ is compact. Note that $K$ is not compact, so that $W/L$ must be zero. It follows that $W = L$. □

One can show using Haar measures that any locally compact Hausdorff topological vector space over a local field is finite-dimensional [W, Section I.2, Corollary 2 to Theorem 3].

# Chapter 2

# Tate's thesis

## 2.1 Pontryagin duality

Let $G$ be a topological abelian group. We write the group law multiplicatively.

**Definition 2.1.1.** A *unitary character* of $G$ is a continuous homomorphism $G \to S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. The *Pontryagin dual* of $G$ is the abelian group $\hat{G}$ of unitary characters of $G$ with multiplication defined by $(\chi\chi')(x) = \chi(x)\chi'(x)$, equipped with the *compact-open topology* (also known as topology of compact convergence): A base of the topology is given by $W(K,U) = \{\chi \in \hat{G} \mid \chi(K) \subseteq U\}$, $K \subseteq G$ compact, $U \subseteq S^1$ open.

The compact-open topology is finer than the topology of pointwise convergence (namely, the weakest topology such that for all $x \in G$, the function $\chi \mapsto \chi(x)$ is continuous on $\hat{G}$). A fundamental system of neighborhoods of $1 \in \hat{G}$ is given by $W(K,U) = \{\chi \in \hat{G} \mid \chi(K) \subseteq U\}$, $K \subset G$ compact and $U$ running through neighborhoods of $1 \in S^1$. To analyze the topology of $\hat{G}$, we consider the open neighborhood $N(\epsilon) = e((-\frac{\epsilon}{3}, \frac{\epsilon}{3})) \subseteq S^1$ of 1, for $0 < \epsilon \leq 1$. Here $e(x) = \exp(2\pi i x)$. Note that $N(1)$ does not contain any nontrivial subgroup of $S^1$. We have the following refinement.

**Lemma 2.1.2.** *Let $m \geq 1$ be an integer and let $0 < \epsilon \leq 1$. If $x \in S^1$ is such that $x, x^2, \dots, x^m \in N(\epsilon)$, then $x \in N(\epsilon/m)$.*

It follows that for any subset $X \subseteq G$ containing $1 \in G$ and any homomorphism $\chi\colon G \to S^1$, not necessarily continuous, such that $\chi(X^{(m)}) \subseteq N(\epsilon)$, we have $\chi(X) \subseteq N(\epsilon/m)$. Here $X^{(m)} = \{x_1 \cdots x_m \mid x_1, \dots, x_m \in X\} \subseteq G$.

*Proof.* We proceed by induction. The case $m = 1$ is trivial. For $m \geq 2$, we have $x \in N(\epsilon/(m-1))$ by induction hypothesis, so that $x = e(\alpha)$, $|\alpha| < \frac{\epsilon}{3(m-1)}$. Since $x^m \in N(\epsilon)$, we have $m\alpha \in (-\frac{\epsilon}{3} + r, \frac{\epsilon}{3} + r)$ for an integer $r$. In particular, $-\frac{\epsilon}{3} + r < m\alpha < m\frac{\epsilon}{3(m-1)}$, so that $r < \frac{2m-1}{3(m-1)} \leq 1$. Similarly, $r > -1$. Thus $r = 0$, $\alpha \in (-\frac{\epsilon}{3m}, \frac{\epsilon}{3m})$, and $x \in N(1/m)$. □

**Proposition 2.1.3.** *A group homomorphism $\chi\colon G \to S^1$ is continuous if and only if $\chi^{-1}(N(1))$ is a neighborhood of $1 \in G$.*

*Proof.* The "only if" part is trivial. Conversely, if $\chi^{-1}(N(1))$ is a neighborhood of $1 \in G$, then for any integer $m \geq 1$, there exists a neighborhood $U$ of $1 \in G$ such that $U^{(m)} \subseteq \chi^{-1}(N(1))$, so that $\chi(U) \subseteq N(1/m)$ by the lemma. □

**Proposition 2.1.4.** *A fundamental system of neighborhoods of* $1 \in \hat{G}$ *is given by* $W(K, N(1))$, $K \subseteq G$ *compact.*

*Proof.* It suffices to show that for every $K$ and $m \geq 1$, $W(K', N(1)) \subseteq W(K, N(1/m))$ for some compact subset $K' \subseteq G$. We may assume $1 \in K$. By the lemma, we may take $K' = K^{(m)}$. □

**Proposition 2.1.5.** *(1)* $\hat{G}$ *is Hausdorff.*

*(2) If* $G$ *is discrete, then* $\hat{G}$ *is compact.*

*(3) If* $G$ *is compact, then* $\hat{G}$ *is discrete.*

*(4) If* $G$ *is locally compact, then* $\hat{G}$ *is locally compact.*

*Proof.* (1) Indeed, $\{1\} = \bigcap_{g\in G} g^{\perp}$, where $g^{\perp} = \{\chi \in \hat{G} \mid \chi(g) = 1\}$ is closed in $\hat{G}$.

(2) $\hat{G}$ is a closed subgroup of the compact group $(S^1)^G = \prod_{g\in G} S^1$. Indeed, $\hat{G} = \bigcap_{g,h\in G} V_{g,h}$, where $V_{g,h} = \{\chi\colon G \to S^1 \mid \chi(g)\chi(h) = \chi(gh)\} \subseteq (S^1)^G$ is closed.

(3) For any $\chi \in W(G, N(1))$, $\chi(G) \subseteq N(1)$ is a subgroup of $N(1)$, hence $\chi(G) = \{1\}$. Thus $W(G, N(1)) = \{1\}$.

(4) Let $V$ be a compact neighborhood of $1 \in G$. We show that $W = W(V, \overline{N(1/3)})$ is a compact neighborhood of $1 \in \hat{G}$. Here the bar denotes closure. Clearly $W \supseteq W(V, N(1/3))$ is a neighborhood of $1 \in \hat{G}$. Let $G_0$ be $G$ equipped with the discrete topology. Then $\hat{G} \subseteq \hat{G}_0$. The latter is compact by (2). Let $W_0 = \{\chi \in \hat{G}_0 \mid \chi(V) \subseteq \overline{N(1/3)}\}$, so that $W = W_0 \cap \hat{G}$. Note that every $\chi \in W_0$ is continuous on $G$ by Proposition 2.1.3, so that $W = W_0$. As $W_0$ is closed in $\hat{G}_0$, $W_0$ is compact for the topology $\tau_0$ induced from $\hat{G}_0$. The topology $\tau$ on $W$ induced from $\hat{G}$ is finer than $\tau_0$, and it suffices to show the converse. For $\chi \in W$ and $K \subseteq G$ compact, let $X = (\chi W(K, N(1))) \cap W$. By Proposition 2.1.4, it suffices to show that $X$ is a $\tau_0$-neighborhood of $\chi$. By the compactness of $K$, there exists a finite subset $F \subseteq G$ such that $K \subseteq FV$. Then $X_0 = (\chi W(F, N(1/3))) \cap W$ is a $\tau_0$-neighborhood of $\chi$, and it suffices to show that $X_0 \subseteq X$. Let $\chi_0 \in X_0$. Then $\chi_0 = \chi\mu$ for some $\mu \in \hat{G}_0$ such that $\mu(F) \subseteq N(1/3)$. Since $\mu = \chi^{-1}\chi_0 \in W^{(2)}$, $\mu(V) \subseteq \overline{N(2/3)}$. By Proposition 2.1.3, $\mu$ is continuous on $G$. Moreover, $\mu(K) \subseteq \mu(F)\mu(V) \subseteq N(1/3)\overline{N(2/3)} = N(1)$. Thus $\mu \in X$.

□

We say that an element $a$ of an abelian group $A$ is *divisible*, if for each integer $n \geq 1$, $nx = a$ admits a solution in $A$. We say that $A$ is *divisible*, if every $a \in A$ is divisible.

**Remark 2.1.6.** If $G$ is divisible, then $\hat{G}$ is torsion-free. Indeed, if $\chi \in \hat{G}[n]$, then $\chi(G) \subseteq S^1[n]$ is divisible, so that $\chi = 1$.

Let $f\colon G \to G'$ be a continuous homomorphism of topological abelian groups. Composition with $f$ induces a continuous homomorphism $\hat{f}\colon \hat{G}' \to \hat{G}$. Indeed, $\hat{f}^{-1}(W(K, U)) = W(f(K), U)$. For a sequence $G \xrightarrow{f} G' \xrightarrow{f'} G''$ of continuous homomorphisms, $(f' \circ f)\hat{} = \hat{f} \circ \hat{f}'$.

**Proposition 2.1.7.** *Let $H$ be a subgroup of $G$ and let $i\colon H \to G$ be the inclusion. Then*
$$H^\perp = \{\chi \in \hat{G} \mid \chi(H) = \{1\}\} = \operatorname{Ker}(\hat{i}\colon \hat{G} \to \hat{H})$$
*is a closed subgroup of $\hat{G}$. Moreover, $\hat{p}$, where $p$ is the quotient map $p\colon G \to G/H$, induces a continuous isomorphism $(G/H)^\wedge \xrightarrow{\sim} H^\perp$, which is an isomorphism of topological groups if $G$ is locally compact.*

*Proof.* For the first assertion is obvious. The map $(G/H)^\wedge \xrightarrow{\sim} H^\perp$ is clearly a continuous isomorphism. For every compact $K \subseteq G/H$, there exists a compact $K' \subseteq G$ such that $K \subseteq p(K')$. Thus the map is a homeomorphism. □

**Example 2.1.8.** The map $\mathbb{Z}^\wedge \to S^1$ carrying $\chi$ to $\chi(1)$ is an isomorphism of topological groups.

**Example 2.1.9.** For $n \geq 1$, the map $(\mathbb{Z}/n\mathbb{Z})^\wedge \to \mu_n = S^1[n]$ carrying $\chi$ to $\chi(1)$ is an isomorphism of topological groups. Choosing a primitive $n$-root of unity $\zeta_n \in S^1$, we obtain an isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\wedge$carrying $\xi$ to $x \mapsto \zeta_n^{\xi x}$. It follows that for every finite abelian group $G$, there exists a (noncanonical) isomorphism $G \simeq \hat{G}$.

Let $V$ be a finite-dimensional $\mathbb{F}_p$-vector space. Then we have an isomorphism $\operatorname{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p) = V^\vee \xrightarrow{\sim} V^\wedge$carrying $\phi$ to $x \mapsto \zeta_p^{\phi(x)}$. For $V = \mathbb{F}_q$, $q = p^f$, composing with the isomorphism $\mathbb{F}_q \xrightarrow{\sim} V^\vee$ carrying $\xi$ to $x \mapsto \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\xi x)$, we obtain an isomorphism $\mathbb{F}_q \to \mathbb{F}_q^\wedge$ carrying $\xi$ to $x \mapsto \zeta_p^{\operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\xi x)}$.

**Example 2.1.10.** Consider the isomorphisms $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} (p^{-n}\mathbb{Z}/\mathbb{Z})^\wedge$carrying $\xi$ to $x \mapsto e(\xi x)$, where $\xi x \in p^{-n}\mathbb{Z}/\mathbb{Z}$. For $m \leq n$, the isomorphisms are compatible with the projection $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ and the inclusion $p^{-m}\mathbb{Z}/\mathbb{Z} \subseteq p^{-n}\mathbb{Z}/\mathbb{Z}$ for $m \leq n$. Taking limit, we obtain an isomorphism of topological groups $\mathbb{Z}_p \xrightarrow{\sim} (\mathbb{Q}_p/\mathbb{Z}_p)^\wedge$ carrying $\xi$ to $x \mapsto e(\xi x)$, where $\xi x \in \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathbb{Q}/\mathbb{Z} \subseteq \mathbb{R}/\mathbb{Z}$. Note that $\mathbb{Q}_p/\mathbb{Z}_p = \mathbb{Z}[p^{-1}]/\mathbb{Z} = \bigcup_n p^{-n}\mathbb{Z}/\mathbb{Z}$ is discrete.

**Example 2.1.11.** The isomorphisms $p^{-n}\mathbb{Z}_p \xrightarrow{\sim} (\mathbb{Q}_p/p^n\mathbb{Z}_p)^\wedge$carrying $\xi$ to $x \mapsto e(\xi x)$ are compatible with the inclusion $p^{-m}\mathbb{Z}_p \subseteq p^{-n}\mathbb{Z}_p$ and the projection $\mathbb{Q}_p/p^n\mathbb{Z}_p \to \mathbb{Q}_p/p^m\mathbb{Z}_p$ for $m \leq n$. Note that $\mathbb{Q}_p = \bigcup_n p^{-n}\mathbb{Z}_p$. Moreover, for every unitary character $\chi$ of $\mathbb{Q}_p$, $\chi(p^n\mathbb{Z}_p) \subseteq N(1)$ for some $n$, so that $\chi$ is trivial on $p^n\mathbb{Z}_p$. Taking union, we obtain an isomorphism of topological groups $\mathbb{Q}_p \simeq \mathbb{Q}_p^\wedge$ carrying $\xi$ to $x \mapsto e(\lambda(\xi x))$, where $\lambda\colon \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p$ is the projection.

**Example 2.1.12.** Let $V$ be a finite-dimensional $\mathbb{Q}_p$-vector space. Then we have an isomorphism $\operatorname{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p) = V^\vee \xrightarrow{\sim} \hat{V}$ carrying $\phi$ to $x \mapsto e(\lambda(\phi(x)))$. For $V = K$ a finite field extension of $\mathbb{Q}_p$, composing with the isomorphism $K \xrightarrow{\sim} V^\vee$ carrying $\xi$ to $\operatorname{tr}_{K/\mathbb{Q}_p}(\xi x)$, we obtain an isomorphism $K \xrightarrow{\sim} K^\wedge$carrying $\xi$ to $x \mapsto e(\lambda(\operatorname{tr}_{K/\mathbb{Q}_p}(\xi x)))$.

**Example 2.1.13.** Let $V$ be a finite-dimensional real vector space. Then we have an isomorphism $\operatorname{Hom}_{\mathbb{R}}(V, \mathbb{R}) = V^\vee \xrightarrow{\sim} \hat{V}$ carrying $\phi$ to $x \mapsto e(\phi(x))$. For $V = K$ is either $\mathbb{R}$ or $\mathbb{C}$, composing with the isomorphism $K \xrightarrow{\sim} V^\vee$ carrying $\xi$ to $\operatorname{tr}_{K/\mathbb{R}}(\xi x)$, we obtain an isomorphism $K \xrightarrow{\sim} K^\wedge$carrying $\xi$ to $x \mapsto e(\operatorname{tr}_{K/\mathbb{R}}(\xi x))$.

We have proved the following.

**Proposition 2.1.14.** *Let $K$ be a local field of characteristic $0$ and let $\psi$ be a nonzero additive character of $K$. Then the map $K \to K^{\wedge}$ carrying $\xi$ to $\psi_\xi$ is an isomorphism of topological groups. Here $\psi_\xi$ is defined by $\psi_\xi(x) = \psi(\xi x)$.*

For $g \in G$, the map $\hat{G} \to S^1$ carrying $\chi$ to $\chi(g)$ is a unitary character. We obtain a homomorphism $\eta\colon G \to \hat{\hat{G}}$ carrying $g$ to $\chi \mapsto \chi(g)$, which is continuous if $G$ is locally compact. To see the continuity, let $K \subseteq \hat{G}$ be a compact subset, and let $W = \{\phi \in \hat{\hat{G}} \mid \phi(K) \subseteq N(1)\}$. Let $V$ be a compact neighborhood of $1 \in G$. Then there exists a finite subset $F \subset K$ such that $K \subseteq FW(V, N(1/2))$. Let $U = V \cap \bigcap_{\chi \in F} \chi^{-1}(N(1/2))$. Then $\eta(U) \subseteq W$.

**Theorem 2.1.15** (Pontryagin)**.** *Let $G$ be a locally compact abelian group. The map $\eta\colon G \to \hat{\hat{G}}$ is an isomorphism of topological groups.*

**Corollary 2.1.16.** *Let $H$ be a closed subgroup of $G$. Then the short exact sequence $1 \to H \xrightarrow{i} G \xrightarrow{p} G/H \to 1$ induces a short exact sequence*

$$1 \to (G/H)^{\wedge} \xrightarrow{\hat{p}} \hat{G} \xrightarrow{\hat{i}} \hat{H} \to 1,$$

*identifying $\hat{H}$ with the quotient of $\hat{G}$ by the closed subgroup $H^\perp$.*

*Proof.* We have seen that $\hat{p}$ induces an isomorphism of topological groups $(G/H)^{\wedge} \xrightarrow{\sim} H^\perp = \mathrm{Ker}(\hat{i})$. It remains to show that $\hat{i}$ is a quotient map. Let $L$ be the Pontryagin dual of $\hat{G}/H^\perp$, so that $\hat{L} = \hat{G}/H^\perp$. We have $\hat{i} = \hat{\psi} \circ \hat{\phi}$, where $\hat{G} \xrightarrow{\hat{\psi}} \hat{L} \xrightarrow{\hat{\phi}} \hat{H}$, corresponding to $H \xrightarrow{\phi} L \xrightarrow{\psi} G$. Since $\psi \circ \phi = i$, $\psi(L) \supseteq H$. Since $\hat{\psi} \circ \hat{p}$ factors through $\{1\}$, $p \circ \psi$ factors through $\{1\}$, so that $\psi(L) \subseteq H$. Thus $\psi(L) = H$, hence $\psi$ induces an isomorphism of topological groups $L \xrightarrow{\sim} H$. It follows that $\phi$ is an isomorphism of topological groups. Therefore, $\hat{\phi}$ is an isomorphism of topological groups. □

**Corollary 2.1.17.** *Let $H$ be a subgroup of $G$. Then $(H^\perp)^\perp = \bar{H}$.*

*Proof.* Since $H^\perp = \bar{H}^\perp$, we may assume that $H$ is closed. Then the assertion follows Corollary 2.1.16. □

We refer the reader to [B4, Section II.1] for a proof of the Pontryagin duality. The proof makes use of Fourier transformation. Let us recall the definition and a few facts.

We fix a Haar measure $dx$ on $G$. For $1 \le p < \infty$, let $L^p(G)$ be the completion of $C_c(G, \mathbb{C})$ with respect to the $L^p$-norm. For $f \in L^1(G)$, we define its *Fourier transform* $\mathcal{F}f\colon \hat{G} \to \mathbb{C}$ by $(\mathcal{F}f)(\chi) = \int_G f(x)\chi(x)\,dx$.[1] Then $\mathcal{F}f \in C(G, \mathbb{C})$ and $\|\mathcal{F}f\|_\infty \le \|f\|_1$. The convolution product $f * g$ for $f, g \in L^1(G)$ is defined by $(f * g)(x) = \int_G f(xy^{-1})g(y)\,dy$. This makes $L^1(G)$ into a commutative Banach algebra. We have $\mathcal{F}(f * g) = \mathcal{F}(f)\mathcal{F}(g)$. In other words, for $\chi \in \hat{G}$, the map $L^1(G) \to \mathbb{C}$, $f \mapsto (\mathcal{F}f)(\chi)$ is a character of $L^1(G)$, in the following sense.

[1] Bourbaki [B4, Section II.1] calls $\mathcal{F}$ the Fourier cotransform and defines the Fourier transform by $\chi \mapsto \int_G f(x)\chi(x^{-1})\,dx$.

**Remark 2.1.18.** Let $A$ be a (non-unital) commutative complex algebra. We define a *character* of $A$ to be a homomorphism $A \to \mathbb{C}$ of complex algebras. We let $X(A)$ denote the set of nonzero characters of $A$. We equip $X(A)$ with the topology of pointwise convergence. Then $X(A)$ is a Hausdorff space. The *Gelfand transform* $\mathcal{G}f \in C(X(A), \mathbb{C})$ of $f \in A$ is defined by $(\mathcal{G}f)(\chi) = \chi(f)$. If $A$ is a commutative Banach algebra, every character is continuous of norm $\leq 1$ [B4, I.3.1], so that $X(A) \cup \{0\}$ is a closed subset of the closed unit ball $B$ of $A^*$, the dual of the Banach space $A$ consisting of continuous linear functionals on $A$, equipped with the topology of pointwise convergence (also known as the weak-* topology). By the Banach-Alaoglu theorem, $B$ is compact (indeed, $B$ is a closed subset of the compact set $\prod_{f\in A} B_{\leq \|f\|}(0)$, where $B_{\leq r}(0) \subseteq \mathbb{C}$ denotes the closed disc of radius $r$), hence $X(A) \cup \{0\}$ is compact, so that $X(A)$ is locally compact. Moreover, $\chi \mapsto \mathrm{Ker}(\chi)$ defines a bijection from $X(A)$ to the set of maximal regular ideals of $A$ (an ideal $I$ of $A$ is *regular* if the quotient $A/I$ admits a multiplicative identity 1). One can show that $\chi \mapsto (f \mapsto (\mathcal{F}f)(\chi))$ defines a homeomorphism $\hat{G} \xrightarrow{\sim} X(L^1(G))$. Via this homeomorphism $\mathcal{F}f$ can be identified with $\mathcal{G}f$.

**Theorem 2.1.19** (Plancherel)**.** *There exists a unique Haar measure $d\hat{x}$ on $\hat{G}$ such that $\int_{\hat{G}} |\mathcal{F}f|^2\, d\hat{x} = \int_G |f|^2\, dx$ for all $f \in C_c(X, \mathbb{C})$. The map $\mathcal{F}\colon C_c(X, \mathbb{C}) \to L^2(\hat{G})$ extends uniquely to an isometry $\mathcal{F}\colon L^2(G) \to L^2(\hat{G})$.*

The Haar measure $d\hat{x}$ on $\hat{G}$ is called the *dual measure* of $dx$. Note that for $c > 0$, the dual measure of $c\, dx$ is $c^{-1}\, d\hat{x}$.

**Theorem 2.1.20** (Fourier inversion)**.** *Via the isomorphism $\eta\colon G \xrightarrow{\sim} \hat{\hat{G}}$, $dx$ can be identified with $d\hat{\hat{x}}$, and $(\mathcal{F}\mathcal{F}f)(\eta x) = f(x^{-1})$ for $f \in L^2(G)$ and $x \in G$.*

**Definition 2.1.21.** A quasi-character of a topological abelian group $G$ is a continuous homomorphism $G \to \mathbb{C}^\times$.

## 2.2 Local zeta integrals

### Duality of the additive group

Let $k$ be a local field of characteristic 0 and let $\psi$ be a nontrivial additive character of $k$. For every Haar measure $dx$ on the additive group of $k$, the dual measure $d\hat{x}$ can be regarded as a Haar measure on $k$ via the isomorphism $k \xrightarrow{\sim} k^\frown$carrying $\xi$ to $\psi_\xi$. There exists a unique Haar measure $dx$ on $k$, depending only on $\psi$, that is *self-dual*, namely $dx = d\hat{x}$. Indeed, if $d\hat{x} = c\, dx$, then $\sqrt{c}\, dx$ is self-dual. For a function $f$ on $k$, we write $\hat{f}$ for $\mathcal{F}f$, regarded as a function on $k$ by $\hat{f}(\xi) = \int_k f(x)\psi(\xi x)\, dx$.

In the sequel we fix an additive character $\psi$ by $\psi(x) = e(-\mathrm{tr}_{k/\mathbb{R}}(x))$ for $k = \mathbb{R}$ or $k = \mathbb{C}$ and $\psi(x) = e(\lambda(\mathrm{tr}_{K/\mathbb{Q}_p}(x)))$ if $k$ is $p$-adic. Let $dx$ be the self-dual measure determined by $\psi$. For $k = \mathbb{R}$, $dx$ is the usual Lebesgue measure. For $k = \mathbb{C}$, $dx$ is twice the usual Lebesgue measure. If $k$ is $p$-adic, let $\mathcal{O}$ be the ring of integers of $k$. Recall that the different $\mathfrak{d}$ of $k$ is an ideal of $\mathcal{O}$ defined by the following condition: For $x \in k$, $x \in \mathfrak{d}^{-1}$ if and only if $\mathrm{tr}_{k/\mathbb{Q}_p}(xy) \in \mathbb{Z}_p$ for all $y \in \mathcal{O}$. We have $\int_{\mathcal{O}} dx = (N\mathfrak{d})^{-1/2}$, where $N\mathfrak{d} = \#(\mathcal{O}/\mathfrak{d})$. [2]

We let $\mathcal{S}(k)$ denote the space of Schwartz-Bruhat functions. In the Archimedean case, this is the space of Schwartz functions. Recall that a Schwartz function on $\mathbb{R}^n$ is a function such that $\sup_{x\in\mathbb{R}^n}|x^\alpha D^\beta f(x)| < \infty$ for all $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. For $1 \leq p < \infty$, $\mathcal{S}(k)$ is dense in $L^p(k, \mathbb{C})$.

**Proposition 2.2.1.** *For $f \in \mathcal{S}(k)$, we have $\hat{f} \in \mathcal{S}(k)$.*

In the Archimedean case all the above facts are classical and our proof of Theorem 2.2.8 below also implies that $dx$ is as described above. We give proofs in the $p$-adic case. The following lemma applies to all cases.

**Lemma 2.2.2.** *Let $a \in k$, $g(x) = f(x-a)$, $h(x) = \psi(ax)f(x)$. Then $\hat{g}(x) = \psi(ax)f(x)$ and $\hat{h}(x) = \hat{f}(x+a)$.*

*Proof.* Indeed,

$$\begin{aligned}\hat{g}(x) &= \int_k f(y-a)\psi(xy)\,dy = \int_k f(y)\psi(x(y+a))\,dy = \psi(ax)\hat{f}(x),\\ \hat{h}(x) &= \int_k \psi(ay)f(y)\psi(xy)\,dx = \int_k f(y)\psi((x+a)y)\,dy = \hat{f}(x+a).\end{aligned}$$

□

**Lemma 2.2.3.** *Let $G$ be a compact abelian group and let $dg$ be a Haar measure on $G$. Let $\chi\colon G \to S^1$ be a character. Then*

$$\int_G \chi\,dg = \begin{cases}\mathrm{vol}(G) & \chi = 1,\\ 0 & \chi \neq 1.\end{cases}$$

*Proof.* The case $\chi = 1$ is trivial. For every $g \in G$, $\chi(g)\int_G \chi(h)\,dh = \int_G \chi(gh)\,dh = \int_G \chi(h)\,dh$. The case $\chi \neq 1$ follows. □

Assume now that $k$ is $p$-adic.

**Lemma 2.2.4.** *Let $\mathfrak{a}$ be a fractional ideal. Then $\widehat{\mathbf{1}_{\mathfrak{a}}} = (N\mathfrak{d})^{-1/2}(N\mathfrak{a})^{-1}\mathbf{1}_{\mathfrak{d}^{-1}\mathfrak{a}^{-1}}$.*

*Proof.* We have $\widehat{\mathbf{1}_{\mathfrak{a}}}(x) = \int_{\mathfrak{a}} \psi(xy)\,dy$. Note that $x \in \mathfrak{d}^{-1}\mathfrak{a}^{-1}$ if and only if $y \mapsto \psi(xy)$ is a trivial character of $\mathfrak{a}$. The assertion then follows from the preceding lemma and the fact that $\mathrm{vol}(\mathfrak{a}) = (N\mathfrak{d})^{-1/2}(N\mathfrak{a})^{-1}$. □

By Lemma 1.4.11, the proposition reduces to the case $f = \mathbf{1}_B$ for some ball $B = a + \mathfrak{a}$. By Lemma 2.2.2, we reduce to Lemma 2.2.4.

The space $\mathcal{S}(k)$ is dense in $C_c(k, \mathbb{C}) = \bigcup_K C(k, \mathbb{C})$ equipped with the topology defined similarly to Remark 1.4.2, which is stronger than the $L^p$-topology for $1 \leq p < \infty$. Indeed, the density follows from the density of $\mathcal{S}(k) \cap C_K(k, \mathbb{C})$ in $C_K(k, \mathbb{C})$, which is a consequence of uniform continuity. It follows that $\mathcal{S}(k)$ is dense in $L^p(k, \mathbb{C})$.

[2] In view of our convention for $\psi$, our convention for $\hat{f}$ differs from that of Tate [T1] by a sign. In the Archimedean case, our convention coincides with that of the classical Fourier transform.

To show Fourier inversion, we are thus reduced to the case $f \in \mathcal{S}(k)$, and then to $f = \mathbf{1}_B$ by Lemma 1.4.11, and finally to $f = \mathbf{1}_{\mathfrak{a}}$ by Lemma 2.2.2. In this case, we have

$$\hat{\hat{f}}(x) = (N\mathfrak{d})^{-1/2}(N\mathfrak{a})^{-1}\widehat{\mathbf{1}_{\mathfrak{d}^{-1}\mathfrak{a}^{-1}}} = (N\mathfrak{d})^{-1/2}(N\mathfrak{a})^{-1}(N\mathfrak{d})^{-1/2}(N(\mathfrak{d}^{-1}\mathfrak{a}^{-1}))^{-1}\mathbf{1}_{\mathfrak{a}} = \mathbf{1}_{\mathfrak{a}}.$$

## Local zeta integrals

Let $k$ be a local field of characteristic 0. We let $X(k^\times)$ denote the abelian group of quasi-characters of $k^\times$ with group law defined by pointwise multiplication. We have a short exact sequence

$$1 \to C \to k^\times \xrightarrow{|-|} |k^\times| \to 1.$$

Note that $C$ is compact. We say $\chi$ is *unramified* if $\chi(C) = |1|$. In this case $\chi$ factors through $|k^\times|$, so that $\chi = |-|^s$ for some $s \in \mathbb{C}$. In the Archimedean case, $|k^\times| = \mathbb{R}_{>0}$ so that $s$ is unique. In the $p$-adic case, we have $|k^\times| = |N\mathfrak{p}|^{\mathbb{Z}}$ so that $\mathbb{C}/2\pi i \log(N\mathfrak{p})\mathbb{Z}$. Here $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$.

The sequence is split. In the $p$-adic case the splitting depends on the choice of a uniformizer $\pi$. In all cases the sequence induces a split short exact sequence $1 \to X^{\mathrm{ur}}(k^\times) \to X(k^\times) \to \hat{C} \to 1$, which equips $X(k^\times)$ with the structure of a complex Lie group of dimension 1 (that does not depend on the choice of a splitting), with $\hat{C}$ being the group of connected components.

For $k = \mathbb{R}$, $C = \{\pm 1\}$, so that every quasi-character can be uniquely written as $\chi = |-|^s$ or $\chi = \mathrm{sgn}|-|^s$ for $s \in \mathbb{C}$. For $k = \mathbb{C}$, $C = S^1$, so that every quasi-character can be uniquely written as $\chi = \chi_n|-|^s$ for $n \in \mathbb{Z}$, $s \in \mathbb{C}$, where $\chi_n$ is the unitary character $\chi_n(z) = (z/|z|_{\mathbb{C}})^n$. For $k$ $p$-adic, $C = \mathcal{O}^\times$, so that every quasi-character can be uniquely written as $\chi = \chi_0|-|^s$, where $\chi_0$ is a unitary character satisfying $\chi_0(\pi) = 1$, and $s \in \mathbb{C}/2\pi i \log(N\mathfrak{p})\mathbb{Z}$. Since the subgroups $1 + \mathfrak{p}^n$, $n \geq 1$ of $\mathcal{O}^\times$ form a fundamental system of neighborhoods of 1, there exists $n$ such that $\chi(1 + \mathfrak{p}^n) = \{1\}$. If $\chi$ is ramified, the *conductor* is defined to be $\mathfrak{p}^n$, where $n$ is the least integer such that $\chi(1 + \mathfrak{p}^n) = \{1\}$. For $\chi$ unramified, we define the conductor to be $\mathcal{O}$.Note that $\hat{C} = \bigcup_n (\mathcal{O}^\times/(1 + \mathfrak{p}^n))^\wedge$is countable.

In all cases $\sigma(\chi) = \mathrm{Re}(s)$ is well-defined.

For fix a Haar measure $d^\times x = \delta(k)\, dx/|x|$ on $k^\times$ as follows. For $k$ Archimedean, we take $\delta(k) = 1$. For $k$ $p$-adic, we take $\delta(k) = \frac{N\mathfrak{p}}{N\mathfrak{p}-1}\frac{dx}{|x|}$, so that $\int_{\mathcal{O}^\times} d^\times x = (N\mathfrak{d})^{-\frac{1}{2}}$.

**Definition 2.2.5.** For $f \in \mathcal{S}(k)$ and $\chi \in X(k^\times)$, we define the *local zeta integral* by

$$\zeta(f, \chi) = \int_{k^\times} f(x)\chi(x)d^\times x.$$

**Lemma 2.2.6.** *$\zeta(f, \chi)$ converges absolutely to a holomorphic function for $\sigma(\chi) > 0$.*

*Proof.* This follows from the fact that $\int_{k^\times} f(x)\chi(x)d^\times x$ and $\int_{k^\times} f(x)\chi(x)\log(|x|)d^\times x$ converge absolutely and uniformly on any compact in $\sigma(\chi) > 0$. □

Recall that the Gamma function is defined by $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}\, dx$, which converges absolutely to a holomorphic function for $\mathrm{Re}(s) > 0$. It extends to a meromorphic function on $\mathbb{C}$ without zeroes.

**Definition 2.2.7.** For a quasi-character $\chi$ of $k^\times$, we define the *local L-factor* $L(\chi)$ as follows.

(1) For $k = \mathbb{R}$,

$$L(|\cdot|^s) = \Gamma_{\mathbb{R}}(s), \quad L(\mathrm{sgn}|\cdot|^s) = \Gamma_{\mathbb{R}}(s+1),$$

where

$$\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right).$$

(2) For $k = \mathbb{C}$,

$$L(\chi_n|\cdot|^s) = \Gamma_{\mathbb{C}}\left(s + \frac{|n|}{2}\right),$$

and

$$\Gamma_{\mathbb{C}}(s) = (2\pi)^{1-s}\Gamma(s).$$

(3) Assume that $k$ is $p$-adic. For $\chi = |\cdot|^s$ unramified,

$$L(|\cdot|^s) = \frac{1}{1-(N\mathfrak{p})^{-s}} = \frac{1}{1-\chi(\pi)},$$

where $\pi$ is a uniformizer of $k$, and for $\chi$ ramified,

$$L(\chi) = 1.$$

We note that $L(\chi)$ is a meromorphic function on $X(k^\times)$ with no poles for $\sigma(\chi) > 0$ and no zeros for all $\chi$.

**Theorem 2.2.8.** *For any $f \in \mathcal{S}(k)$, the function $\chi \mapsto \zeta(f, \chi)$ extends to a meromorphic function on the space of all quasi-characters, such that $\zeta(f,\chi)/L(\chi)$ is holomorphic and satisfies the functional equation*

$$\frac{\zeta(f,\chi)}{L(\chi)}\epsilon(\chi) = \frac{\zeta(\hat{f},\chi^\vee)}{L(\chi^\vee)},$$

*where $\chi^\vee = \chi^{-1}|-|$, and $\epsilon(\chi)$ is a holomorphic function of $\chi$ with no zeros, independent of $f$, given as follows.*

*(1) For $k = \mathbb{R}$,*

$$\epsilon(|\cdot|^s) = 1, \quad \epsilon(\mathrm{sgn}|\cdot|^s) = -i.$$

*(2) For $k = \mathbb{C}$,*

$$\epsilon(\chi_n|\cdot|^s) = (-i)^{|n|},$$

*where $\chi_n$ is the unitary character $\chi_n(z) = (z/|z|)^n$.*

*(3) If $k$ is $p$-adic, then*

$$\epsilon(|\cdot|^s) = (N\mathfrak{d})^{\frac{1}{2}-s}, \quad \epsilon(\chi_0|\cdot|^s) = (N(\mathfrak{d}\mathfrak{f}))^{\frac{1}{2}-s}\tau_0(\overline{\chi_0}),$$

*where $\chi_0$ is unitary, ramified of conductor $\mathfrak{f}$ satisfying $\chi_0(\pi) = 1$, and*

$$\tau_0(\overline{\chi_0}) = (N\mathfrak{f})^{-\frac{1}{2}}\sum_x \overline{\chi_0}(x)\psi\left(\frac{x}{\pi^m}\right)$$

*is the normalized Gauss sum, $x$ running through a set of representatives of $\mathcal{O}^\times/(1+\mathfrak{f})$, with $\mathfrak{d}\mathfrak{f} = \mathfrak{p}^m$.*

*Moreover, for each connected component $X$ of $X(k^\times)$, there exists a $f \in \mathcal{S}(k)$ such that $\zeta(f,\chi) = L(\chi)$ for $\chi \in X$.*

In some sense, $L(\chi)$ is the greatest common divisor of $\zeta(f,\chi)$, $f \in \mathcal{S}(k)$. The proof of the theorem relies on the following.

**Lemma 2.2.9.** *For all $f, g \in \mathcal{S}(k)$ and $\chi \in X(k^\times)$ with $0 < \sigma(\chi) < 1$, we have*

$$\zeta(f,\chi)\zeta(\hat{g},\chi^\vee) = \zeta(\hat{f},\chi^\vee)\zeta(g,\chi).$$

*Proof.* We have

$$\begin{aligned} \zeta(f,\chi)\zeta(\hat{g},\chi^\vee) &= \int_{k^\times}\int_{k^\times} f(x)\chi(x)\hat{g}(y)\chi^{-1}(y)|y|\,d^\times x\,d^\times y \\ (y \mapsto xy) \qquad &= \int_{k^\times}\int_{k^\times} f(x)\chi(x)\hat{g}(xy)\chi^{-1}(xy)|xy|\,d^\times x\,d^\times y \\ &= \delta(k)\int_{k^\times}\left(\int_k\int_k f(x)g(z)\psi(xyz)\,dx\,dz\right)\chi(y^{-1})|y|\,dy, \end{aligned}$$

which is symmetric in $f$ and $g$. □

*Proof of Theorem 2.2.8.* We will show for each connected component $X$ of $X(k^\times)$ that there exists one choice of $f$ such that $\zeta(f,\chi) = L(\chi)$ for $\chi \in X$, $\sigma(\chi) > 0$ and $\zeta(\hat{f},\chi^\vee) = \epsilon(\chi)L(\chi^\vee)$ holds for $\chi \in X$, $\sigma(\chi) < 1$. In particular, the functional equation holds for this $f$ and $\zeta(f,\chi)$ is not identically zero on any component. By the lemma, for $0 < \sigma(\chi) < 1$, multiplying by $\zeta(g,\chi)$ and dividing by $\zeta(f,\chi)$, we see that the functional equation holds for all $f$ (more informally, $\zeta(\hat{f},\chi^\vee)/\zeta(f,\chi)$ is independent of $f$). Since $\zeta(f,\chi)/L(\chi)$ is homomorphic for $\sigma(\chi) > 0$ and $\zeta(\hat{f},\chi^\vee)/L(\chi^\vee)$ is holomorphic for $\sigma(\chi) < 1$, $\zeta(f,\chi)/L(\chi)$ admits a holomorphic continuation to $X(k^\times)$.

(1) Assume $k = \mathbb{R}$. For $\chi = |\cdot|^s$, we take $f(x) = e^{-\pi x^2}$. Then

$$\begin{aligned} \zeta(f,|\cdot|^s) &= \int_{\mathbb{R}^\times} e^{-\pi x^2}|x|^s\,d^\times x = 2\int_0^\infty e^{-\pi x^2}x^{s-1}\,dx \\ (y = \pi x^2) \qquad &= \pi^{-\frac{s}{2}}\int_0^\infty e^{-y}y^{\frac{s}{2}-1}\,dy = \Gamma_{\mathbb{R}}(s) = L(|\cdot|^s). \end{aligned} \tag{2.2.1}$$

Moreover,

$$\hat{f}(y) = \int_{\mathbb{R}} e^{-\pi x^2 - 2\pi ixy}\,dx = e^{-\pi y^2}\int_{\mathbb{R}} e^{-\pi(x+yi)^2}\,dx.$$

By contour integral and Gaussian integral,

$$\int_{\mathbb{R}} e^{-\pi(x+yi)^2}\,dx = \int_{\mathbb{R}} e^{-\pi x^2}\,dx = 1.$$

Thus

$$\hat{f} = f, \tag{2.2.2}$$

so that $\zeta(\hat{f},\chi^\vee) = \zeta(f,\chi^\vee) = L(\chi^\vee)$.

For $\chi = \mathrm{sgn}|\cdot|^s$, we take $f(x) = xe^{-\pi x^2}$. By (2.2.1), we have

$$\zeta(f,\chi) = 2\int_0^\infty e^{-\pi x^2} x^s\,dx = \Gamma_{\mathbb{R}}(s+1) = L(\chi).$$

Moreover, taking derivative in (2.2.2), we get $-2\pi i\hat{f} = -2\pi f$, so that $\hat{f} = -if$. Thus $\zeta(\hat{f},\chi^\vee) = \zeta(-if,\chi^\vee) = \epsilon(\chi)L(\chi^\vee)$.

(2) Assume $k = \mathbb{C}$. We take $f_n(z) = \bar{z}^n e^{-2\pi z\bar{z}}$ for $n \geq 0$ and $f_n(z) = z^{-n}e^{-2\pi z\bar{z}}$ for $n \leq 0$. We have

$$\begin{aligned}
& \zeta(f_n,\chi_n|\cdot|^s) = \int_{\mathbb{C}^\times} f_n(z)\chi_n(z)(z\bar{z})^s\,d^\times z\\
(dx\,dy = r\,dr\,d\theta) \qquad & = \int_{\theta=0}^{2\pi}\int_{r=0}^{\infty} e^{-2\pi r^2} r^{2s+|n|}\frac{2r\,dr\,d\theta}{r^2}\\
& = 4\pi\int_0^\infty e^{-2\pi r^2} r^{2s+|n|-1}\,dr\\
(t = 2\pi r^2) \qquad & = (2\pi)^{1-(s+\frac{|n|}{2})}\int_0^\infty e^{-t}t^{s+\frac{|n|}{2}-1}\,dt = L(\chi_n|\cdot|^s).
\end{aligned}$$

We have

$$\begin{aligned}
& \widehat{f_0}(z) = \int_{\mathbb{C}} e^{-2\pi w\bar{w}} e^{-2\pi i(zw+\bar{z}\bar{w})}\,dw\\
(z = x+iy,\ w = u+iv) \qquad & = 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-2\pi(u^2+v^2)}e^{-4\pi i(ux-vy)}\,du\,dv\\
& = 2e^{-2\pi(x^2+y^2)}\int_{-\infty}^{\infty} e^{-2\pi(u+ix)^2}\,du\int_{-\infty}^{\infty} e^{-2\pi(v-iy)^2}\,dv\\
& = f_0(z).
\end{aligned}$$

Regarding $z$ and $\bar{z}$ as independent variables and taking derivatives with respect to $\frac{\partial^n}{\partial z^n}$ and $\frac{\partial^n}{\partial \bar{z}^n}$, we get $(2\pi i)^n\widehat{f_n} = (2\pi)^n f_{-n}$ and $(2\pi i)^n\widehat{f_{-n}} = (2\pi)^n f_n$ for $n \geq 0$. Thus for all $n$, $\widehat{f_n} = (-i)^{|n|}f_{-n}$. For $\chi = \chi_n|\cdot|^s$, $\chi^\vee = \chi_{-n}|\cdot|^{1-s}$, so that

$$\zeta(\hat{f}_n,\chi^\vee) = \zeta((-i)^{|n|}f_{-n},\chi^\vee) = \epsilon(\chi)L(\chi^\vee).$$

(3) Assume that $k$ is $p$-adic. For $\chi = |\cdot|^s$ unramified, we take $f = (N\mathfrak{d})^{\frac{1}{2}}\mathbf{1}_{\mathcal{O}}$. Then $\hat{f} = \mathbf{1}_{\mathfrak{d}^{-1}}$. We have

$$\begin{aligned}
& \zeta(f,\chi) = (N\mathfrak{d})^{\frac{1}{2}}\int_{\mathcal{O}-\{0\}}|x|^s d^\times x\\
(\mathcal{O}-\{0\} = \coprod_{n=0}^{\infty}\pi^n\mathcal{O}^\times) \qquad & = (N\mathfrak{d})^{\frac{1}{2}}\sum_{n=0}^{\infty}|\pi|^{ns}\int_{\mathcal{O}^\times} d^\times x = \frac{1}{1-|\pi|^{ns}} = L(\chi),
\end{aligned}$$

and

$$\begin{aligned}
& \zeta(\hat{f},\chi^\vee) = \int_{\mathfrak{d}^{-1}-\{0\}}|x|^{1-s}d^\times x\\
(\mathfrak{d}^{-1}-\{0\} = \coprod_{n=-d}^{\infty}\pi^n\mathcal{O}^\times) \qquad & = \sum_{n=-d}^{\infty}|\pi|^{n(1-s)}\int_{\mathcal{O}^\times} d^\times x = (N\mathfrak{d})^{-\frac{1}{2}}\frac{|\pi|^{-d(1-s)}}{1-|\pi|^{1-s}}\\
& = (N\mathfrak{d})^{\frac{1}{2}-s}L(|\cdot|^{1-s}) = \epsilon(\chi)L(\chi^\vee).
\end{aligned}$$

For $\chi = \chi_0|\cdot|^s$ ramified of conductor $\mathfrak{f}$ with $\chi_0(\pi) = 1$, we take $f = c^{-1}\mathbf{1}_{1+\mathfrak{f}}$, where $c = \int_{1+\mathfrak{f}} d^\times x$. Then $\zeta(f,\chi) = 1 = L(\chi)$ and $\hat{f} = c^{-1}(N\mathfrak{d})^{-\frac{1}{2}}(N\mathfrak{f})^{-1}\psi\mathbf{1}_{(\mathfrak{d}\mathfrak{f})^{-1}}$. We have

$$\zeta(\psi\mathbf{1}_{(\mathfrak{d}\mathfrak{f})^{-1}},\chi^\vee) = \int_{(\mathfrak{d}\mathfrak{f})^{-1}-\{0\}} \psi(x)\overline{\chi_0}(x)|x|^{1-s}d^\times x = \sum_{n=-m}^{\infty}|\pi|^{n(1-s)}I_n,$$

where $I_n = \int_{\mathcal{O}^\times}\psi(\pi^n x)\overline{\chi_0}(x)d^\times x$. For $n \geq -d$, we have $\pi^n x \in \mathfrak{d}^{-1}$ for $x \in \mathcal{O}^\times$, so that $\psi(\pi^n x) = 1$ and $I_n = \int_{\mathcal{O}^\times}\overline{\chi_0}(x)d^\times x = 0$. Assume $-m \leq n < -d$. For $y \in 1+\mathfrak{p}^{-n}\mathfrak{d}^{-1}$, we have $\psi(\pi^n xy) = \psi(\pi^n x)$. Thus, if $S$ denotes a set of representatives of $\mathcal{O}^\times/(1+\mathfrak{p}^{-n}\mathfrak{d}^{-1})$, we have

$$I_n = \sum_{x\in S}\overline{\chi_0}(x)\psi(\pi^n x)\int_{1+\mathfrak{p}^{-n}\mathfrak{d}^{-1}}\overline{\chi_0}(y)\,d^\times y.$$

For $n > -m$, $1+\mathfrak{p}^{-n}\mathfrak{d}^{-1}$ strictly contains $1+\mathfrak{f}$, or, in other words, $\chi_0$ is nontrivial on $1+\mathfrak{p}^{-n}\mathfrak{d}^{-1}$, so that the integral is zero. For $n = -m$, we have

$$I_{-m} = \sum_{x\in S}\overline{\chi_0}\psi(\pi^{-m}x)\int_{1+\mathfrak{f}} d^\times y = c(N\mathfrak{f})^{\frac{1}{2}}\tau_0(\overline{\chi_0}).$$

Therefore,

$$\zeta(\hat{f},\chi^\vee) = (N(\mathfrak{d}\mathfrak{f}))^{\frac{1}{2}-s}\tau_0(\overline{\chi_0}) = \epsilon(\chi)L(\chi^\vee).$$

□

**Remark 2.2.10.** We have

$$\epsilon(\chi)\epsilon(\chi^\vee) = \chi(-1), \quad \epsilon(\bar{\chi}) = \chi(-1)\overline{\epsilon(\chi)}. \tag{2.2.3}$$

Indeed, the first equality follows from

$$\frac{\zeta(f,\chi)}{L(\chi)}\epsilon(\chi)\epsilon(\chi^\vee) = \frac{\zeta(\hat{f},\chi^\vee)}{L(\chi^\vee)}\epsilon(\chi^\vee) = \frac{\zeta(\hat{\hat{f}},\chi^{\vee\vee})}{L(\chi^{\vee\vee})} = \chi(-1)\frac{\zeta(f,\chi)}{L(\chi)},$$

where we used $\hat{\hat{f}}(x) = f(-x)$ in the last equality. The second equality of (2.2.3) can be shown similarly using the fact that $\hat{\bar{f}}(x) = \bar{\hat{f}}(-x)$. The equalities (2.2.3) also follow from the explicit formulas for $\epsilon$. For $\sigma(\chi) = \frac{1}{2}$, $\chi^\vee = \bar{\chi}$, so that $|\epsilon(\chi)| = 1$.

## 2.3 Global zeta integrals

Let $K$ be a number field.

### Duality on $\mathbb{A}_K$

We fix a character $\psi\colon \mathbb{A}_K \to \mathbb{C}^\times$ by $\psi(x) = \prod_{v\in V}\psi_v(x_v)$, where $\psi_v$ is the additive character of $K_v$ in the previous section. For $\xi \in \mathbb{A}_K$, $\psi_\xi(x) = \psi(\xi x)$ defines a character $\psi_\xi\colon \mathbb{A}_K \to \mathbb{C}^\times$.

**Proposition 2.3.1.** *The map $\mathbb{A}_K \to \widehat{\mathbb{A}_K}$ carrying $\xi$ to $\psi_\xi$ is an isomorphism of topological groups.*

**Proposition 2.3.2.** *The character $\psi_\xi$ factorizes through $\mathbb{A}_K/K$ if and only if $\xi \in K$. In particular, $\xi \mapsto \psi_\xi$ induces an isomorphism $K \to (\mathbb{A}_K/K)\widehat{}$.*

The local self-dual measures $dx_v$ on $K_v$ with respect to $\psi_v$ induce a self-dual measure $dx$ on $\mathbb{A}_K$ with respect to $\psi$. The volume of the quotient $\mathbb{A}_K/K$ with respect to the self-dual measure on $\mathbb{A}_K$ and the counting measure on $K$ is 1. This is consistent with our computation in Example 1.4.31 by the product formula $|\Delta_K| = \prod_v N\mathfrak{d}_v$.

For a function on $\mathbb{A}_K$, we write $\hat{f}$ for $\mathcal{F}f$, considered as a function on $\mathbb{A}_K$ by $\hat{f}(\xi) = \int_{\mathbb{A}_K} f(x)\psi(\xi x)\,dx$. The space $\mathcal{S}(\mathbb{A}_K)$ of *Schwartz functions* on $\mathbb{A}_K$ is the space of finite linear combinations of functions of the form $f = \otimes_v f_v$, where each $f_v \in \mathcal{S}(K_v)$ and $f_v = \mathbf{1}_{\mathcal{O}_v}$ for all but finitely many $v$. Note that for $f$ as above, we have $\hat{f} = \otimes_v \widehat{f_v} \in \mathcal{S}(\mathbb{A}_K)$. We obtained the following proposition.

**Proposition 2.3.3.** *The Fourier transform $f \mapsto \hat{f}$ preserves $\mathcal{S}(\mathbb{A}_K)$ and $\hat{\hat{f}}(x) = f(-x)$ for $f \in \mathcal{S}(\mathbb{A}_K)$.*

**Proposition 2.3.4** (Poisson summation formula)**.** *For $f \in \mathcal{S}(\mathbb{A}_K)$, $\sum_{x\in K} f(x)$ converges absolutely and*

$$\sum_{x\in K} f(x) = \sum_{\xi\in K} \hat{f}(\xi).$$

**Corollary 2.3.5.** *Let $f \in \mathcal{S}(\mathbb{A}_K)$ and $x \in \mathbb{I}_K$. Then*

$$\sum_{\xi\in K} f(x\xi) = \frac{1}{|x|}\sum_{\xi\in K} \hat{f}\left(\frac{\xi}{x}\right).$$

In the function field case, this formula implies the Riemann-Roch theorem. See [RV, Section 7.2].

*Proof.* This is the Poisson summation formula applied to the function $g \in \mathcal{S}(\mathbb{A}_K)$ given by $g(y) = f(xy)$. Indeed, $\hat{g}(y) = \frac{1}{|x|}\hat{f}\left(\frac{y}{x}\right)$. □

## Global zeta integrals

A *Hecke character* of $K$ is a quasi-character $\mathbb{I}_K/K^\times \to \mathbb{C}^\times$. We let $X$ denote the space of Hecke characters of $K$. We have a split exact sequence

$$1 \to \mathbb{I}_K^1/K^\times \to \mathbb{I}_K/K^\times \xrightarrow{|-|} \mathbb{R}_{>0}^\times \to 1,$$

which induces a split exact sequence $1 \to X^{\mathrm{ur}} \to X \to (\mathbb{I}_K^1/K^\times)\widehat{}\to 1$. This equips $X$ with the structure of a complex Lie group of dimension 1, with $(\mathbb{I}_K^1/K^\times)\widehat{}$ being the group of connected components. For any Hecke character $\chi$, there exists a unique real number $\sigma(\chi)$ such that $|\chi(x)| = |x|^{\sigma(\chi)}$.

**Definition 2.3.6.** Let $f \in \mathcal{S}(\mathbb{A}_K)$ and let $\chi\colon \mathbb{I}_K/K^\times \to \mathbb{C}^\times$ be a Hecke character. We define the *global zeta integral* by

$$\zeta(f,\chi) = \int_{\mathbb{I}_K} f(x)\chi(x)d^\times x.$$

**Lemma 2.3.7.** *The zeta integral $\zeta(f,\chi)$ converges absolutely to a holomorphic function for $\sigma(\chi) > 1$.*

**Theorem 2.3.8** (Tate, Iwasawa)**.** *Let $f \in \mathcal{S}(\mathbb{A}_K)$. The function $\chi \mapsto \zeta(f,\chi)$ extends to a meromorphic function on the space of all Hecke characters of $K$, holomorphic except for simple poles at $\chi = 1$ and $\chi = |\cdot|$, satisfying the functional equation*

$$\zeta(f,\chi) = \zeta(\hat{f},\chi^\vee). \tag{2.3.1}$$

*Moreover, the residues of $\zeta(f,\chi)$ are $-f(0)\mathrm{vol}$ at $\chi = 1$ and $\hat{f}(0)\mathrm{vol}$ at $\chi = |\cdot|$, where*

$$\mathrm{vol} = \mathrm{vol}(\mathbb{I}_K^1/K^\times) = \frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|\Delta_K|}}.$$

*Proof.* We have $\mathbb{I}_K = \mathbb{I}_K^{\leq 1} \cup \mathbb{I}_K^{\geq 1}$, where $\mathbb{I}_K^{\leq 1}$ and $\mathbb{I}_K^{\geq 1}$ denote the sets of idèles of content $\leq 1$ and $\geq 1$, respectively. We have

$$\zeta(f,\chi) = \int_{\mathbb{I}_K} f(x)\chi(x)d^\times x = \int_{\mathbb{I}_K^{\leq 1}} f(x)\chi(x)d^\times x + \int_{\mathbb{I}_K^{\geq 1}} f(x)\chi(x)d^\times x.$$

Moreover,

$$\begin{aligned}
\int_{\mathbb{I}_K^{\leq 1}} f(x)\chi(x)d^\times &= \int_{\mathbb{I}_K^{\leq 1}/K^\times} \sum_{\xi\in K^\times} f(x\xi)\chi(x)d^\times x \\
\text{(by Corollary 2.3.5)} \quad &= \int_{\mathbb{I}_K^{\leq 1}/K^\times} \frac{1}{|x|} \sum_{\xi\in K^\times} \hat{f}(\frac{\xi}{x})\chi(x)d^\times x + \int_{\mathbb{I}_K^{\leq 1}/K^\times} (\frac{1}{|x|}\hat{f}(0) - f(0))\chi(x)d^\times x \\
&= A + B.
\end{aligned}$$

Putting $y = 1/x$, we get

$$A = \int_{\mathbb{I}_K^{\geq 1}/K^\times} \sum_{\xi\in K^\times} \hat{f}(y\xi)\chi^\vee(y)d^\times y = \int_{\mathbb{I}_K^{\geq 1}} \hat{f}(y\xi)\chi^\vee(y)d^\times y.$$

We choose a splitting $\mathbb{I}_K/K^\times \simeq I_K^1/K^\times \times \mathbb{R}_{>0}^\times$ and write $\chi = \chi_0|-|^s$. Then

$$B = \int_{\mathbb{I}_K^1/K^\times} \chi_0(x)d^\times x \int_0^1 (\frac{1}{t}\hat{f}(0) - f(0))t^{s-1}dt = \begin{cases} \mathrm{vol}(\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}) & \chi = |-|^s, \\ 0 & \chi \text{ ramified.} \end{cases}$$

In summary, we have

$$\zeta(f,\chi) = \int_{\mathbb{I}_K^{\geq 1}} f(x)\chi(x)d^\times x + \int_{\mathbb{I}_K^{\geq 1}} \hat{f}(x)\chi^\vee(x)d^\times x + \begin{cases} \mathrm{vol}(\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}) & \chi = |-|^s, \\ 0 & \chi \text{ ramified.} \end{cases}$$

The two integrals converge absolutely to holomorphic functions on $X$. The functional equation follows. □

**Definition 2.3.9.** For a Hecke character $\chi$ of $K$, we define the *Hecke $L$-function* by

$$L(\chi) = \prod_{v \in V} L(\chi_v).$$

Let $S$ be the finite set of places $v \in V_f$ for which $\chi_v$ is ramified. Note that $L(s, \chi) = L(\chi|\cdot|^s)$ is a product of gamma factors and the Dirichlet series

$$L_f(s, \chi) = L_f(\chi|\cdot|^s) = \prod_{v \in V_f - S} \frac{1}{1 - \chi_v(\pi_v)|\pi_v|_v^s} = \sum_{\mathfrak{a}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ runs through ideals of $\mathcal{O}_K$ prime to $S$ and $\chi(\prod \mathfrak{p}_v^{a_v})$ denotes $\prod \chi_v(\pi_v)^{a_v}$. This notation is justified by the fact that $\chi_v(\pi_v)$ does not depend on the choice of $\pi_v$.

$L(\chi)$ converges absolutely to a holomorphic function without zeros for $\sigma(\chi) > 1$.

**Remark 2.3.10.** We have seen in Theorem 2.2.8 that for each connected component of $X(K_v^\times)$, $L(\chi_v) = \zeta(f_v, \chi_v)$ for some $f_v \in \mathcal{S}(K_v)$. Moreover, $f_v = \mathbf{1}_{\mathcal{O}_v}$ for all but finitely many $v$. Thus for each connected component of $X$, $L(\chi) = \zeta(f, \chi)$ with $f = \bigotimes_{v \in V} f_v \in \mathcal{S}(\mathbb{A}_K)$.

**Example 2.3.11.** We have

$$L(|\cdot|^s) = Z_K(s) = \Gamma_\mathbb{R}(s)^{r_1} \Gamma_\mathbb{C}(s)^{r_2} \zeta_K(s),$$

where

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

is the Dedekind zeta function of $K$.

**Example 2.3.12.** Let $\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. There exists a unique Hecke character $\chi_\mathbb{I} \colon \mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times \to \mathbb{C}^\times$ such that $\chi_\mathbb{I}(p_\mathbb{I}) = \chi(p)$ for all $p \nmid N$, where $p_\mathbb{I}$ is the image of $p$ under the embedding $\mathbb{Q}_p \to \mathbb{I}_\mathbb{Q}$. Note that for $x \in \mathbb{R}_{>0}^\times \times \hat{\mathbb{Z}}^\times$, $\chi_\mathbb{I}(x) = \bar{\chi}(\pi(x))$, where $\pi \colon \hat{\mathbb{Z}}^\times \to (\mathbb{Z}/N\mathbb{Z})^\times$ is the projection. Thus $1 = \chi_\mathbb{I}(-1) = \chi_{\mathbb{I},\mathbb{R}}(-1)\bar{\chi}(-1)$, so that $\chi_{\mathbb{I},\mathbb{R}} = \operatorname{sgn}^a$, where $a = 0, 1$ satisfies $\chi(-1) = (-1)^a$. Then

$$L(\chi_\mathbb{I}|\cdot|^s) = \Lambda(s, \chi) = \Gamma_\mathbb{R}(s + a) L(s, \chi),$$

where

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}} = \sum_{n=1}^\infty \chi(n) n^{-s}$$

is the Dirichlet $L$-function. Here $\chi$ is extended to a function $\chi \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ where $m$ is the conductor of $\chi$ and $\chi(n) = 0$ for $n \notin (\mathbb{Z}/m\mathbb{Z})^\times$.

**Corollary 2.3.13** (Hecke)**.** *Let $K$ be a number field. The Hecke $L$-function $L(\chi)$ extends to a meromorphic function on the space of Hecke characters, holomorphic except for simple poles at $\chi = 1$ and $\chi = |\cdot|$, satisfying the functional equation*

$$L(\chi) = \epsilon(\chi) L(\chi^\vee)$$

*where*

$$\epsilon(\chi) = \prod_{v\in V} \epsilon(\chi_v)$$

*in a holomorphic function without zeros, $\epsilon(\chi_v)$ being defined in Theorem 2.2.8. In particular, $Z_K(s)$ can be analytically continued to a meromorphic function on the complex plane, holomorphic except for simple poles at $s = 0$ and $s = 1$, satisfying the functional equation*

$$Z_K(s) = |\Delta_K|^{\frac{1}{2}-s} Z_K(1-s).$$

*Moreover, the residues of $Z_K(s)$ are $-\sqrt{|\Delta_K|}\mathrm{vol}$ at $s = 0$ and* vol *at $s = 1$.*

Note that $\epsilon(\chi_v) = 1$ for all but finitely many $v$. It follows from the functional equation that $L(\chi)$ has no zeros for $\sigma(\chi) < 0$.

*Proof.* Let $f$ be as in Remark 2.3.10. The assertion on meromorphic continuation follows from Theorem 2.3.8. The assertion on $\epsilon$ is obvious. By Theorem 2.2.8,

$$L(\chi_v^\vee)\epsilon(\chi_v) = \zeta(\hat{f}_v, \chi_v^\vee).$$

Taking product and applying (2.3.1), we get

$$L(\chi^\vee)\epsilon(\chi) = \zeta(\hat{f}, \chi^\vee) = \zeta(f, \chi) = L(\chi).$$

For the residues, it suffices to note that $f(0) = \sqrt{|\Delta_K|}$ and $\hat{f}(0) = 1$. □

**Corollary 2.3.14.** *The Dedekind zeta function $\zeta_K(s)$ extends to a meromorphic function on the complex place, holomorphic except for a simple pole at $s = 1$ with residue* vol*. Moreover $\zeta_K(s)$ has a zero of order $r = r_1 + r_2 - 1$ at $s = 0$ with leading term $-hR/w$.*

*Proof.* Indeed, $\Gamma_\mathbb{R}(1) = \Gamma_\mathbb{C}(1) = 1$, $\mathrm{res}_{s=0}\Gamma_\mathbb{R}(s) = 2$, $\mathrm{res}_{s=0}\Gamma_\mathbb{C}(s) = 2\pi$. □

**Corollary 2.3.15.** *Let $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character of conductor $N > 1$. Then $\Lambda(s, \chi)$ extends to an entire function, satisfying the functional equation*

$$\Lambda(s, \chi) = (-i)^a N^{-s} \tau(\chi)\Lambda(1-s, \bar{\chi}),$$

*where*

$$\tau(\chi) = \sum_{x\in(\mathbb{Z}/N\mathbb{Z})^\times} \chi(x)e(x/N)$$

*is the Gauss sum.*

*Proof.* We put $N = \prod_p p^{n_p}$. For $p \mid N$, we have $\chi_{\mathbb{I},p} = \chi_p|\cdot|_p^t$ with $\chi_p(p) = 1$, so that $\chi_{\mathbb{I},p}(p) = p^{-t}$. Moreover, $1 = \chi_\mathbb{I}(p) = \chi_{\mathbb{I},p}(p)\prod_{q|N/p^{n_p}} \chi_q(p)$. Thus

$$\epsilon(\chi_{\mathbb{I},p}|\cdot|_p^s) = (p^{n_p})^{-s-t}\tau(\overline{\chi_p}) = (p^{n_p})^{-s}\tau(\overline{\chi_p}) \prod_{q|N/p^{n_p}} \overline{\chi_q}(p)^{n_p},$$

where

$$\tau(\overline{\chi_p}) = \sum_{x\in(\mathbb{Z}/p^{n_p}\mathbb{Z})^\times} \overline{\chi_p}(x)e(x/p_p^n).$$

Therefore,

$$\epsilon(\chi_{\mathbb{I}}|\cdot|^s) = (-i)^a N^{-s} \prod_p \overline{\chi_p}(\frac{N}{p^{n_p}})\tau(\overline{\chi_p}).$$

For $x \in \mathbb{Z}/N\mathbb{Z}$, we write $x = \sum_p \frac{N}{p^{n_p}} x_p$. Then

$$\begin{aligned}\tau(\chi) = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(x)e(x/N) &= \sum_{x_p \in (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times} \chi(\sum \frac{N}{p^{n_p}} x_p) e(\sum x_p/p^{n_p}) \\ &= \sum_{x_p \in (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times} \prod_p \overline{\chi_p}(\frac{N}{p^{n_p}} x_p) e(x_p/p^{n_p}) = \prod_p \overline{\chi_p}(\frac{N}{p^{n_p}})\tau(\overline{\chi_p}).\end{aligned}$$

□

## Class number formula

Let $K$ be an abelian extension of $\mathbb{Q}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. In the next chapter, as a consequence of class field theory, we will prove the Kronecker-Weber Theorem, which says that $K$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_N)$. Recall that we have an isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ carrying $a$ to $\zeta_N \mapsto \zeta_N^a$. Via this isomorphism, characters of the quotient $G$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ can be viewed as Dirichlet characters.

**Proposition 2.3.16.** *We have* $\zeta_K(s) = \prod_{\chi \in \hat{G}} L(s, \chi)$.

*Proof.* It suffices to show that for every rational $p$, we have

$$\prod_{\mathfrak{p}|p} (1 - (N\mathfrak{p})^{-s}) = \prod_{\chi \in \hat{G}} (1 - \chi(p)p^{-s}),$$

where $\mathfrak{p}$ runs through prime ideals of $\mathcal{O}_K$ above $p$.

The left-hand side is $(1 - p^{-fs})^g$, where $g$ is the number of primes above $p$ and $f$ is the degree of the residue field extension.

Let $N = p^k m$ with $p \nmid m$. Note that $\mathbb{Q}(\zeta_m)$ is the maximal sub-extension of $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ in which $p$ is unramified. Let $K_0 = K \cap \mathbb{Q}(\zeta_m)$. Then $K_0$ is the maximal sub-extension of $K/\mathbb{Q}$ in which $p$ is unramified. For $\chi \in \hat{G}$, we have $\chi(p) \neq 0$ if and only if $\chi$ is a Dirichlet character of modulo $m$, or equivalently, if it $\chi$ factorizes through $G_0 := \mathrm{Gal}(K_0/\mathbb{Q})$. Thus

$$\prod_{\chi \in \hat{G}} (1 - \chi(p)p^{-s}) = \prod_{\chi \in \widehat{G_0}} (1 - \chi(p)p^{-s}).$$

The decomposition group $D_p < G_0$ is generated by the Frobenius $\sigma_p$, which is the image of $p$ under the isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. We have a short exact sequence $0 \to \widehat{G_0/D_p} \to \widehat{G_0} \to \widehat{D_p} \to 0$. Since $[G_0\colon D_p] = g$, each character of $D_p$ lifts to $g$ characters of $G_0$, so that we have

$$\prod_{\chi \in \widehat{G_0}} (1 - \chi(p)p^{-s}) = \prod_{\chi \in \widehat{D_p}} (1 - \chi(\sigma_p)p^{-s})^g = \prod_\xi (1 - \xi p^{-s})^g = (1 - p^{-fs})^g,$$

where $\xi$ runs through the $f$-th roots of unity. □

**Corollary 2.3.17.** *We have*

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|\Delta_K|}} = \prod_{\substack{\chi\in\hat{G}\\ \chi\neq 1}} L(1,\chi).$$

*Proof.* This follows from the proposition by taking residue at $s=1$. Indeed, by Corollary 2.3.14, the residue of $\zeta_K(s)$ at $s=1$ is the left hand side and the residue of $L(s,1)=\zeta(s)$ at $s=1$ is 1. □

The value $L(1,\chi)$ can be expressed explicitly.

**Proposition 2.3.18.** *Let* $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ *be a primitive Dirichlet character of conductor* $N>1$. *Then*

$$L(1,\chi) = \begin{cases} -\frac{1}{\tau(\bar\chi)}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\bar\chi(a)\log|1-\zeta_N^a| & \chi(-1)=1,\\ -\frac{\pi i}{N\tau(\bar\chi)}\sum_{a=1}^{N-1}\bar\chi(a)a & \chi(-1)=-1,\end{cases}$$

*where*

$$\tau(\bar\chi) = \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\bar\chi(a)\zeta_N^a$$

*is the Gauss sum.*

*Proof.* For $N\nmid a$, the sum

$$\sum_{n=1}^\infty \frac{\zeta_N^{an}}{n^s} = \sum_{m=1}^\infty\sum_{b=1}^N \frac{\zeta_N^{ab}}{mN+b^s} = \sum_{m=1}^\infty\sum_{b=1}^N \zeta_N^{ab}\left(\frac{1}{mN+b^s}-\frac{1}{mN+N^s}\right)$$

converges (conditionally) to a homomorphic function on $\mathrm{Re}(s)>0$. We have

$$\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\bar\chi(a)\sum_{n=1}^\infty\frac{\zeta_N^{an}}{n^s} = \sum_{n=1}^\infty\frac{1}{n^s}\left(\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\bar\chi(a)\zeta_N^{an}\right) = \tau(\bar\chi)\sum_{n=1}^\infty\frac{\chi(n)}{n^s} = \tau(\bar\chi)L(s,\chi).$$

Here we used the fact $\sum_{a\in(\mathbb{Z}/N\mathbb{Z})}\bar\chi(a)\zeta_N^{an}=0$ for $(n,N)>1$. Letting $s\to 1^+$, we get

$$\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\bar\chi(a)\sum_{n=1}^\infty\frac{\zeta_N^{an}}{n} = \tau(\bar\chi)L(1,\chi).$$

Note that for $1\le a\le N-1$, we have

$$\sum_{n=1}^\infty\frac{\zeta_N^{an}}{n} = -\log(1-\zeta_N^a) = -\log|1-\zeta_N^a| - \pi i\left(\frac{a}{N}-\frac{1}{2}\right).$$

Thus

$$-\tau(\bar\chi)L(1,\chi) = \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\bar\chi(a)\log|1-\zeta_N^a| + \frac{\pi i}{N}\sum_{a=1}^{N-1}\bar\chi(a)a.$$

The first (resp. second) term of the right-hand side vanishes if $\chi(-1)=-1$ (resp. $\chi(-1)=1$). □

# Chapter 3

# Class field theory

## 3.1 Main statements

**Theorem 3.1.1.** *Let $F$ be a local field of characteristic zero. Then $E \mapsto N_{E/F}(E^\times)$ induces a bijection from the set of isomorphism classes of finite abelian extensions of $F$ to the set of open subgroups of $F^\times$ of finite indices. Moreover, for each $E$, we have a canonical isomorphism*

$$r_{E/F} \colon \mathrm{Gal}(E/F) \xrightarrow{\sim} F^\times/N_{E/F}(E^\times).$$

Note that subgroups of $F^\times$ of finite exponents are automatically open (exercise). This fails however for local fields of positive characteristic.

**Theorem 3.1.2.** *Let $F$ be a number field. Then $E \mapsto N_{E/F}(\mathbb{I}_E)F^\times/F^\times$ induces a bijection from the set of isomorphism classes of finite abelian extensions of $F$ to the set of open subgroups of $\mathbb{I}_F/F^\times$. Moreover, for each $E$, we have a canonical isomorphism*

$$r_{E/F} \colon \mathrm{Gal}(E/F) \simeq \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E).$$

By the compactness of $\mathbb{I}_F^1/F^\times$, open subgroups of $\mathbb{I}_F/F^\times$ are of finite indices. Equivalently, $E \mapsto F^\times N_{E/F}(\mathbb{I}_E)$ induces a bijection to the set of open subgroups of $\mathbb{I}_F$ (of finite indices) containing $F^\times$.

The local and global theories are compatible.

### Absolute Galois groups

Let $G$ be a Hausdorff topological group. The *abelianization* $G^{\mathrm{ab}}$ of $G$ is the maximal Hausdorff quotient group, or equivalently, the quotient of $G$ by the closure of $[G, G]$. The *profinite completion* $\hat{G}$ of $G$ is the limit $\lim G/H$ of finite discrete quotients of $G$, where $H$ runs through open subgroups of $G$ of finite indices. For any field $F$ of separable closure $\bar{F}$, the abelianization of the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$ of $F$ can be identified with $\mathrm{Gal}(F^{\mathrm{ab}}/F)$, where $F^{\mathrm{ab}}$ is the maximal abelian extension of $F$.

**Corollary 3.1.3.** *Let $F$ be a local field of characteristic zero. Then we have a canonical isomorphism*

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \simeq \widehat{F^\times}.$$

If $F$ is a finite extension of $\mathbb{Q}_p$, we have split short exact sequences

$$\begin{tikzcd}
1 \arrow[r] & U_F \arrow[r] \arrow[d, equal] & F^\times \arrow[r, "v_F"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & U_F \arrow[r] & \widehat{F^\times} \arrow[r] & \hat{\mathbb{Z}} \arrow[r] & 0.
\end{tikzcd}$$

**Corollary 3.1.4.** *Let $F$ be a number field. Then we have a canonical isomorphism*

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \simeq \widehat{\mathbb{I}_F/F^\times}.$$

The profinite completion of $C = \mathbb{I}_F/F^\times$ can be identified with the quotient $C/D$, where $D$ denotes the identity component of $C$.

## Local class field theory

For Archimedean local fields, the statement is trivial. Indeed, the only nontrivial extension in this case is $\mathbb{C}/\mathbb{R}$ and $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \{\pm 1\} \simeq \mathbb{R}^\times/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$.

Let $F$ be a finite extension of $\mathbb{Q}_p$. We let $k_F$ denote the residue field of $F$. Let $\pi_F$ be a uniformizer of $F$. We have $F^\times = \pi_F^{\mathbb{Z}} \times U_F$, where $U_F = \mathcal{O}_F^\times$.

For any integer $f \geq 1$, there exists an unramified extension $E$ of $F$ of degree $f$, unique up to isomorphisms. Recall that $E$ is a cyclic extension of $F$. Indeed, $E$ is the splitting field of the polynomial $X^{q_F^f} - 1$ over $F$, where $q_F = \# k_F$. The canonical map $\mathrm{Gal}(E/F) \to \mathrm{Gal}(k_E/k_F)$ is an isomorphism and $\mathrm{Gal}(k_E/k_F)$ is a cyclic group of order $f$ generated by the Frobenius substitution $x \mapsto x^{q_F}$. The corresponding element of $\mathrm{Gal}(E/F)$ is also called the Frobenius substitution and denoted $\mathrm{Frob}_{E/F}$. Note that $\pi_F$ is also a uniformizer of $E$. Thus $E^\times = \pi_F^{\mathbb{Z}} \times U_E$. Since $N_{E/F}(U_E) = U_F$ (exercise), $N_{E/F}(E^\times) = \pi_F^{f\mathbb{Z}} \times U_F$. Therefore, $F^\times/N_{E/F}(E^\times)$ is a cyclic group of order $f$ generated by the image of $\pi_F$, which does not depend on the choice of $\pi_F$.

More generally, for a finite extension $E$ of $F$, $N_{E/F}(E^\times)$ is an open subgroup of $F^\times$ (exercise) of finite index. We have a morphism of short exact sequences

$$\begin{tikzcd}
1 \arrow[r] & U_E \arrow[r] \arrow[d, "N_{E/F}"'] & E^\times \arrow[r, "v_E"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, "\times f"] & 0 \\
1 \arrow[r] & U_F \arrow[r] & F^\times \arrow[r, "v_F"] & \mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

where $f = [k_E : k_F]$. Indeed, $v_E(N_{E/F}(\pi_E)) = d = [E : F]$, so that $v_F(N_{E/F}(\pi_E)) = f$. By the snake lemma, we obtain a short exact sequence

$$1 \to U_F/N_{E/F}(U_E) \to F^\times/N_{E/F}(E^\times) \xrightarrow{v_F} \mathbb{Z}/f\mathbb{Z} \to 0.$$

If $E/F$ is a Galois extension, we have a short exact sequence

$$1 \to I \to \mathrm{Gal}(E/F) \to \mathrm{Gal}(k_E/k_F) \to 1,$$

where $I$ is the inertia group.

**Theorem 3.1.5** (Reciprocity)**.** *There exists a unique way to define, for every finite Galois extension $E/F$ of local fields of characteristic zero, an isomorphism*

$$r_{E/F}\colon \mathrm{Gal}(E/F)^{\mathrm{ab}} \xrightarrow{\sim} F^\times/N_{E/F}(E^\times),$$

*satisfying the following properties.*

(1) *(Normalization) For $E/F$ unramified and $F$ non-Archimedean, $r_{E/F}(\mathrm{Frob}_{E/F}) = \pi_F N_{E/F}(E^\times)$.*

(2) *(Functoriality) For finite Galois extensions $E/F$ and $E'/F'$ and an embedding $\tau\colon E \hookrightarrow E'$ such that $\tau(F) \subseteq F'$, the diagram*

$$\begin{tikzcd}
\mathrm{Gal}(E'/F')^{\mathrm{ab}} \arrow[r, "r_{E'/F'}", "\sim"'] \arrow[d] & F'^\times/N_{E'/F'}(E'^\times) \arrow[d, "N_{F'/F}"] \\
\mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[r, "r_{E/F}", "\sim"'] & F^\times/N_{E/F}(E^\times)
\end{tikzcd}$$

*commutes. Here the left vertical arrow is induced by the homomorphism* $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$ *given by restriction by $\tau$.*

**Notation 3.1.6.** For $x \in F^\times$, the *norm residue symbol* is defined to be

$$(x, E/F) = r_{E/F}^{-1}(xN_{E/F}(E^\times)).$$

**Example 3.1.7.** The following three special cases of Property (2) above will be of use.

(a) Assume that $\tau\colon E \xrightarrow{\sim} E'$ is an isomorphism of local fields, and $F' = \tau(F)$. Then the diagram

$$\begin{tikzcd}
\mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[r, "r_{E/F}", "\sim"'] \arrow[d, "\simeq"] & F^\times/N_{E/F}(E^\times) \arrow[d, "\tau", "\simeq"'] \\
\mathrm{Gal}(E'/F')^{\mathrm{ab}} \arrow[r, "r_{E'/F'}", "\sim"'] & F'^\times/N_{E'/F'}(E'^\times)
\end{tikzcd}$$

commutes. Here the left vertical arrow is induced by the isomorphism

$$\mathrm{Gal}(E/F) \xrightarrow{\sim} \mathrm{Gal}(E'/F') \quad \sigma \mapsto \tau\sigma\tau^{-1}.$$

(b) Case $E = E'$, $\tau = \mathrm{id}_E$. Then $\mathrm{Gal}(E/F') \subseteq \mathrm{Gal}(E/F)$ and the following diagram commutes

$$\begin{tikzcd}
\mathrm{Gal}(E/F')^{\mathrm{ab}} \arrow[r, "r_{E/F'}", "\sim"'] \arrow[d] & F'^\times/N_{E/F'}(E^\times) \arrow[d, "N_{F'/F}"] \\
\mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[r, "r_{E/F}", "\sim"'] & F^\times/N_{E/F}(E^\times).
\end{tikzcd}$$

(c) Case where $F = F'$ and $\tau$ is an inclusion $E \subseteq E'$. Then the diagram

$$\begin{tikzcd}
\mathrm{Gal}(E'/F)^{\mathrm{ab}} \arrow[r, "r_{E'/F}", "\sim"'] \arrow[d] & F^\times/N_{E'/F}(E'^\times) \arrow[d] \\
\mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[r, "r_{E/F}", "\sim"'] & F^\times/N_{E/F}(E^\times)
\end{tikzcd}$$

commutes. Here the left vertical arrow is induced by the surjection $\mathrm{Gal}(E'/F) \to \mathrm{Gal}(E/F)$ given by restriction, and the right vertical arrow is induced by $\mathrm{id}_F$. The vertical arrows are surjections.

*Proof of the uniqueness in Theorem 3.1.5.* The Archimedean case is trivial. In the non-Archimedean case, let $\sigma \in G = \mathrm{Gal}(E/F)$. We want to show that $r_{E/F}(\sigma[G,G])$ is uniquely determined by (1) and (2). Let $E'$ be a finite unramified extension of $E$. Then $E'/F$ is a Galois extension and we have a morphism of short exact sequences of groups

$$\begin{tikzcd}
1 \arrow[r] & I \arrow[r] \arrow[d, equal] & \mathrm{Gal}(E'/F) \arrow[r] \arrow[d] & \mathrm{Gal}(k_{E'}/k_F) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I \arrow[r] & \mathrm{Gal}(E/F) \arrow[r] & \mathrm{Gal}(k_E/k_F) \arrow[r] & 1.
\end{tikzcd}$$

It follows that $\mathrm{Gal}(E'/F) \simeq \mathrm{Gal}(k_{E'}/k_F) \times_{\mathrm{Gal}(k_E/k_F)} \mathrm{Gal}(E/F)$. The order of the image $\bar\sigma \in \mathrm{Gal}(k_E/k_F)$ of $\sigma$ divides the order $m$ of $\sigma$. We may choose $E'$ so that there exists a lifting $\bar\sigma' \in \mathrm{Gal}(k_{E'}/k_F)$ of $\bar\sigma$ of order $m$. Then $\sigma' = (\bar\sigma', \sigma) \in \mathrm{Gal}(E'/F)$ has order $m$, so that $E'$ is unramified over $E'^{\sigma'} = \{x \in E' \mid \sigma'(x) = x\}$. By (2), $r_{E/F}(\sigma[G,G]) = N_{E'^{\sigma'}/F}(r_{E'/E'^{\sigma'}}(\sigma'))$, where $r_{E'/E'^{\sigma'}}(\sigma')$ is determined by (1). □

Let $F$ be a local field of characteristic zero. For a finite extension $E/F$, we let $\mathcal{N}_E = N_{E/F}(E^\times) \subseteq F^\times$. For an extension $E'$ of $E$ such that $E'/F$ is a finite abelian extension, $\mathcal{N}_E \supseteq \mathcal{N}_{E'}$. Theorem 3.1.5 has the following consequence.

**Corollary 3.1.8.** *Let $E$ and $E'$ be finite abelian extensions of $F$. Then*

$$\mathcal{N}_{EE'} = \mathcal{N}_E \cap \mathcal{N}_{E'}.$$

Recall that for Galois extensions $K$ and $K'$ of $F$,

$$\mathrm{Gal}(KK'/F) = \mathrm{Gal}(K/F) \times_{\mathrm{Gal}(K\cap K'/F)} \mathrm{Gal}(K'/F).$$

Thus $KK'/F$ is abelian if and only if $K/F$ and $K'/F$ are both abelian.

*Proof.* This follows from the above description of the Galois group as a fiber product and the functoriality of reciprocity. More precisely, we have $\mathcal{N}_{EE'} \subseteq \mathcal{N}_E \cap \mathcal{N}_{E'}$. Conversely, for $x \in \mathcal{N}_E \cap \mathcal{N}_{E'}$, we want to show that its image $\bar x \in F^\times/\mathcal{N}_{EE'}$ is trivial. We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(E/F) \arrow[d, "r_{E/F}"', "\simeq"] & \mathrm{Gal}(EE'/F) \arrow[l] \arrow[r] \arrow[d, "r_{EE'/F}"', "\simeq"] & \mathrm{Gal}(E'/F) \arrow[d, "r_{E'/F}"', "\simeq"] \\
F^\times/\mathcal{N}_E & F^\times/\mathcal{N}_{EE'} \arrow[l] \arrow[r] & F^\times/\mathcal{N}_{E'}.
\end{tikzcd}$$

Let $\sigma = r_{EE'/F}^{-1}(\bar x)$. Then the restriction $\sigma_E$ of $\sigma$ to $E$ is the identity, because $r_{E/F}(\sigma_E) = 1$. Similarly, the restriction $\sigma_{E'}$ of $\sigma$ to $E'$ is the identity. It follows that $\sigma = \mathrm{id}_{EE'}$, so that $\bar x = 1$. □

**Corollary 3.1.9.** *For $E$ and $E'$ as above, $\mathcal{N}_E \supseteq \mathcal{N}_{E'}$ if and only if $E'$ is an extension of $E$. Moreover, $\mathcal{N}_E = \mathcal{N}_{E'}$ if and only if $E/F$ and $E'/F$ are isomorphic.*

*Proof.* The "if" part if the first assertion is trivial. Conversely, $\mathcal{N}_E \supseteq \mathcal{N}_{E'}$ implies $\mathcal{N}_{EE'} = \mathcal{N}_E \cap \mathcal{N}_{E'} = \mathcal{N}_{E'}$, which implies $[EE' : F] = [E' : F]$, which implies $EE' = E'$, which means that $E'$ is an extension of $E$. The second assertion follows from the first one. □

**Remark 3.1.10.** For any finite extension $E/F$ of finite extensions of $\mathbb{Q}_p$, if $F'/F$ is the maximal unramified sub-extension, then $k_{F'} = k_E$, so that $\mathcal{N}_{F'} = U_F\mathcal{N}_E$. Indeed, we have $\mathcal{N}_{F'} \supseteq U_F\mathcal{N}_E$, and both groups have index $f = [k_E : k_F]$ in $F^\times$.

Thus, by Corollary 3.1.9, a finite *abelian* extension $E/F$ of finite extensions of $\mathbb{Q}_p$ is unramified if and only if $\mathcal{N}_E \supseteq U_F$. More generally, for $E/F$ finite abelian, the compatibility of $r_{E/F}$ and $r_{F'/F}$ provides an isomorphism of short exact sequences

$$\begin{tikzcd} 1 \arrow[r] & I \arrow[r] \arrow[d, "\simeq"'] & \mathrm{Gal}(E/F) \arrow[r] \arrow[d, "\simeq"', "r_{E/F}"] & \mathrm{Gal}(k_E/k_F) \arrow[r] \arrow[d, "\simeq"] & 1 \\ 1 \arrow[r] & U_F/N_{E/F}(U_F) \arrow[r] & F^\times/N_{E/F}(E^\times) \arrow[r, "v_F"] & \mathbb{Z}/f\mathbb{Z} \arrow[r] & 0, \end{tikzcd} \tag{3.1.1}$$

where the vertical arrow on the right carries Frobenius to the class of 1.

**Example 3.1.11** (Cyclotomic extensions of $\mathbb{Q}_p$)**.** Let $F = \mathbb{Q}_p$. Let $m = p^d n$, $(p, n) = 1$. We have $\mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p(\zeta_{p^d})\mathbb{Q}_p(\zeta_n)$, so that $\mathcal{N}_{\mathbb{Q}_p(\zeta_m)} = \mathcal{N}_{\mathbb{Q}_p(\zeta_n)} \cap \mathcal{N}_{\mathbb{Q}_p(\zeta_{p^d})}$. Note that $\mathbb{Q}_p(\zeta_{p^d})$ is purely ramified of degree $\phi(p^d)$ over $\mathbb{Q}_p$, and $\mathcal{N}_{\mathbb{Q}_p(\zeta_p^d)} = p^{\mathbb{Z}}(1 + p^d\mathbb{Z}_p)$ for $d \geq 1$ (exercise). Moreover, $\mathbb{Q}_p(\zeta_n)$ is unramified of degree $\alpha$ over $\mathbb{Q}_p$, where $\alpha$ is the order of $p$ modulo $n$, so that $\mathcal{N}_{\mathbb{Q}(\zeta_n)} = p^{\alpha\mathbb{Z}}\mathbb{Z}_p^\times$. Note that every open subgroup of $\mathbb{Q}_p^\times$ of finite index contains $\mathcal{N}_{\mathbb{Q}_p(\zeta_m)}$ for some $m$. By Corollary 3.1.9, we obtain the following.

**Theorem 3.1.12.** *Every finite abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_m)$ for some $m$.*

Corollary 3.1.9 implies that the map $E \mapsto \mathcal{N}_E$ is injective. The surjectivity can be stated as follows.

**Theorem 3.1.13** (Existence)**.** *Let $F$ be a local field of characteristic zero. Every open subgroup of finite index of $F^\times$ is of the form $\mathcal{N}_E$ for some finite abelian extension $E$ of $F$.*

**Corollary 3.1.14.** *For finite abelian extensions $E$ and $E'$ of $F$,*

$$\mathcal{N}_{E\cap E'} = \mathcal{N}_E\mathcal{N}_{E'}.$$

*Proof.* Clearly $\mathcal{N}_{E\cap E'} \supseteq \mathcal{N}_E\mathcal{N}_{E'}$. By the existence theorem, there exists $K$ such that $\mathcal{N}_E\mathcal{N}_{E'} = \mathcal{N}_K$. Then $K$ is an extension of $E \cap E'$. But $\mathcal{N}_K \supseteq \mathcal{N}_E$ and $\mathcal{N}_K \supseteq \mathcal{N}_{E'}$, so that $E$ and $E'$ are extensions of $K$. Therefore, $K \simeq E \cap E'$, so that $\mathcal{N}_K = \mathcal{N}_{E\cap E'}$. □

**Remark 3.1.15.** Taking limit in (3.1.1), we obtain an isomorphism of short exact sequences

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(F^{\mathrm{ab}}/F^{\mathrm{ur}}) \arrow[r] \arrow[d, "\simeq"'] & \mathrm{Gal}(F^{\mathrm{ab}}/F) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Gal}(\overline{k_F}/k_F) \arrow[r] \arrow[d, "\simeq"] & 1 \\ 1 \arrow[r] & U_F \arrow[r] & \widehat{F^\times} \arrow[r] & \hat{\mathbb{Z}} \arrow[r] & 0, \end{tikzcd} \tag{3.1.2}$$

where $F^{\mathrm{ur}}$ is the maximal unramified extension of $F$, and the vertical arrow on the right carries Frobenius to 1.

## Global class field theory

Let $F$ be a number field. Let $E$ be a finite extension of $F$. For any place $v$ of $F$,

$$F_v \otimes_F E \simeq \prod_{w|v} E_w. \tag{3.1.3}$$

We have

$$\mathbb{A}_F \otimes_F E \simeq \mathbb{A}_E. \tag{3.1.4}$$

Trace and norm maps $\mathrm{tr}_{E/F}\colon E \to F$, $N_{E/F}\colon E^\times \to F^\times$ induce via (3.1.4) $\mathrm{tr}_{E/F}\colon \mathbb{A}_E \to \mathbb{A}_F$, $N_{E/F}\colon \mathbb{I}_E \to \mathbb{I}_F$, fitting into the commutative diagrams

$$\begin{tikzcd} E \arrow[r] \arrow[d, "\mathrm{tr}_{E/F}"'] & \mathbb{A}_E \arrow[d, "\mathrm{tr}_{E/F}"] \\ F \arrow[r] & \mathbb{A}_F \end{tikzcd} \qquad \begin{tikzcd} E^\times \arrow[r] \arrow[d, "N_{E/F}"'] & \mathbb{I}_E \arrow[d, "N_{E/F}"] \\ F^\times \arrow[r] & \mathbb{I}_F, \end{tikzcd}$$

where the horizontal arrows are diagonal embeddings. We have

$$(\mathrm{tr}_{E/F}(x))_v = \sum_{w|v} \mathrm{tr}_{E_w/F_v}(x_w), \quad (N_{E/F}(x))_v = \prod_{w|v} N_{E_w/F_v}(x_w).$$

Note that $N_{E/F}(\mathbb{I}_E) \supseteq \prod_v U_v$, $v$ running through finite places of $F$ unramified in $E$, thus $N_{E/F}(\mathbb{I}_E)$ is an open subgroup of $\mathbb{I}_F$. It follows that $F^\times N_{E/F}(\mathbb{I}_E)$ is an open subgroup of $\mathbb{I}_F$ (of finite index) containing $F^\times$.

Let $E$ be a finite Galois extension of $F$ of group $G$. Then $G$ acts on the set of places $w$ of $E$: $|x|_{\sigma(w)} := |\sigma^{-1}(x)|_w$. Note that $w|_F = \sigma w|_F$. Let $v = w|_F$. The decomposition group $D(w/v) \subseteq G$ is by definition the stabilizer of $w$. We have $D(w/v) \simeq \mathrm{Gal}(E_w/F_v)$ and $D(\sigma w/v) = \sigma D(w/v)\sigma^{-1}$. The isomorphisms (3.1.3) and (3.1.4) are $G$-equivariant. On the right hand side, $G$ acts as follows. For $\sigma \in G$, $(\sigma x)_{\sigma w} = \sigma_w x_w$, where $\sigma_w\colon E_w \to E_{\sigma w}$. Comparing $G$-invariants on both sides, we see that $G$ acts transitively on the set of places of $E$ above $v$. If $v$ is a finite place unramified in $E$, then we have $\mathrm{Frob}_{E_w/F_v} \in G$, whose conjugacy class $\mathrm{Frob}_v$ does not depend on $w$.

Let $E$ be a finite Galois extension of $F$. For a place $v$ of $F$ and a place $w$ of $E$ above $v$, the homomorphism

$$F_v^\times \to F_v^\times/N_{E_w/F_v}(E_w^\times) \xrightarrow[\sim]{(-,E_w/F_v)} \mathrm{Gal}(E_w/F_v)^{\mathrm{ab}} \to \mathrm{Gal}(E/F)^{\mathrm{ab}} \tag{3.1.5}$$

does not depend on the choice of $w$. Moreover, if $v$ is a finite place unramified in $E/F$ and $x_v \in U_{F_v}$, its image in $\mathrm{Gal}(E/F)^{\mathrm{ab}}$ is trivial. We thus obtain a continuous homomorphism

$$\mathbb{I}_F \to \mathrm{Gal}(E/F)^{\mathrm{ab}}, \tag{3.1.6}$$

trivial on $N_{E/F}(\mathbb{I}_E)$, such that the composition with the inclusion $F_v^\times \to \mathbb{I}_F$ is (3.1.5). We let $(x, E/F)$ denote the image of $x$ under (3.1.6) and we call it the *norm residue symbol.*

**Theorem 3.1.16** (Artin reciprocity). *Let $E/F$ be a finite Galois extension of number fields. The homomorphism* (3.1.6) *is trivial on $F^\times$ and induces an isomorphism*

$$\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E) \xrightarrow{\sim} \mathrm{Gal}(E/F)^{\mathrm{ab}}.$$

**Remark 3.1.17.**
1. It follows from the functoriality of local reciprocity that Artin reciprocity also satisfies functoriality.
2. Note that the map (3.1.6) is uniquely determined by the fact that it is a continuous homomorphism trivial on $F^\times$ and $U_v$, and sending $\pi_v$ to the image of $\mathrm{Frob}_v$, for all (or all but finitely many) unramified finite places $v$ of $F$.

For a finite extension $E$ of $F$, we write $\mathcal{N}_E = F^\times N_{E/F}(\mathbb{I}_E)$. Corollary 3.1.8 holds with the same proof. More precisely, for $E/F$ and $E'/F$ abelian, $\mathcal{N}_{EE'} = \mathcal{N}_E \cap \mathcal{N}_{E'}$, so that $E'$ is an extension of $E$ if and only if $\mathcal{N}_{E'} \supseteq \mathcal{N}_E$. In particular, $E/F$ and $E'/F$ are isomorphic if and only if $\mathcal{N}_E = \mathcal{N}_{E'}$.

**Remark 3.1.18.** For $E/F$ abelian, the map $\mathrm{Gal}(E_w/F_v) \to \mathrm{Gal}(E/F)$ is injective. In this case, the first assertion of Theorem 3.1.16 can be stated as follows: for $x \in F^\times$, $\prod_v (x, E_w/F_v) = 1$, where $v$ runs through all places of $v$. Moreover, this implies, for every place $v$ of $F$, the injectivity of the map $F_v^\times/N_{E_w/F_v}(E_w^\times) \to \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)$. In other words,

$$F_v^\times \cap F^\times N_{E/F}(\mathbb{I}_E) = N_{E_w/F_v}(E_w^\times).$$

It follows that a finite place $v$ of $F$ is unramified in $E$ if and only if $\mathcal{N}_E \supseteq U_{F_v}$.

**Theorem 3.1.19** (Existence). *Let $F$ be a number field. Every open subgroup of $\mathbb{I}_F$ (of finite index) containing $F^\times$ is of the form $\mathcal{N}_E$ for some finite abelian extension $E$ of $F$.*

$E$ is called the *class field* of $\mathcal{N}_E$.

Corollary 3.1.14 holds with the same proof. More precisely, for finite abelian extensions $E/F$ and $E'/F$, we have $\mathcal{N}_{E\cap E'} = \mathcal{N}_E\mathcal{N}_{E'}$.

## Ideal-theoretic formulation

We can reformulate global class field theory in terms of ideals via the isomorphism (1.5.1). Let $F$ be a number field and let $E$ be a finite Galois extension of $F$. Let $m$ be a modulus for $F$ such that $v$ is unramified in $E$ for every finite place satisfying $m(v) = 0$. We consider the homomorphism

$$\mathcal{I}_F(m) \to \mathrm{Gal}(E/F)^{\mathrm{ab}} \tag{3.1.7}$$

carrying $\mathfrak{p}_v$ for $m(v) = 0$ to the image of $\mathrm{Frob}_{w/v}$, for a place $w$ of $E$ above $v$. We let $\left(\frac{E/F}{\mathfrak{a}}\right)$ denote the image of $\mathfrak{a}$ under this homomorphism and we call it the *Artin symbol*. We let $\mathcal{I}_E(m) \subseteq \mathcal{I}_E$ denote the subgroup of fractional ideals generated by $\mathfrak{p}_w$ such that $m(w|_F) = 0$. The homomorphism (3.1.7) is trivial on $N_{E/F}(\mathcal{I}_E(m))$.

**Theorem 3.1.20** (Artin reciprocity)**.** *Let $E/F$ be a finite Galois extension of number fields. There exists a modulus $m$ for $F$ such that $v$ is unramified in $E$ for every finite place satisfying $m(v) = 0$, and such that* (3.1.7) *is trivial on $\mathcal{P}_F(m)$ and induces an isomorphism*

$$\mathcal{I}_F(m)/\mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m)) \xrightarrow{\sim} \mathrm{Gal}(E/F)^{\mathrm{ab}}.$$

*Proof.* Note that for $m = (\mathfrak{a}, (m_v)_v)$, we may equip $E$ with the modulus $m' = (\mathfrak{a}\mathcal{O}_E, (m_{w|F})_w)$. Since the isomorphism (1.5.1) is compatible with $N_{E/F}$, we have

$$\mathcal{I}_F(m)/\mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m)) \simeq \mathbb{I}_F/F^\times U_{F,m}N_{E/F}(\mathbb{I}_E).$$

The open subgroup $N_{E/F}(\mathbb{I}_E)$ of $\mathbb{I}_F$ contains $U_{F,m}$ for $m$ big enough, and we conclude by Theorem 3.1.16. □

**Definition 3.1.21.** Let $m$ be a modulus for $F$. The *ray class field* of $F$ modulo $m$, denoted by $F^m$, is the class field of $F^\times U_{F,m}$. The *Hilbert class field $H_F$* is the ray class field modulo $m = (\mathcal{O}_F, 0)$ (in other words, $m$ constant of value 0).

Artin reciprocity provides isomorphisms

$$\mathcal{C}l_F(m) \xrightarrow{\sim} \mathrm{Gal}(F^m/F), \quad \mathcal{C}l_F \xrightarrow{\sim} \mathrm{Gal}(H_F/F).$$

Recall that $U_{F,m} = \prod_v U_v^{(m_v)}$, where $U_v^{(0)} = F_v^\times$ for $v$ Archimedean, $U_v^{(1)} = \mathbb{R}_{>0}^\times$ for $v$ real, $U_v^{(0)} = U_v$ for $v$ finite, and $U_v^{(n)} = 1 + \pi_v^n\mathcal{O}_v$ for $v$ finite and $n \geq 1$. For $m \leq m'$ (namely $m_v \leq m'_v$ for all places $v$ of $F$), $U_{F,m} \supseteq U_{F,m'}$, so that $F^{m'}$ is an extension of $F^m$.

**Theorem 3.1.22.** *Every finite abelian extension $E$ of $F$ is contained in a ray class field $F^m$. Moreover, there exists a smallest modulus $\mathfrak{f}$ for $F$ such that $E$ is contained in $F^{\mathfrak{f}}$.*

*Proof.* Indeed, $E$ is contained in $F^m$ if and only if $U_{F,m} \subseteq \mathcal{N}_E$. The first assertion then follows from the fact that every open subgroup of $\mathbb{I}_F$ contains $U_{F,m}$ for some $m$. The second assertion is obvious, with $\mathfrak{f}_v$ being the least integer $n$ such that $U_{F_v}^{(n)} \subseteq \mathcal{N}_E$. □

**Definition 3.1.23.** Let $E/F$ be a finite abelian extension. The smallest modulus $\mathfrak{f}$ such that $E$ is contained in $F^{\mathfrak{f}}$ is called the *conductor* of $E/F$.

For $E/F$ finite abelian, the conclusion of Theorem 3.1.20 holds for every $m \geq \mathfrak{f}$. By Remark 3.1.18, we have the following.

**Proposition 3.1.24.** *Let $E/F$ be a finite abelian extension of conductor $\mathfrak{f}$. Then for every place $v$ of $F$, $\mathfrak{f}_v$ is the least integer $n$ such that $U_{F_v}^{(n)} \subseteq N_{E_w/F_v}(E_w^\times)$, where $w$ is a place of $E$ above $v$. In particular, $v$ ramifies in $E$ if and only if $\mathfrak{f}_v > 0$.*

For Archimedean places, we use the convention that $\mathbb{C}$ is ramified over $\mathbb{R}$. For a real place $v$ of $F$, $\mathfrak{f}_v = 0$ if and only if $v$ splits in $w$.

One can show that the finite part of $\mathfrak{f}(E/F)$ divides the discriminant $\mathfrak{d}(E/F)$.

**Corollary 3.1.25.** *The Hilbert class field $H_F$ is the maximal unramified abelian extension of $F$.*

The proof of the following theorem uses transfer, and will be given later.

**Theorem 3.1.26** (Principal ideal). *For every ideal $\mathfrak{a}$ of $\mathcal{O}_F$, $\mathfrak{a}\mathcal{O}_{H_F}$ is principal.*

**Remark 3.1.27.** Let $m$ be a modulus for $F$. By the above, a place $v$ of $F$ is ramified in $F^m$ if and only if $m_v > 0$. Now let $v$ be a finite place with $m_v = 0$, hence unramified. By Artin reciprocity, the degree $f(w/v)$ of the residue field extension of a place $w$ of $F^m$ above $v$ equals the order of $\mathfrak{p}_v$ in the ray class group $\mathcal{C}l_F(m)$. In particular, $\mathfrak{p}_v$ splits in $F^m$ if and only if $\mathfrak{p}_v \in \mathcal{P}_F(m)$.

We note that $\mathfrak{f}(F^m/F) \leq m$. Equality does not always hold, because it may happen that $F^m = F^{m'}$ for $m \lneq m'$, as shown by the following.

**Example 3.1.28.** Let $F = \mathbb{Q}$ and let $n \geq 1$ be an integer. We consider the modulus $m = ((n), 1)$ for $\mathbb{Q}$. We have $\mathcal{N}_{\mathbb{Q}(\zeta_n)} \supseteq \mathbb{Q}^\times U_{\mathbb{Q},m}$, where $U_{\mathbb{Q},m} = \mathbb{R}^\times_{>0} \prod_{p\nmid n} \mathbb{Z}_p^\times \prod_{p\mid n}(1 + p^{v_p(n)}\mathbb{Z}_p)$. Thus $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}^m$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathcal{C}l_{\mathbb{Q}}(m)$, we get $\mathbb{Q}^m = \mathbb{Q}(\zeta_n)$. Note that $\mathbb{Q} = \mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2)$.

Since any modulus is of the form $((n), 0)$ or $((n), 1)$, Theorem 3.1.22 in this case takes the following form.

**Theorem 3.1.29** (Kronecker-Weber). *Every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some $n$.*

The problem of explicit construction of abelian extensions of number fields is known as Kronecker's *Jugendtraum* or Hilbert's 12th problem. The theory of complex multiplication solves this for imaginary quadratic fields and more generally CM fields. The problem for more general number fields remains open.

Let us give a direct proof of the Kronecker-Weber theorem for quadratic fields.

**Proposition 3.1.30.** *Let $m \neq 0, 1$ be a square-free integer and let $n = |\Delta|$, where $\Delta$ is the discriminant of $\mathbb{Q}(\sqrt{m})$. Then $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_n)$.*

Recall

$$\Delta = \begin{cases} m & m \equiv 1 \mod 4 \\ 4m & m \equiv 2, 3 \mod 4. \end{cases}$$

*Proof.* We write $\Delta = 2^r m'$ with $m'$ odd. We define a primitive Dirichlet character $\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \{\pm 1\}$ by $\chi(a) = \chi_2(a)\prod_{p\mid m'}\left(\frac{a}{p}\right)$ (note that any primitive Dirichlet character of order 2 has this form), where $p$ runs through odd primes and $\chi_2\colon (\mathbb{Z}/2^r\mathbb{Z})^\times \to \{\pm 1\}$ is a primitive Dirichlet character defined as follows. For $m \equiv 1 \mod 4$, we have $r = 0$ and $\chi_2$ is trivial. For $m \equiv 3 \mod 4$, we have $r = 2$ and $\chi_2$ is the unique isomorphism $\theta\colon (\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\sim} \{\pm 1\}$. We have $\theta(a) = (-1)^{\frac{a-1}{2}}$. For $m$ even, we have $r = 3$ and we take

$$\chi_2(a) = \begin{cases} 1 & a \equiv 1, 1-m \mod 8 \\ -1 & \text{otherwise.} \end{cases}$$

In all cases $\chi_2(-1) = \theta(m')$, so that $\chi(-1) = \chi_2(-1)\prod_{p|m'}\left(\frac{-1}{p}\right) = \theta(m')\prod_{p|m'}\theta(p) = \theta(m'|m'|) = \mathrm{sgn}(m)$. Consider the Gauss sum $G(\chi) = \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}\chi(a)\zeta_n^a$. Since $n = G(\chi)\overline{G(\chi)} = \chi(-1)G(\chi)^2$, we have $G(\chi)^2 = m$ or $4m$. Thus

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(G(\chi)) \subseteq \mathbb{Q}(\zeta_n).$$

□

The character $\chi$ in the proof is determined by the commutative diagram

$$\begin{tikzcd}
(\mathbb{Z}/n\mathbb{Z})^\times \arrow[r, "\sim"] \arrow[d, "\chi"'] & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \arrow[d] \\
\{\pm 1\} \arrow[r, "\sim"] & \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}),
\end{tikzcd}$$

where the upper horizontal arrow carries $a$ to $\sigma_a$ defined by $\sigma_a(\zeta_n) = \zeta_n^a$ and the vertical arrow on the right is the restriction. Recall that the simple case where $n$ is prime implies quadratic reciprocity.

**Theorem 3.1.31** (Quadratic reciprocity)**.** *Let $p$ and $q$ be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

*Proof.* Take $m = p^* = (-1)^{\frac{p-1}{2}}p \equiv 1 \pmod 4$, so that $n = p$. Then $\left(\frac{p^*}{q}\right) = 1 \iff p^*$ has a square root in $\mathbb{Q}_q \iff q$ splits in $\mathbb{Q}(\sqrt{p^*}) \iff$ the restriction $\sigma_q|_{\mathbb{Q}(\sqrt{m})}$ (which is the Frobenius element at $q$) is trivial $\iff \chi(q) = 1 \iff \left(\frac{q}{p}\right) = 1$. □

**Remark 3.1.32.** The character $\chi(a)$ in the proof of Proposition 3.1.30 can be identified with the Kronecker symbol $\left(\frac{\Delta}{a}\right)$. Indeed, $\chi$ is the unique primitive Dirichlet character $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(-1) = \mathrm{sgn}(m)$.

## 3.2 The power reciprocity law

### First cohomology of groups

Let $G$ be a group. By a (left) *$G$-module*, we mean an abelian group equipped with a (left) $G$-action, or equivalently, a (left) $\mathbb{Z}[G]$-module. The functor carrying an abelian group $A$ to $A$ equipped with trivial $G$-action admits a right adjoint $(-)^G$ and a left adjoint $(-)_G$, which can be described as follows. For a $G$-module $M$, $M^G$ is the maximal $G$-invariant subgroup of $M$, which is the set of $G$-invariant elements of $M$. Moreover, $M_G$ is the group of $G$-coinvariants of $M$, namely the maximal $G$-invariant quotient group of $M$. Note that $M_G = M/I_GM$, where $I_G = \mathrm{Ker}(\mathbb{Z}[G] \to \mathbb{Z})$ (the map given $\sum_{g\in G}a_gg \mapsto \sum a_g$) is the augmentation ideal. In other words, $M_G$ is the cokernel of the map

$$\bigoplus_{g\in G} M \to M \quad (m_g)_{g\in G} \mapsto \sum_{g\in G} gm_g - m_g. \tag{3.2.1}$$

**Definition 3.2.1.** A *crossed homomorphism* is a map $f\colon G \to M$ such that $f(gh) = f(g) + gf(h)$ for all $g, h \in G$. For $m \in M$, let $d^0(m)\colon G \to M$ be the $g \mapsto gm - m$, which is clearly a crossed homomorphism. Indeed, $ghm - m = (gm - m) + g(hm - m)$. A crossed homomorphism of the form $d^0(m)$ for some $m \in M$ is called a *principal* crossed homomorphism. We let $Z^1(G, M)$ and $B^1(G, M)$ denote the abelian groups of crossed homomorphisms and principal crossed homomorphisms, respectively. We define the *first cohomology* of $G$ with coefficients in $M$ to be

$$H^1(G, M) = Z^1(G, M)/B^1(G, M).$$

Note that $M^G$ and $H^1(G, M)$ are cohomology groups of the sequence

$$0 \to M \xrightarrow{d^0} \mathrm{Map}(G, M) \xrightarrow{d^1} \mathrm{Map}(G^2, M),$$

where $d^1(f)\colon (g, h) \mapsto f(g) + gf(h) - f(gh)$. Indeed, we have $M^G = \mathrm{Ker}(d^0)$, and $H^1(G, M) = \mathrm{Ker}(d^1)/\mathrm{Im}(d^0)$, with $\mathrm{Ker}(d^1) = Z^1(G, M)$, $\mathrm{Im}(d^0) = B^1(G, M)$.

The functor $H^1(G, -)$ commutes with arbitrary products. If $G$ is a finite group, $H^1(G, -)$ also commutes with filtered colimits.

**Proposition 3.2.2.** *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of $G$-modules. Then we have exact sequences*

$$M'_G \to M_G \to M''_G \to 0,$$
$$0 \to M'^G \to M^G \to M''^G \to H^1(G, M') \to H^1(G, M) \to H^1(G, M'').$$

*Proof.* The first exact sequence follows from snake lemma applied to the diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_{g\in G} M' \arrow[r] \arrow[d] & \bigoplus_{g\in G} M \arrow[r] \arrow[d] & \bigoplus_{g\in G} M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where the vertical arrows are (3.2.1). Applying the snake lemma to a similar diagram with vertical arrows given by $d^1$, we obtain a diagram

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, "d^0"'] & M \arrow[r] \arrow[d, "d^0"] & M'' \arrow[r] \arrow[d, "d^0"] & 0 \\
0 \arrow[r] & Z^1(G, M') \arrow[r] & Z^1(G, M) \arrow[r] & Z^1(G, M'') &
\end{tikzcd}$$

with exact rows. Applying the snake lemma to the diagram, we obtain the long exact sequence. □

**Example 3.2.3.** If $M$ is a trivial $G$-module, then $B^1(G, M) = 0$ and $H^1(G, M) = Z^1(G, M) = \mathrm{Hom}(G, M) = \mathrm{Hom}(G^{\mathrm{ab}}, M)$.

**Theorem 3.2.4.** *Let $E/F$ be a finite Galois extension of arbitrary fields of Galois group $G$. Then $H^1(G, E^\times) = 1$.*

## Kummer theory

Let $F$ be a field and let $E$ be a finite Galois extension of $F$ of group $G$. Let $n \geq 1$ and let $\mu_{n,E}$ be the group of $n$-th roots of unity in $E$. We have a $G$-equivariant short exact sequence

$$1 \to \mu_{n,E} \to E^\times \xrightarrow{(-)^n} E^{\times n} \to 1,$$

which induces the long exact sequence

$$1 \to \mu_{n,F} \to F^\times \xrightarrow{(-)^n} E^{\times n} \cap F^\times \to H^1(G, \mu_{n,E}) \to H^1(G, E^\times) = 1.$$

We get an isomorphism $E^{\times n} \cap F^\times / F^{\times n} \xrightarrow{\sim} H^1(G, \mu_{n,E})$ carrying the class of $x^n$ to the class of $g \mapsto gx/x$. Assume now that $\mu_{n,E} = \mu_{n,F}$. Then $G$ acts trivially on $\mu_{n,E}$, so that $H^1(G, \mu_{n,E}) = \operatorname{Hom}(G, \mu_{n,E})$.

**Theorem 3.2.5** (Kummer)**.** *Let $n \geq 1$ be an integer and let $F$ be a field containing $n$ distinct $n$-th roots of unity. Then we have a bijection from the set of isomorphism classes of finite abelian extensions of $F$ of exponent dividing $n$, to the set of subgroups of $F^\times$ containing $F^{\times n}$ as a subgroup of finite index, carrying $E$ to $E^{\times n} \cap F^\times$, with inverse carrying $\Delta$ to $F(\sqrt[n]{\Delta})$. If $\Delta$ is the image of $E$ under the above bijection, then the pairing $\operatorname{Gal}(E/F) \times \Delta/F^{\times n} \to \mu_n$ carrying $(g, \bar{y})$ to $g\sqrt[n]{y}/\sqrt[n]{y}$ is perfect and $[E : F] = [\Delta : F^{\times n}]$.*

*Proof.* The second assertion follows from the computation preceding the theorem and (Pontryagin) duality of finite abelian groups of exponent $n$.

Let $F^{\times n} < \Delta < F^\times$ such that $[\Delta : F^{\times n}] < \infty$. It is easy to check that $E_\Delta = F(\sqrt[n]{\Delta})$ is a finite abelian extension of $F$ of exponent dividing $n$. Taking a composition series, we see that $[E_\Delta : F] \leq [\Delta : F^{\times n}]$. We have $\Delta_{E_\Delta} = E_\Delta^{\times n} \cap F^\times \supseteq \Delta$ and $[\Delta_{E_\Delta} : F^{\times n}] = [E_\Delta : F] \leq [\Delta : F^{\times n}]$, which implies that $\Delta_{E_\Delta} = \Delta$ and $[E_\Delta : F] = [\Delta : F^{\times n}]$.

Let $E$ be a finite abelian extensions of $F$ of exponent dividing $n$ and $\Delta_E = E^{\times n} \cap F^\times$. We have $E_{\Delta_E} = F(\sqrt[n]{\Delta_E}) \subseteq E$ and $[E_{\Delta_E} : F] = [\Delta_E : F^{\times n}] = [E : F]$, which implies that $E_{\Delta_E} = E$. □

We can remove the finiteness assumptions by passing to limits.

**Corollary 3.2.6.** *We have a bijection from the set of isomorphism classes of abelian extensions of $F$ of exponent dividing $n$ to the set of subgroups of $F^\times$ containing $F^{\times n}$, carrying $E$ to $E^{\times n} \cap F^\times$, with inverse carrying $\Delta$ to $F(\sqrt[n]{\Delta})$. If $\Delta$ is the image of $E$ under the above bijection, then the pairing $\operatorname{Gal}(E/F) \times \Delta/F^{\times n} \to \mu_n$ carrying $(g, \bar{y})$ to $g\sqrt[n]{y}/\sqrt[n]{y}$ identifies $\operatorname{Gal}(E/F)$ with the Pontryagin dual of the discrete group $\Delta/F^{\times n}$.*

**Corollary 3.2.7.** *If $E \mapsto \Delta$ and $E' \mapsto \Delta'$ under the bijection above, then $E \cap E' \mapsto \Delta \cap \Delta'$ and $EE' \mapsto \Delta\Delta'$.*

*Proof.* The first assertion is trivial. The second assertion follows from the construction of the inverse of the bijection. □

## Hilbert symbol

Let $F$ be a local field of characteristic zero containing all $n$-th roots of unity. Let $E = F(\sqrt[n]{F^\times})$ be the maximal abelian extension of $F$ of exponent dividing $n$. Since $F^{\times n}$ has finite index in $F^\times$, $E/F$ is a finite extension.

**Proposition 3.2.8.** *We have $N_{E/F}E^\times = F^{\times n}$.*

*Proof.* Let $\mathcal{N}_E = N_{E/F}E^\times$. By reciprocity $F^\times/\mathcal{N}_E \simeq \mathrm{Gal}(E/F)$ has exponent $n$, so that $\mathcal{N}_E \supseteq F^{\times n}$. Moreover, $[F^\times : \mathcal{N}_E] = [E : F] = [F^\times : F^{\times n}]$ by Kummer theory. Therefore, $\mathcal{N}_E = F^{\times n}$. □

Via reciprocity $F^\times/F^{\times n} \xrightarrow{\sim} \mathrm{Gal}(E/F)$, the pairing in Kummer theory takes the following form.

**Definition 3.2.9** (Hilbert symbol)**.** The $n$-th *Hilbert symbol* over $F$ is the perfect pairing

$$F^\times/F^{\times n} \times F^\times/F^{\times n} \to \mu_n$$

given by $(x, y)\sqrt[n]{y} = (x, E/F)\sqrt[n]{y}$, where $(x, E/F) \in \mathrm{Gal}(E/F)$ is the norm residue symbol.

By the functoriality of norm residue symbol, we have

$$(x, y)\sqrt[n]{y} = (x, F(\sqrt[n]{y})/F)\sqrt[n]{y}.$$

Note that $(x, y)$ determines $(x, F(\sqrt[n]{y})/F)$. Thus $(x, y) = 1$ if and only if $x \in N_{F(\sqrt[n]{y})/F}(F(\sqrt[n]{y})^\times)$.

By definition, Hilbert symbol is bimultiplicative: $(xx', y) = (x, y)(x', y)$ and $(x, yy') = (x, y)(x, y')$.

**Proposition 3.2.10.** *(1) For $y \in F^\times$ and $z \in F$ such that $z^n - y \neq 0$, we have $(z^n - y, y) = 1$. In particular, $(1 - y, y) = 1$ (if $y \neq 1$) and $(-y, y) = 1$.*

*(2) (skew-symmetry) For $x, y \in F^\times$, we have $(x, y) = (y, x)^{-1}$.*

*Proof.* (1) The conjugates of $\sqrt[n]{y}$ over $F$ are $\zeta_n^{mj}\sqrt[n]{y}$ for some $m \mid n$. Thus

$$z^n - y = \prod_{i=0}^{n-1}(z - \zeta_n^i\sqrt[n]{y}) = N_{F(\sqrt[n]{y})/F}\prod_{i=0}^{m-1}(z - \zeta_n^i\sqrt[n]{y}),$$

so that $(z^n - y, y) = 1$ by definition. The second assertion follows immediately $z = 0$ and $z = 1$.

(2) By (1), we have

$$(x, y)(y, x) = (x, y)(y, x)(-x, x)(-y, y) = (-xy, x)(-xy, y) = (-xy, xy) = 1.$$

□

For $F = \mathbb{C}$ we have $(x, y) = 1$.

For $F = \mathbb{R}$, the assumption that $\mathbb{R}$ contains all $n$-th roots of unity implies that $n = 1$ or $n = 2$. If $n - 1$, we have $(x, y) = 1$. If $n = 2$, we have $(x, y) = \max\{\mathrm{sgn}(x), \mathrm{sgn}(y)\}$.

Assume that $F$ is non-Archimedean of residue field $\mathbb{F}_q$ of characteristic $p \nmid n$. Note that $\mathbb{F}_q^\times$ is a cyclic group of order $q - 1$ and $\mu_{n,\mathbb{F}_q}$ is a subgroup of order $n$. We have $\mu_n = \mu_{n,F} \xrightarrow{\sim} \mu_{n,\mathbb{F}_q}$.

**Definition 3.2.11** ($n$-th power residue symbol)**.** For $x \in U_F$, we let $\left(\frac{x}{F}\right) \in \mu_n$ denote the $n$-th root of unity congruent to $x^{(q-1)/n}$ modulo the maximal ideal $\mathfrak{p}_F$ of $\mathcal{O}_F$.

Note that $\left(\frac{x}{F}\right) = 1$ if and only if $x$ is an $n$-th power modulo $\mathfrak{p}_F$.

**Proposition 3.2.12.** *For $x, y \in F^\times$, we have*

$$(x, y) = \left(\frac{(-1)^{ij} y^i x^{-j}}{F}\right),$$

*where $i = v_F(x)$ and $j = v_F(y)$.*

*Proof.* Since both sides are bimultiplicative, we are reduced to two cases: (a) $x \in U_F$ or $y \in U_F$; (b) $x = \pi$, $y = -\pi$ for some uniformizer $\pi$. Case (b) is trivial. For case (a), since both sides are skew-symmetric, we may assume that $y \in U_F$. The extension $F(\sqrt[n]{y})/F$ is unramified by Hensel's lemma. Then $(x, F(\sqrt[n]{y})/F) = \mathrm{Frob}^i$. Since $\mathrm{Frob}(\sqrt[n]{y})/\sqrt[n]{y} \equiv \sqrt[n]{y}^{q-1} \equiv \left(\frac{y}{F}\right) \mod \mathfrak{p}_F$, we have $\mathrm{Frob}(\sqrt[n]{y})/\sqrt[n]{y} = \left(\frac{y}{F}\right)$, so that $(x, y) = (x, F(\sqrt[n]{y})/F)\sqrt[n]{y}/\sqrt[n]{y} = \left(\frac{y^i}{F}\right)$. □

**Corollary 3.2.13.** *Let $\pi$ be a uniformizer. Then for all $y \in U_F$, we have $(\pi, y) = \left(\frac{y}{F}\right)$.*

**Notation 3.2.14.** We define $\left(\frac{x}{y}\right)$ for $x, y \in F^\times$ satisfying $x \in U_F$ or $y \in U_F$ as follows. For $x \in U_F$, we put $\left(\frac{x}{y}\right) = \left(\frac{x}{F}\right)^{v_F(y)}$. For $y \in U_F$, we put $\left(\frac{x}{y}\right) = 1$.

**Corollary 3.2.15.** *For $x, y \in F^\times$ satisfying $x \in U_F$ or $y \in U_F$, we have $(x, y) = \left(\frac{x}{y}\right)^{-1}\left(\frac{y}{x}\right)$.*

The determination of the Hilbert symbol for $p \mid n$ is more subtle. We consider the special case $F = \mathbb{Q}_2$ and $n = 2$, which will be used to deduce Gauss's quadratic reciprocity from the product formula (Corollary 3.2.20 below).

**Proposition 3.2.16.** *Let $F = \mathbb{Q}_2$ and $n = 2$. Then for $x, y \in 1 + 2\mathbb{Z}_2$, we have*

$$(x, y) = (-1)^{\frac{x-1}{2}\frac{y-1}{2}}, \quad (x, 2) = (2, x) = (-1)^{\frac{x^2-1}{8}}, \quad (2, 2) = 1.$$

We adopt the convention that $(-1)^a = 1$ for $a \in 2\mathbb{Z}_2$ and $(-1)^a = -1$ for $a \in 1 + 2\mathbb{Z}_2$.

*Proof.* Note that $(1 + 2\mathbb{Z}_2)^2 = 1 + 8\mathbb{Z}_2$, and $1 + 2\mathbb{Z}_2/1 + 8\mathbb{Z}_2$ is generated by $-1$ and 5. For $z \in \mathbb{Q}_2^\times$, $(z, -1) = 1$ if and only if $z$ is a norm for $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$, or in other words, $z = a^2 + b^2$ for $a, b \in \mathbb{Q}_2$. We have $2 = 1 + 1$ and $5 = 1 + 2^2$, so that $(2, -1) = (5, -1) = 1$. It follows that $(-1, -1) = -1$; otherwise $(z, -1) = 1$ for all $z$, which would imply $-1 \in (\mathbb{Q}_2^\times)^2$. Moreover $(2, 2) = (5, 5) = 1$. Finally $(2, 5) = -1$; otherwise $(2, z) = 1$ for all $z$, which would imply $2 \in (\mathbb{Q}_2^\times)^2$. □

## The power reciprocity law

Let $F$ be a number field containing all $n$-th roots of unity.

**Theorem 3.2.17.** *For $x, y \in F^\times$, we have $\prod_v (x, y)_v = 1$, where $v$ runs through all places of $F$.*

Note that for all but finitely many places $v$, we have $x, y \in U_v$, so that $(x, y)_v = 1$.

*Proof.* This follows immediately from Artin reciprocity $\prod_v (x, F_v(\sqrt[n]{y})/F_v) = 1$. □

**Notation 3.2.18.** Let $y \in F^\times$ be prime to $n$ and let $x \in F^\times$ be prime to $y$. We write

$$\left(\frac{x}{y}\right) = \prod_{v \in V - S} \left(\frac{x}{y}\right)_v = \prod_{\substack{v \in V - S \\ v(x)=0}} \left(\frac{x}{v}\right)^{v(y)},$$

where $S$ denotes the set of places that are either Archimedean or dividing $n$.

Note that $\left(\frac{x}{uy}\right) = \left(\frac{x}{y}\right)$ for all $u \in \mathcal{O}_F^\times$.

Applying the theorem and Corollary 3.2.15, we get the following.

**Corollary 3.2.19.** *Let $y \in F^\times$ be prime to $n$. For $x \in F^\times$ prime to $y$ and $n$, we have*

$$\left(\frac{x}{y}\right)\left(\frac{y}{x}\right)^{-1} = \prod_{v \in S} (x, y)_v.$$

*For $x \in F^\times$ which is a unit outside $S$, we have*

$$\left(\frac{x}{y}\right) = \prod_{v \in S} (x, y)_v.$$

For $F = \mathbb{Q}$ and $n = 2$, the above notation extends the Jacobi symbol. Applying the corollary and Proposition 3.2.16, we obtain Gauss's quadratic reciprocity.

**Corollary 3.2.20.** *Let $F = \mathbb{Q}$ and $n = 2$. Let $x$ and $y$ be relatively prime odd integers. Then*

$$\left(\frac{x}{y}\right)\left(\frac{y}{x}\right) = \max\{\operatorname{sgn}(x), \operatorname{sgn}(y)\}(-1)^{\frac{x-1}{2}}(-1)^{\frac{y-1}{2}}, \quad \left(\frac{2}{x}\right) = (-1)^{\frac{x^2-1}{8}}.$$

**Remark 3.2.21.** The Hilbert symbol can be interpreted as a cup product. Let $F$ be a field of characteristic not dividing $n$. We have $F^\times/F^{\times n} \xrightarrow{\sim} H^1(G_F, \mu_n)$, where $G_F = \mathrm{Gal}(\bar{F}/F)$. Cup product provides a bimultiplicative map

$$F^\times/F^{\times n} \times F^\times/F^{\times n} \to H^2(G_F, \mu_n^{\otimes 2})$$

called the Galois symbol, satisfying the Steinberg identity $(x, 1-x) = 1$ for $x \neq 0, 1$. (Recall that $K_2(F)$ can be defined as the quotient $F^\times \otimes F^\times$ by the subgroup generated by $x \otimes (1-x)$, $x \neq 0, 1$. The Galois symbol induces a homomorphism $K_2(F)/nK_2(F) \to H^2(G_F, \mu_n^{\otimes 2})$, which is in fact an isomorphism by the Merkurjev-Suslin Theorem.)

For any field $K$ of separable closure $K^{\mathrm{sep}}$, the Brauer group $\mathrm{Br}_K = H^2(G_K, (K^{\mathrm{sep}})^\times)$ is defined. We have $\mathrm{Br}_F[n] = H^2(G_F, \mu_n)$. If $F$ contains $\mu_n$, then $H^2(G_F, \mu_n^{\otimes 2}) \simeq \mu_n \otimes \mathrm{Br}_F[n]$. If $F$ is a local field containing $\mu_n$, then the Hilbert symbol is the Galois symbol composed with the injection $\mu_n \otimes \mathrm{Br}_F \to \mu_n \otimes \mathbb{Q}/\mathbb{Z} \simeq \mu_n$ induced by inv (see below).

**Remark 3.2.22.** For any non-Archimedean local field $K$, Hasse invariant provides an isomorphism $\mathrm{inv}\colon \mathrm{Br}_K \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Moreover, we have $\mathrm{inv}\colon \mathrm{Br}_{\mathbb{R}} \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and $\mathrm{inv}\colon \mathrm{Br}_{\mathbb{C}} \xrightarrow{\sim} 0$. For a global field $K$, the Brauer group fits into a short exact sequence

$$0 \to \mathrm{Br}_K \to \bigoplus_v \mathrm{Br}_{K_v} \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

The fact that the composition of the two nontrivial arrows above is zero implies the product formula of Hilbert symbols.

The norm residue symbol can also be interpreted as a cup product. For any local field $K$, the cup product

$$K^\times \times H^2(G_K, \mathbb{Z}) \to H^2(G_K, (K^{\mathrm{sep}})^\times) = \mathrm{Br}_K \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z}$$

carries $(a, \chi)$ to $\chi((a, K^{\mathrm{sep}}/K))$. Here we used the isomorphism $\mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z}) = H^1(G_K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G_K, \mathbb{Z})$. A similar interpretation holds for global fields $K$, after replacing $K^\times$ by $\mathbb{I}_K/K^\times$.

## 3.3 The first inequality

Let $F$ be a number field, and let $\mathcal{S}_F$ be the set of maximal ideals of $\mathcal{O}_F$.

**Definition 3.3.1.** Let $\mathcal{S} \subseteq \mathcal{S}_F$ be a subset. The *arithmetic density* (or natural density) of $\mathcal{S}$ is the limit

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in \mathcal{S} \mid N\mathfrak{p} \le X\}}{\#\{\mathfrak{p} \in \mathcal{S}_F \mid N\mathfrak{p} \le X\}}$$

if the limit exists. The *analytic density* of a subset is the limit

$$\delta(\mathcal{S}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathcal{S}} (N\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in\mathcal{S}_F} (N\mathfrak{p})^{-s}}$$

if the limit exists.

The sums in the definition of analytic density converges, since $\sum_{\mathfrak{p}\in\mathcal{S}_F} (N\mathfrak{p})^{-s}$ converges absolutely for $\mathrm{Re}(s) > 1$.

**Remark 3.3.2.** One can show that if $\mathcal{S}$ has arithmetic density $\delta$, then it has analytic density $\delta$. However, the set of rational primes whose first decimal digit is 1 has analytic density $\log_{10}(2)$ but no arithmetic density.

We will only use analytic density. The results of this section also holds for arithmetic density, but additional arguments are needed to prove this.

**Remark 3.3.3.** (1) If $\mathcal{S} = \mathcal{S}' \coprod \mathcal{S}''$, then $\delta(\mathcal{S}) = \delta(\mathcal{S}') + \delta(\mathcal{S}'')$ (if two of the three exist then so does the third one).

(2) If $\mathcal{S} \subseteq \mathcal{S}' \subseteq \mathcal{S}''$ and $\delta(\mathcal{S}) = \delta(\mathcal{S}'') = \delta$, then $\delta(\mathcal{S}') = \delta$.

**Proposition 3.3.4.** *We have* $\sum_{\mathfrak{p}\in\mathcal{S}_F}(N\mathfrak{p})^{-s} = \log(\frac{1}{s-1}) + O(1)$ *as* $s \to 1^+$.

*Proof.* For $\mathrm{Re}(s) > 1$,

$$\log\zeta_F(s) = \sum_{\mathfrak{p}\in\mathcal{S}_F}\sum_{n\geq 1}\frac{1}{n}(N\mathfrak{p})^{-ns}.$$

Since $\zeta_F(s)$ has a simple pole at $s = 1$, it suffices to show that

$$\sum_{\mathfrak{p}\in\mathcal{S}_F}\sum_{n\geq 2}\frac{1}{n}(N\mathfrak{p})^{-ns}$$

converges absolutely in a neighborhood of $s = 1$. Indeed, for $\sigma > \frac{1}{2}$,

$$\sum_{\mathfrak{p}\in\mathcal{S}_F}\sum_{n\geq 2}\frac{1}{n}(N\mathfrak{p})^{-n\sigma} < 2\sum_{\mathfrak{p}\in\mathcal{S}_F}\sum_{m\geq 1}\frac{1}{2m}(N\mathfrak{p})^{-2m\sigma} = \log\zeta_F(2\sigma) < \infty,$$

where we have set $n = 2m$ and $n = 2m + 1$. □

**Corollary 3.3.5.** *A finite subset of $\mathcal{S}_F$ has analytic density zero.*

**Proposition 3.3.6.** *Let $\mathcal{S}$ be the set of maximal ideals of $F$ whose norms are not primes. Then $\mathcal{S}$ has analytic density zero.*

*Proof.* Let $d = [F : \mathbb{Q}]$. For each rational prime $p$, there are at most $d$ maximal ideals of $F$ above $p$. Thus, for $\sigma > 1/2$,

$$\sum_{\mathfrak{p}\in\mathcal{S}}(N\mathfrak{p})^{-\sigma} \leq d\sum_{p} p^{-2\sigma} < \infty.$$

□

**Theorem 3.3.7.** *Let $E/F$ be a finite Galois extension of number fields of degree $d$. Let $\mathcal{S}$ be the set of maximal ideals of $F$ that split in $E$. Then $\delta(\mathcal{S}) = 1/d$.*

*Proof.* Let $\mathcal{T}$ be the set of maximal ideals $\mathfrak{q}$ of $\mathcal{S}_E$ such that $\mathfrak{q} \cap F \in \mathcal{S}$. Then $\sum_{\mathfrak{q}\in\mathcal{T}}(N\mathfrak{q})^{-s} = d\sum_{\mathfrak{p}\in\mathcal{S}}(N\mathfrak{q})^{-s}$. It thus suffices to show that $\delta(\mathcal{T}) = 1$. Note that $\mathcal{S}_E - \mathcal{T} \subseteq \mathcal{T}' \cup \mathcal{T}''$, where $\mathcal{T}'$ is the set of maximal ideals of $E$ whose norms are not primes, and $\mathcal{T}''$ is the finite set of maximal ideals of $E$, ramified over $F$. Since $\delta(\mathcal{T}') = \delta(\mathcal{T}'') = 0$, $\delta(\mathcal{T}) = 1$. □

**Corollary 3.3.8.** *Let $E/F$ be a finite Galois extension of number fields and let $S \subseteq \mathcal{S}_F$ be a finite set of maximal ideals containing all the ramified maximal ideals. Then the Artin homomorphism* (3.1.7)

$$\mathcal{I}_F^S \to \mathrm{Gal}(E/F)^{\mathrm{ab}}$$

*is surjective. Here $\mathcal{I}_F^S$ denotes the group of fractional ideals of $F$ generated by maximal ideals not in $S$.*

*Proof.* Let $G = \mathrm{Gal}(E/F)$ and let $H \subseteq G$ be the pullback of the image of the Artin homomorphism. For any prime $\mathfrak{p} \in \mathcal{S}_F - S$, the conjugacy class of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is contained in $H$, so that $\mathrm{Frob}_{(\mathfrak{q}|_{E^H})/\mathfrak{p}} = 1$, hence $\mathfrak{p}$ splits in $E^H$. Here $\mathfrak{q} \in \mathcal{S}_E$ is a lifting of $\mathfrak{p}$. Therefore $\frac{1}{[E^H:F]} = \delta(\mathcal{S}_F - S) = 1$, so that $E^H = F$, $H = G$. □

**Theorem 3.3.9** (The first inequality). *Let $E/F$ be a finite Galois extension of number fields. Then*

$$\#(\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)) \leq \#\mathrm{Gal}(E/F). \tag{3.3.1}$$

Historically this inequality was proven earlier than the second inequality, using analytic methods as in these notes. However, it is possible to deduce (3.3.1) (or more precisely that the left-hand side divides the right-hand side) from the second inequality without analytic methods. For this reason, some authors, notably Artin and Tate [AT], call (3.3.1) the second inequality.

*Proof.* Let $H = \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)$. A character $\chi\colon H \to \mathbb{C}^\times$ induces a Hecke character on $F$, that we still denote by $\chi$. For $\mathrm{Re}(s) > 1$, we have

$$\log L_f(s,\chi) = \sum_{\mathfrak{p}\in\mathcal{S}_F - S_\chi} \sum_{n\geq 1} \frac{1}{n}\chi(\pi_\mathfrak{p})^n (N\mathfrak{p})^{-ns},$$

where $S_\chi$ is the set of maximal ideals of $\mathcal{O}_F$ such that $\chi_\mathfrak{p}$ is ramified. As before, $\sum_{\mathfrak{p}\in\mathcal{S}_F - S_\chi}\sum_{n\geq 2}\frac{1}{n}\chi(\pi_\mathfrak{p})(N\mathfrak{p})^{-ns}$ converges absolutely for $\mathrm{Re}(s) > 1/2$. By the meromorphic continuation of $L_f(s,\chi)$, we have

$$\sum_{\mathfrak{p}\in\mathcal{S}_F - S} \chi(\pi_\mathfrak{p})(N\mathfrak{p})^{-s} = -\alpha_\chi \log\frac{1}{s-1} + O(1) \tag{3.3.2}$$

as $s \mapsto 1^+$. Here $S$ is the set of maximal ideals of $\mathcal{O}_F$ ramified in $E$ and $\alpha_\chi$ is the order of $L_f(s,\chi)$ at $s = 1$. We have $\alpha_1 = -1$ and $\alpha_\chi \geq 0$ for $\chi \neq 1$. Summing over all $\chi$, we get

$$\#H\sum_{\mathfrak{p}\in\mathcal{T}}(N\mathfrak{p})^{-s} = (1 - \sum_{\chi\neq 1}\alpha_\chi)\log\frac{1}{s-1} + O(1),$$

where $\mathcal{T} \subseteq \mathcal{S}_F - S$ is the set of maximal ideals $\mathfrak{p}$ such that $\pi_\mathfrak{p} \in F^\times N_{E/F}(\mathbb{I}_E)$. Note that every maximal ideal of $\mathcal{O}_F$ split in $E$ belongs to $\mathcal{T}$. Thus, by Theorem 3.3.7,

$$\frac{1}{[E:F]} \leq \delta(\mathcal{T}) = \frac{1}{\#H}(1 - \sum_{\chi\neq 1}\alpha_\chi).$$

It follows that $\alpha_\chi = 0$ for all $\chi \neq 1$ and $\#H \leq [E:F]$. □

**Remark 3.3.10.** The proof shows that $L_f(\chi, 1) \neq 0$ for $\chi \neq 1$. In fact, this holds more generally for every unitary Hecke character $\chi\colon \mathbb{I}_F/F^\times \to \mathbb{C}^\times$ [RV, Theorem 7.28].

Theorem 3.3.7 has the following generalization.

**Theorem 3.3.11** (Chebotarev's density)**.** *Let $E/F$ be a finite Galois extension of number fields of group $G$. Let $C \subseteq G$ be a conjugacy class. Then the set $\mathcal{S}$ of maximal ideals $\mathfrak{p}$ of $\mathcal{O}_F$, unramified in $E$, such that $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in C$, where $\mathfrak{q}$ is a maximal ideal of $\mathcal{O}_E$ above $\mathfrak{p}$, has analytic density $\#C/\#G$.*

For $F = \mathbb{Q}$ and $E = \mathbb{Q}(\zeta_m)$, we have an isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$ carrying the automorphism defined by $\zeta_m \mapsto \zeta_m^i$ to the class of $i$. Moreover, a prime $p$ ramifies in $\mathbb{Q}(\zeta_m)$ if and only if $p \mid m/(2,m)$, and for $p \nmid m$, the image of $\mathrm{Frob}_{p,\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ is the class of $p$. Chebotarev's density theorem thus takes the following form.

**Corollary 3.3.12** (Dirichlet's density theorem)**.** *For $(n,m) = 1$, the set of primes congruent to $n$ modulo $m$ has analytic density $1/\phi(m)$.*

*Proof of Chebotarev's theorem, assuming Artin reciprocity for cyclic extensions.* Let $\sigma \in C$ and let $K = E^{\langle\sigma\rangle}$. We assume the existence of a bijection

$$H = \mathbb{I}_K/K^\times N_{E/K}(\mathbb{I}_E) \xrightarrow{\sim} \mathrm{Gal}(E/K) \simeq \langle\sigma\rangle,$$

carrying the class of $\pi'_\mathfrak{p}$ to $\mathrm{Frob}_{\mathfrak{q},K/E}$ for all but finitely many maximal ideals $\mathfrak{p}'$ of $K$. A character $\chi$ of $\langle\sigma\rangle$ induces a character $\chi_H$ of $H$.

Let $\mathcal{S}' \subseteq \mathcal{S}_K$ be the set of maximal ideals $\mathfrak{p}'$ such that $\mathfrak{p}' \cap \mathcal{O}_F$ is unramified in $E$ and $\mathrm{Frob}_{\mathfrak{p}',K/E} = \sigma$. We have

$$\begin{aligned}\#\langle\sigma\rangle \sum_{\mathfrak{p}'\in\mathcal{S}'} (N\mathfrak{p}')^{-s} &= \sum_{\mathfrak{p}'\in\mathcal{S}_K - S}\sum_\chi \chi(\sigma)^{-1}\chi(\mathrm{Frob}_{\mathfrak{p}'})(N\mathfrak{p}')^{-s}\\ &= \sum_\chi \chi(\sigma)^{-1}\sum_{\mathfrak{p}'\in\mathcal{S}_K-S}\chi_H(\pi'_\mathfrak{p})(N\mathfrak{p}')^{-s} + O(1) = \log(\frac{1}{s-1}) + O(1)\end{aligned}$$

as $s \to 1^+$ by the proof of Theorem 3.3.9. Here $S \subseteq \mathcal{S}_K$ denotes the set of maximal ideals $\mathfrak{p}'$ such that $\mathfrak{p}'\cap\mathcal{O}_F$ is ramified in $E$, and $\chi$ runs through characters $\langle\sigma\rangle \to \mathbb{C}^\times$.

Let $\mathcal{T} \subseteq \mathcal{S}_E$ be the set of maximal ideals $\mathfrak{q}$ such that $\mathfrak{p} = \mathfrak{q}\cap\mathcal{O}_F$ is unramified in $E$ and $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} = \sigma$. The map $\mathcal{T} \to \mathcal{S}'$, $\mathfrak{q} \mapsto \mathfrak{p}' = \mathfrak{q}\cap\mathcal{O}_K$ is a bijection. Indeed, $D(\mathfrak{q}/\mathfrak{p}') = \langle\sigma\rangle = \mathrm{Gal}(E/K)$. The map $\mathcal{T} \to \mathcal{S}$, $\mathfrak{q} \mapsto \mathfrak{p} = \mathfrak{q}\cap\mathcal{O}_F$ is surjective. For $\tau \in G$, $\mathrm{Frob}_{\tau\mathfrak{q}/\mathfrak{p}} = \tau\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\tau^{-1} = \tau\sigma\tau^{-1}$, so that $\tau\mathfrak{q} \in \mathcal{T}$ if and only if $\tau$ belongs to the centralizer $\mathrm{Cent}_G(\sigma)$. Moreover, $\tau\mathfrak{q} = \mathfrak{q}$ if and only if $\tau \in D(\mathfrak{q}/\mathfrak{p}) = \langle\sigma\rangle$. Therefore, the fibers of the map $\mathcal{T} \to \mathcal{S}$ have cardinality $\#\mathrm{Cent}_G(\sigma)/\#\langle\sigma\rangle$. Since $f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}') = \#\langle\sigma\rangle$, we have

$$\sum_{\mathfrak{p}\in\mathcal{S}}(N\mathfrak{p})^{-s} = \frac{\#\langle\sigma\rangle}{\#\mathrm{Cent}_G(\sigma)}\sum_{\mathfrak{p}'\in\mathcal{S}'}(N\mathfrak{p}')^{-s} = \frac{1}{\#\mathrm{Cent}_G(\sigma)}\log\frac{1}{s-1} + O(1).$$

Therefore, $\delta(\mathcal{S}) = 1/\#\mathrm{Cent}_G(\sigma) = \#C/\#G$. □

## 3.4 Cohomology of groups

### Induced modules

Let $\phi\colon H \to G$ be group homomorphism. For a $G$-module $A$, we let $\mathrm{res}^G_H A$ denote the underlying $H$-module. The functor $\mathrm{res}^G_H$ admits a left adjoint $\mathrm{ind}^G_H$ and a right adjoint $\mathrm{coind}_H^G$, which can be described as follows. For an $H$-module $B$, we have

$$\mathrm{coind}_H^G B = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B), \quad \mathrm{ind}_H^G B = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B,$$

with the $G$-module structure given respectively by right and left multiplication. Note that $\mathrm{coind}_H^G B$ can be identified with the set of maps $f\colon G \to B$ such that $f(hg) = hf(g)$ for all $h \in H$, with the $G$-module structure given by $(gf)(g') = f(g'g)$. The adjunctions

$$\mathrm{Hom}_{\mathbb{Z}[H]}(\mathrm{res}_H^G A, B) \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{coind}_H^G B),$$
$$\mathrm{Hom}_{\mathbb{Z}[H]}(B, \mathrm{res}_H^G A) \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{ind}_H^G B, A)$$

are called *Frobenius reciprocity.* From the sequence $H \to G \to \{1\}$, we get

$$B^H \simeq (\mathrm{coind}_H^G B)^G, \quad B_H \simeq (\mathrm{ind}_H^G B)_G.$$

If $H$ is a subgroup of $G$, then $\mathrm{coind}_H^G$ is an exact functor (with exact left adjoint), so that

$$H^1(G, \mathrm{coind}_H^G B) \simeq H^1(H, B). \tag{3.4.1}$$

This holds for all $H^n$, and is known as Shapiro's lemma. The map (3.4.1) is the composition

$$H^1(G, \mathrm{coind}_H^G B) \to H^1(H, \mathrm{res}_H^G \mathrm{coind}_H^G B) \to H^1(H, B),$$

where the second map is induced by adjunction. The restriction map $\mathrm{res}\colon H^1(G, A) \to H^1(H, \mathrm{res}_H^G A)$ can be identified with the map induced by the adjunction map $A \to \mathrm{coind}_H^G \mathrm{res}_H^G A$ composed with the (3.4.1).

**Lemma 3.4.1.** *Assume $H$ has finite index in $G$, then the homomorphism of $G$-modules $\alpha\colon \mathrm{ind}_H^G B \to \mathrm{coind}_H^G B$ carrying $g \otimes b$ to*

$$g' \mapsto \begin{cases} g'gb & g' \in gH \\ 0 & \textit{otherwise} \end{cases}$$

*is an isomorphism.*

*Proof.* The inverse is given by $\beta(f) = \sum_{g \in G/H} g \otimes f(g^{-1})$, where $g$ runs through a set of representatives of $G/H$. □

The map $\mathrm{cor}\colon H^1(H, A) \to H^1(G, A)$ induced by the adjunction map $\mathrm{ind}_H^G \mathrm{res}_H^G A \to A$, $\beta$, and the inverse of (3.4.1) is called the corestriction map. The composite

$$A \to \mathrm{coind}_H^G \mathrm{res}_H^G A \xrightarrow[\sim]{\beta} \mathrm{ind}_H^G \mathrm{res}_H^G A \to A$$

is multiplication by $[G : H]$. It follows that the composite

$$H^1(G, A) \xrightarrow{\mathrm{res}} H^1(H, \mathrm{res}_H^G A) \xrightarrow{\mathrm{cor}} H^1(G, A)$$

is multiplication by $[G : H]$. Taking $H = \{1\}$, we see that $H^1(G, A)$ is killed by $\#G$.

**Example 3.4.2.** Let $H$ be a subgroup of $G$. Then $\mathrm{ind}_H^G\mathbb{Z} = \mathbb{Z}[G/H]$. Here $H$ acts trivially on $\mathbb{Z}$ and $G$ acts on $\mathbb{Z}[G/H]$ by left multiplication.

**Example 3.4.3.** Let $E/F$ be a finite Galois extension of arbitrary fields of group $G$. By the normal basis theorem, there exists $x \in E$ such that $E = \oplus_{g\in G} g(x)F$. In other words, $E \simeq \mathrm{ind}_{\{1\}}^G F$. Therefore, $H^1(G,E) \simeq H^1(\{1\},F) = 1$.

**Example 3.4.4.** Let $E/F$ be a finite Galois extension of number fields of group $G$. Let $v$ be a place of $E$ and let $w_0$ be a place of $E$ above $v$. Let $D = D(w_0/v) \subseteq G$ be the decomposition group. Then $\prod_{w|v} E_w^\times \simeq \mathrm{ind}_D^G E_{w_0}^\times$ and, if $v$ is ultrametric, then $\prod_{w|v} U_w \simeq \mathrm{ind}_D^G U_{w_0}$.

**Proposition 3.4.5.** *Let $E/F$ be a finite Galois extension of number fields of group $G$. Then $\mathbb{I}_E^G = \mathbb{I}_F$ and $H^1(G,\mathbb{I}_E) = 1$.*

*Proof.* The first assertion follows from the example above. For a finite set of places $S$ of $F$ containing the set $S_\infty$ of Archimedean places, we let $S_E$ denote the set of places above $E$, and we write $\mathbb{I}_{E,S} = \mathbb{I}_{E,S_E} = \prod_{w\in S_E} E_w^\times \times \prod_{w\notin S_E} U_{E_w}$. We have $\mathbb{I}_E = \cup_S \mathbb{I}_{E,S}$. Let $w_0$ be a place of $E$ above $v$ and let $H = D(w_0 \mid v)$. We have $H^1(G, \prod_{w|v} E_w^\times) \simeq H^1(H, E_{w_0}^\times) = 1$. For $v$ ultrametric and unramified in $E$, we have $H^1(G, \prod_{w|v} U_w) \simeq H^1(H, U_{w_0}) = 1$ by the following lemma. Thus $H^1(G, \mathbb{I}_{E,S}) = 1$ for any $S \supseteq S_\infty$ containing all places ramified in $E$. It follows that $H^1(G,\mathbb{I}_E) = 0$. □

**Lemma 3.4.6.** *For any finite extension $L/K$ of group $H$ of ultrametric local fields of ramification index $e$, we have $H^1(H,U_L) = \mathbb{Z}/e\mathbb{Z}$.*

*Proof.* The short exact sequence of $H$-modules

$$1 \to U_L \to L^\times \xrightarrow{w} \mathbb{Z} \to 0$$

induces an exact sequence

$$K^\times \xrightarrow{w} \mathbb{Z} \to H^1(H,U_L) \to H^1(H,L^\times) = 1.$$

Thus $H^1(H,U_L) \simeq \mathbb{Z}/w(K^\times) = \mathbb{Z}/e\mathbb{Z}$. □

## Tate cohomology of finite groups

Let $G$ be a finite group. For a $G$-module $M$, we define the *norm* map $N\colon M \to M$ by $Nm = \sum_{g\in G} gm$. We have $I_G M \subseteq \mathrm{Ker}(N)$ and $\mathrm{Im}(N) \subseteq M^G$.

**Definition 3.4.7.** The $i$-th *Tate cohomology* groups, $i = -1, 0, 1$ are defined by

$$\hat{H}^{-1}(G,M) = \mathrm{Ker}(N)/I_G M, \quad \hat{H}^0(G,M) = M^G/\mathrm{Im}(N), \quad \hat{H}^1(G,M) = H^1(G,M).$$

In other words, $\hat{H}^{-1}(G,M)$ and $\hat{H}^0(G,M)$ are respectively the kernel and cokernel of the map $M_G \to M^G$ induced by $N$.

Note that for $\hat{H}^i(G,M) = \mathrm{Ker}(d^i)/\mathrm{Im}(d^{i-1})$, $i = -1,0,1$, are the cohomology groups of the complex

$$\bigoplus_{g\in G} M \xrightarrow{d^{-2}} M \xrightarrow{d^{-1}} M \xrightarrow{d^0} \mathrm{Map}(G,M) \xrightarrow{d^1} \mathrm{Map}(G^2,M),$$

where $d^{-2}$ is the map (3.2.1) and $d^{-1} = N$.

The functors $\hat{H}^i(G, -)$, $i = -1, 0, 1$, commute with arbitrary products and filtered colimits (hence arbitrary coproducts). Applying the snake lemma as before, we obtain the following.

**Proposition 3.4.8.** *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of $G$-modules. Then we have a long exact sequence*

$$\begin{aligned}\hat{H}^{-1}(G, M') \to \hat{H}^{-1}(G, M) \to \hat{H}^{-1}(G, M'') \to \hat{H}^0(G, M)\\ \to \hat{H}^0(G, M) \to \hat{H}^0(G, M'') \to \hat{H}^1(G, M') \to \hat{H}^1(G, M) \to \hat{H}^1(G, M'').\end{aligned}$$

**Example 3.4.9.** For a trivial $G$-module $M$, $\hat{H}^{-1}(G, M) = \operatorname{Ker}(\#G\colon M \to M)$ and $\hat{H}^0(G, M) = \operatorname{Coker}(\#G\colon M \to M)$. In particular, $\hat{H}^i(\{1\}, M) = 0$ for $i = -1, 0, 1$, and $\hat{H}^{-1}(G, \mathbb{Z}) = H^1(G, \mathbb{Z}) = 0$, where $G$ acts trivially on $\mathbb{Z}$.

**Example 3.4.10.** Let $E/F$ be a finite Galois extension of arbitrary fields of group $G$. Then $\hat{H}^0(G, E^\times) = F^\times / N_{E/F}E^\times$.

**Example 3.4.11.** Let $E/F$ be a finite Galois extension of number fields of group $G$. Then $\hat{H}^0(G, \mathbb{I}_E) = \mathbb{I}_F / N_{E/F}(\mathbb{I}_E)$.

**Proposition 3.4.12.** *Let $E/F$ be a finite Galois extension of number fields of group $G$. Then $(\mathbb{I}_E/E^\times)^G \simeq \mathbb{I}_F/F^\times$ and $\hat{H}^0(G, \mathbb{I}_E/E^\times) \simeq \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)$.*

*Proof.* The long exact sequences associated to the short exact sequence of $G$-modules $1 \to E^\times \to \mathbb{I}_E \to \mathbb{I}_E/E^\times \to 1$ are

$$1 \to F^\times \to \mathbb{I}_F \to (\mathbb{I}_E/E^\times)^G \to H^1(G, E^\times) = 1$$
$$F^\times/N_{E/F}(E^\times) \to \mathbb{I}_F/N_{E/F}(\mathbb{I}_E) \to \hat{H}^0(G, \mathbb{I}_E/E^\times) \to \hat{H}^1(G, E^\times) = 1.$$

□

**Remark 3.4.13.** For a subgroup $H$ of $G$, and an $H$-module $B$, $\hat{H}^i(H, B) \simeq \hat{H}^i(G, \operatorname{ind}_H^G B)$ for $i = -1, 0, 1$. Indeed, for $A = \operatorname{ind}_H^G B$, via the isomorphisms $A_G \simeq B_H$ and $A^G \simeq B^H$, the maps $N_G\colon A_G \to A^G$ and $B_H\colon B_H \to B^H$ can be identified: $N_G(b) = \sum_{g \in G/H} gN_H(b)$.

## Cohomology of finite cyclic groups

Let $G$ be a finite cyclic group. Let $g$ be a generator of $G$. Then $I_G = (1 - g)$, so that

$$\hat{H}^{-1}(G, M) = \operatorname{Ker}(N)/\operatorname{Im}(1 - g), \quad \hat{H}^0(G, M) = \operatorname{Ker}(1 - g)/\operatorname{Im}(N)$$

are cohomology groups of the sequence

$$\begin{tikzcd} M \arrow[r, bend left, "N"] & M. \arrow[l, bend left, "1-g"] \end{tikzcd}$$

Moreover, the map $Z^1(G,M)\to M$ carrying $f$ to $f(g)$ induces an isomorphism

$$H^1(G,M)\xrightarrow{\sim}\hat{H}^{-1}(G,M),$$

functorial in $M$.

Theorem 3.2.4 has the following consequence.

**Corollary 3.4.14** (Hilbert 90). *Let $E/F$ be a finite cyclic extension of arbitrary fields of Galois group $G$ and let $g$ be a generator of $G$. Then, for $x\in E^\times$, $N_{E/F}(x)=1$ if and only if $x=gy/y$ for some $y\in E^\times$.*

*Proof.* Indeed, by the theorem, $\hat{H}^{-1}(G,E^\times)\simeq H^1(G,E^\times)=1$, so that $\mathrm{Ker}(N)=\mathrm{Im}(1-g)$. □

Proposition 3.4.8 takes the following form.

**Proposition 3.4.15** (Hexagon). *Let $0\to M'\to M\to M''\to 0$ be a short exact sequence of $G$-modules. Then we have an exact sequence*

$$\begin{tikzcd}
\hat{H}^0(G,M') \arrow[r] & \hat{H}^0(G,M) \arrow[r] & \hat{H}^0(G,M'') \arrow[d] \\
\hat{H}^{-1}(G,M'') \arrow[u] & \hat{H}^{-1}(G,M) \arrow[l] & \hat{H}^{-1}(G,M'). \arrow[l]
\end{tikzcd}$$

**Definition 3.4.16.** The *Herbrand quotient* of a $G$-module $M$ is

$$Q(M)=Q_G(M)=\#\hat{H}^0(G,M)/\#\hat{H}^{-1}(G,M)$$

if it exists.

**Corollary 3.4.17.** *Let $0\to M'\to M\to M''\to 0$ be a short exact sequence of $G$-modules. Then $Q(M)=Q(M')Q(M'')$ (if two of the Herbrand quotients exist, then so does the third one).*

**Remark 3.4.18.** If the underlying set of $M$ is finite, then $Q(M)=1$.

**Example 3.4.19.** $Q(\mathbb{Z})=\#G$, where $G$ acts trivially on $\mathbb{Z}$.

**Proposition 3.4.20.** *Let $V$ be a finite-dimensional real vector space equipped with an action of $G$ by linear automorphisms. Let $L$ and $L'$ be two $G$-stable lattices of $V$. If $Q(L)$ is well-defined, then $Q(L')$ is as well and $Q(L)=Q(L')$.*

*Proof.* By a general result on linear representations of finite groups [S, Section 12.1], we have $L\otimes_{\mathbb{Z}}\mathbb{Q}\simeq L'\otimes_{\mathbb{Z}}\mathbb{Q}$. (This also follows from the Zariski density of $V=\mathrm{End}_{\mathbb{Q}[G]}(L\otimes\mathbb{Q},L'\otimes\mathbb{Q})$ in $V\otimes_{\mathbb{Q}}\mathbb{R}$, since automorphisms form a Zariski open subset.) Thus we may assume that $L$ and $L'$ are commensurable: $L\otimes_{\mathbb{Z}}\mathbb{Q}=L'\otimes_{\mathbb{Z}}\mathbb{Q}$. Then since $L\cap L'$ has finite indices in $L$ and $L'$, we have $Q(L)=Q(L\cap L')=Q(L')$. □

## 3.5 The second inequality

Let $E/F$ be a finite cyclic extension of number fields.

**Theorem 3.5.1** (The second inequality)**.** *We have*

$$\#(\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)) \geq \#\mathrm{Gal}(E/F).$$

In fact, equality holds by the first inequality.

Let $G = \mathrm{Gal}(E/F)$. Recall $\hat{H}^0(G, \mathbb{I}_E/E^\times) \simeq \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)$.

**Theorem 3.5.2.** *The Herbrand quotient $Q(\mathbb{I}_E/E^\times) = [E : F]$.*

This implies the second inequality: $\#\hat{H}^0 = Q\#\hat{H}^{-1} \geq Q = [E : F]$. Moreover, equality holds by the first inequality, so that $\hat{H}^{-1}(G, \mathbb{I}_E/E^\times) = 1$, where $G = \mathrm{Gal}(E/F)$. This can be extended to Galois extensions as follows, which will not be used in the rest of these notes.

**Corollary 3.5.3.** *Let $E/F$ by a finite Galois extension of number fields of group $G$. We have $H^1(G, \mathbb{I}_E/E^\times) = 1$.*

Of course this implies $H^1(G, \mathbb{I}_E) = 1$.

*Proof.* Let $G_p$ be a $p$-Sylow of $G$. If $H^1(G_p, \mathbb{I}_E/E^\times) = 1$, then $H^1(G, \mathbb{I}_E/E^\times)$ is killed by $[G : G_p]$. That this holds for all $p$ implies $H^1(G, \mathbb{I}_E/E^\times) = 1$. Thus we may assume that $G$ is a $p$-group. We proceed by induction on $\#G$. Let $H$ be a nontrivial normal subgroup of $G$. Then by the following lemma, we have an exact sequence

$$1 \to H^1(G/H, \mathbb{I}_K/K^\times) \to H^1(G, \mathbb{I}_E/E^\times) \to H^1(H, \mathbb{I}_E/E^\times),$$

where $K = E^H$. We conclude by the induction hypothesis applied to $G/H$ and to $H$. □

**Lemma 3.5.4.** *Let $G$ be a group and let $H$ be a normal subgroup. Let $A$ be a $G$-module. Then we have an exact sequence*

$$1 \to H^1(G/H, A^H) \xrightarrow{\mathrm{inf}} H^1(G, A) \xrightarrow{\mathrm{res}} H^1(H, A),$$

*where* inf *is the inflation map induced by the map $Z^1(G/H, A^H) \to Z^1(G, A)$ carrying $f$ to the composite $G \to G/H \xrightarrow{f} A^H \to A$.*

*Proof.* This is a routine verification. One can also derive it from the general exact sequence

$$0 \to (R^1\Psi)R^0\Phi \to R^1(\Psi\Phi) \to R^0\Psi R^1\Phi$$

for derived functors of the composition of two additive functors between abelian categories with enough injectives. We take $\Phi = \mathrm{coind}_{G/H}^G$ and $\Psi = (-)^{G/H}$. □

In the cyclic case, $\hat{H}^{-1}(G, \mathbb{I}_E/E^\times) = 1$ implies the following local-global principle.

**Theorem 3.5.5** (Hasse's norm theorem)**.** *Let $E/F$ by a finite cyclic extension of number fields. Let $a \in F^\times$ such that for each place $v$ of $F$, $a$ is a local norm, namely, for one, or equivalently, for every place $w$ above $v$, $a = N_{E_w/F_v}(x_w)$ for some $x_w \in E_w^\times$. Then $a$ is a global norm, namely, there exists $y \in E^\times$ such that $a = N_{E/F}(y)$.*

*Proof.* The short exact sequence $1 \to E^\times \to \mathbb{I}_E \to \mathbb{I}_E/E^\times \to 1$ induces the long exact sequence

$$\hat{H}^{-1}(G, \mathbb{I}_E/E^\times) \to F^\times/N_{E/F}E^\times \xrightarrow{\phi} \mathbb{I}_F/N_{E/F}\mathbb{I}_E.$$

Since $\hat{H}^{-1}(G, \mathbb{I}_E/E^\times) = 1$, $\phi$ is injective. By assumption $\phi(\bar{a}) = 1$, so that $\bar{a} = 1$. □

**Remark 3.5.6.** The second inequality holds for general finite abelian extensions. On the other hand, Theorem 3.5.5 does not hold for general finite abelian extensions (exercise).

## Proof of the second inequality

We now proceed to prove Theorem 3.5.2. We use the notation $\mathbb{I}_{E,S}$ from the proof of Proposition 3.4.5. Note that $\mathbb{I}_E/E^\times\mathbb{I}_{E,S_\infty} \simeq \mathcal{C}l_E$ and the image of $\mathbb{I}_{E,S}$ in $\mathcal{C}l_E$ is generated by the prime ideals above places of $S - S_\infty$. Since $\mathcal{C}l_E$ is finite, we may take $S$ such that the map $\mathbb{I}_{E,S} \to \mathbb{I}_E/E^\times$ is a surjection. We have a short exact sequence

$$1 \to \mathcal{O}_{E,S}^\times \to \mathbb{I}_{E,S} \to \mathbb{I}_E/E^\times \to 1,$$

where $\mathcal{O}_{E,S}^\times = E^\times \cap \mathbb{I}_{E,S}$. We will compute $Q(\mathbb{I}_{E,S})$ and $Q(\mathcal{O}_{E,S}^\times)$.

Let $v$ be a place of $F$ and let $w_0$ be a place of $E$ above $v$. Let $H = D(w_0/v)$. Then $\hat{H}^i(G, \prod_{w|v} E_w^\times) = \hat{H}^i(H, E_{w_0}^\times)$ and $Q_G(\prod_{w|v} E_w^\times) = Q_H(E_{w_0}^\times) = \#H$, by the following proposition. If $v$ is non-Archimedean, then $Q_G(\prod_{w|v} U_w) = Q_H(U_{w_0}) = 1$. If, moreover, $v$ is unramified in $E$, then $\hat{H}^i(G, \prod_{w|v} U_w) \simeq \hat{H}^i(H, U_{w_0}) = 1$ by Lemma 3.4.6. Thus

$$Q_G(\mathbb{I}_{E,S}) = \prod_{v \in S} [E_{w_0} : F_v].$$

**Proposition 3.5.7.** *For any finite cyclic extension $L/K$ of group $H$ of local fields of characteristic 0, then $\#\hat{H}^0(H, L^\times) = Q_H(L^\times) = \#H$. If moreover, $K$ is non-Archimedean, then $Q_H(U_L) = 1$.*

*Proof.* Since $\hat{H}^{-1}(H, L^\times) = 1$, $\#\hat{H}^0(H, L^\times) = Q_H(L^\times)$. The Archimedean case is then obvious. Assume that $K$ is ultrametric. We have an $H$-equivariant short exact sequence $1 \to U_L \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 1$, so that $Q_H(L^\times) = Q_H(U_L)Q_H(\mathbb{Z})$. Since $Q_H(\mathbb{Z}) = \#H$, it suffices to show $Q_H(U_L) = 1$.

The series $\exp(x) = \sum_{n\geq 0} x^n/n!$ and $\log(1 + x) = \sum_{n\geq 1}(-1)^{n+1}x^n/n$ converge for $v_L(x) > v_L(p)/(p - 1)$ and $v_L(x) > 0$, respectively. They induce $H$-equivariant isomorphisms between $\mathfrak{m}_L^a$ and $1 + \mathfrak{m}_L^a$ for some $a \geq 1$. By the normal basis theorem, there exists $\alpha \in L$ such that $h(\alpha)$, $\alpha \in H$ form a linear basis for $L/K$. We may assume that $\alpha \in \mathfrak{m}_L^a$. Then $M = \bigoplus_{h\in H} \mathcal{O}_K h(\alpha) \simeq \mathrm{ind}_{\{1\}}^H \mathcal{O}_K$ is an $H$-submodule of $\mathfrak{m}_L^a$ of finite index. Therefore,

$$Q_H(U_L) = Q_H(1+\mathfrak{m}_L^a) = Q_H(\mathfrak{m}_L^a) = Q_H(M) = Q_{\{1\}}(\mathcal{O}_K) = 1.$$

□

To compute $Q_G(\mathcal{O}_{E,S}^\times)$, consider the $G$-equivariant homomorphism $\lambda\colon \mathcal{O}_{E,S}^\times \to V = \mathbb{R}^{S_E}$ carrying $(x_w)_w$ to $(\log|x_w|_w)_{w\in S_E}$. Here $G$ acts on $V$ via its action on $S_E$. Then $\mathrm{Ker}(\lambda) = \mu_E$ is a finite group and $L = \lambda(\mathcal{O}_{E,S}^\times)$ is a lattice in the hyperplane $\sum_{w\in S_E} a_w = 0$. Let $e = (1,\dots,1) \in V^G$. Then $L \oplus \mathbb{Z}e$ is a $G$-stable lattice of $V$. Another $G$-stable lattice of $V$ is $\mathbb{Z}^{S_E}$. By Proposition 3.4.20,

$$\begin{aligned}\#G Q_G(L) = Q_G(L)Q_G(\mathbb{Z}) = Q_G(L\oplus \mathbb{Z}e) = Q_G(\mathbb{Z}^{S_E})&\\ = \prod_{v\in S} Q_{D(w_0/v)}(\mathbb{Z}) = \prod_{v\in S} \#D(w_0/v).&\end{aligned}$$

Thus $Q_G(\mathcal{O}_{E,S}^\times) = Q_G(L) = \prod_v [E_{w_0} : F_v]/[E:F]$. Therefore,

$$Q_G(\mathbb{I}_E^\times/E^\times) = Q_G(\mathbb{I}_{E,S})/Q_G(\mathcal{O}_{E,S}^\times) = [E:F].$$

## Hasse-Minkowski Theorem

Let $V$ be a finite-dimensional vector space over a field $K$. Recall that a *quadratic form* on $V$ is a map $f\colon V\to K$ such that $f(ax) = a^2 f(x)$ for all $a\in K$ and $x \in V$ and $(x,y)\mapsto f(x+y)-f(x)-f(y)$ is a (symmetric) bilinear form. Assume that the characteristic of $K$ is different from 2. We put $x.y = \frac{1}{2}(f(x+y)-f(x)-f(y))$, so that $Q(x) = x.x$.

Let $a\in K$. We say that a quadratic form $f$ represents $a$ if there exists nonzero $x\in V$ such that $f(x) = a$. Quadratic spaces $(V,f)$ such that $f$ represents 0 (resp. $f=0$) is called *isotropic* (resp. *totally isotropic*). (Some authors use "isotropic" for $f=0$.)

**Theorem 3.5.8.** *Let $F$ be a number field. Then a quadratic form $f$ over $F$ represents 0 if and only if the quadratic form $f_v$ over $F_v$ induced by $f$ represents 0 for every place $v$ of $F$.*

The case $F=\mathbb{Q}$ is due to Minkowski and the general case is due to Hasse.

**Corollary 3.5.9.** *Let $F$ be a number field and let $a\in F$. Then a quadratic form $f$ over $F$ represents $a$ if and only if the quadratic form $f_v$ over $F_v$ induced by $f$ represents $a$ for every place $v$ of $F$.*

This follows from the theorem and a general result on quadratic forms. See Corollary 3.5.11 below.

**Proposition 3.5.10.** *Let $f$ be an isotropic nondegenerate quadratic form over a field $K$ of characteristic $\neq 2$. Then $f$ has the form $f(X,Y,W_1,\dots,W_n) = XY + g(W_1,\dots,W_n)$. In particular, $f$ represents every $a\in K$.*

*Proof.* Let $x \neq 0$ be an isotropic vector. Since $f$ is nondegenerate, there exists $z \in V$ such that $x.z = 1$. Then $y = z - \frac{1}{2}(z.z)x$ is an isotropic vector and $x.y = 1$. Then $f$ has the desired form under the basis which is the union of $\{x, y\}$ and a basis of $(xK + yK)^\perp$. □

**Corollary 3.5.11.** *Let $g$ be a nondegenerate quadratic form and let $a \in K$. Then $g$ represents $a$ if and only if $g(Y_1, \dots, Y_n) - aX^2$ represents $0$.*

*Proof.* The "only if" part is trivial by taking $X = 1$. For the "if" part, assume $g(y) - ax^2 = 0$. If $x = 0$, then $g$ represents $0$, hence $g$ represents $a$ by the proposition. If $x \neq 0$, then we may assume $x = 1$ so that $g(y) = a$. □

The "only if" part of Theorem 3.5.8 is trivial. For the "if" part, we have $f = a_1X_1^2 + \cdots + a_nX_n^2$, $a_i \in F^\times$ under an orthogonal basis. We may assume $a_1 = 1$ and $f$ is nondegenerate.

**Remark 3.5.12.** Let $K$ be a field of characteristic $\neq 2$ and $a \in K^\times$. Then $X^2 - aY^2$ represents $0$ if and only if $a$ is a square in $K$.

For $n = 2$, $f = X^2 - aY^2$. Since $f_v$ represents $0$, $a$ is a square in $F_v$. Thus $N_{F(\sqrt{a})/F}(\mathbb{I}_{F(\sqrt{a})}) = \mathbb{I}_F$. By the second inequality, $[F(\sqrt{a}) : F] \leq 1$, so that $a$ is a square. One may also use a density argument instead of the second inequality.

For $n = 3$, the theorem follows from the following algebraic result and Hasse's norm theorem.

**Lemma 3.5.13.** *Let $K$ be a field of characteristic $\neq 2$ and $a, b \in K^\times$. Then $X^2 - aY^2 - bZ^2$ represents $0$ if and only if $a \in N_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$.*

*Proof.* If $b = \beta^2$ is a square, both conditions are automatic, with $(\beta, 0, 1)$ being an isotropic vector. Assume that $b$ is not a square. For the "only if" part, note that if $a = N_{K(\sqrt{b})/K}(x - \sqrt{b}z) = x^2 - bz^2$, then $(x, 1, z)$ is an isotropic vector. For the "if" part, if $x^2 - ay^2 - bz^2 = 0$, then $y \neq 0$, so that $a = (x/y)^2 - b(z/y)^2$ is a norm. □

**Remark 3.5.14.** If $K = F_v$ is a local field of characteristic 0, the last condition means that the Hilbert symbol $(a, b)_v = 1$. Thus if $f$ is a quadratic form in 3 variables over a number field $F$, then $f$ represents $0$ in $F_v$ for all but a finite and even number of places $v$. It follows that if $f$ is a quadratic form of at least 3 variables over $F$, then $f$ represents $0$ in $F_v$ for all but finitely many places $v$. Indeed, we may assume $f$ nondegenerate, and if $f(X_1, \dots, X_n) = g(X_1, \dots, X_3) + h(X_4, \dots, X_n)$ with $g$ representing $0$ in $F_v$, then $f$ represents every element of $F_v$, and so does $f$.

For $n = 4$, the theorem follows from the following algebraic result either by reducing to the case $n = 3$ or by Hasse's norm theorem.

**Proposition 3.5.15.** *Let $K$ be a field of characteristic $\neq 2$ and $a, b, c \in K^\times$. The following conditions are equivalent:*

*(1) $X^2 - bY^2 - cZ^2 + acW^2$ represents $0$ in $K$;*

*(2) $c \in N_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)N_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$;*

*(3) $c \in N_{L/K(\sqrt{ab})}L^\times$, where $L = K(\sqrt{a}, \sqrt{b})$;*

*(4)* $X^2 - bY^2 - cZ^2$ *represents* $0$ *in* $K(\sqrt{ab})$.

*Proof.* If $a$ or $b$ is a square in $K$, then the conditions are all automatic. Assume that neither $a$ nor $b$ is a square. In this case (1) and (2) are clearly equivalent. By the lemma, (3) and (4) are equivalent, because $L = K(\sqrt{ab}, \sqrt{b})$. If $ab$ is a square in $K$, then $L = K(\sqrt{a}) = K(\sqrt{b})$, and (2) and (3) are clearly equivalent. Assume that $ab$ is not a square in $K$. Then $L/K$ is a biquadratic extension. Let $\mathrm{Gal}(L/K(\sqrt{b})) = \{1, g\}$ and $\mathrm{Gal}(L/K(\sqrt{a})) = \{1, h\}$. Then $\mathrm{Gal}(L/K(\sqrt{ab})) = \{1, gh\}$. Note that (2) means that there exists $x \in K(\sqrt{a})^\times$ and $y \in K(\sqrt{b})^\times$ such that $c = x(gx)y(hy) = xy((gh)(xy))$. Thus (2) implies (3). Conversely, assume (3). We have $c = z(ghz)$ for some $z \in L^\times$. Take $u = gz/z = gz(hgz)/c$. Then $hu = u$, namely $u \in K(\sqrt{a})$. Moreover, $u(gu) = 1$, and by Hilbert 90, we have $u = gx/x$ for some $x \in K(\sqrt{a})$. Let $y = z/x$. Then $gy/y = 1$, namely $y \in K(\sqrt{b})$, and $c = xy((gh)(xy))$, which is (2). □

For $n \geq 5$, we proceed by induction. Let $f(X_1, \dots, X_n) = aX_1^2 + bX_2^2 - g(X_3, \dots, X_n)$. Since $g$ has at least 3 variables, $g$ represents 0 in $F_v$ for all places $v$ outside a finite set $S$ by Remark 3.5.14. For such $v$, $g$ represents every element of $F_v$. For each $v \in S$, there exist by assumption $x_{1,v}, x_{2,v} \in F_v$ such that $g$ represents $c_v = ax_{1,v}^2 + bx_{2,v}^2$ in $F_v$. By weak approximation, there exist $x_1, x_2 \in K$ such that $c = ax_1^2 + bx_2^2 \in c_v(\mathbb{F}_v^\times)^2$. Then $g$ represents $c$ in $F_v$ for all $v$. Thus $g$ represents $c$ in $F$ by induction hypothesis. It follows that $f$ represents 0 in $F$.

**Remark 3.5.16.** One can show that a quadratic form over a local field of characteristic 0 in at least 5 variables represents 0 unless the field is $\mathbb{R}$ and the form is definite. It follows then from the Hasse-Minkowski theorem that a quadratic form $f$ over a number field $F$ in at least 5 variables represents 0 unless there exists a real place of $F$ at which $f$ is definite.

A field $K$ is called $C_k$ if every homogeneous polynomial over $K$ of degree $d$ in more than $d^k$ variables has a nontrivial zero. Thus a field is $C_0$ if and only if it is algebraically closed. Artin conjectured that $p$-adic fields are $C_2$, namely that every homogeneous polynomial of degree $d$ over such fields in more than $d^2$ variables has a nontrivial zero. Lewis proved the case $d = 3$ but Terjanian disproved the general case. On the other hand the field $\mathbb{F}_q((T))$ is $C_2$, and model theory implies the Ax-Kochen theorem: every homogeneous polynomial over a $p$-adic field $K$ in more than $d^2$ variables has a nontrivial zero for $p$ large enough (depending on $d$ and $[K : \mathbb{Q}_p]$).

**Remark 3.5.17.** Theorem 3.5.8 fails for homogeneous polynomials of degree $\geq 3$. For example, Selmer showed that $C\colon 3X^3 + 4Y^3 + 5Z^3 = 0$ has a nontrivial solution in each $\mathbb{Q}_p$ but not in $\mathbb{Q}$. This example gives a nontrivial element (of order 3) of the Tate-Shafarevich group of the elliptic curve $E\colon X^3 + Y^3 + 60Z^3 = 0$ over $\mathbb{Q}$. In general, the Jacobian of $C\colon aX^3 + bY^3 + cZ^3 = 0$ over a field $F$ of characteristic zero is $E\colon X^3 + Y^3 + dZ^3 = 0$ with $[1 : -1 : 0]$ as the origin, where $a, b, c \in F^\times$, $d = abc$. Choosing $\alpha^3 = a$, $\beta^3 = b$, we get an isomorphism $f\colon C_{\bar{F}} \to E_{\bar{F}}$ carrying $[x : y : z]$ to $[\alpha x : \beta y : \alpha^{-1}\beta^{-1}z]$. For $\sigma \in G_F = \mathrm{Gal}(\bar{F}/F)$,

$$(\sigma f)[x : y : z] = [\zeta_\alpha x : \zeta_\beta y : \zeta_\alpha^{-1}\zeta_\beta^{-1} z] = f[x : y : z] + [\zeta_\beta/\zeta_\alpha : -1 : 0].$$

Here $\zeta_\alpha = \sigma(\alpha)/\alpha$, $\zeta_\beta = \sigma(\beta)/\beta$ are cube roots of unity. Thus the substraction map $C \times C \to E$ carrying $(P, Q)$ to $f(P) - f(Q)$ is defined over $F$. Any genus 1 curve $C$ is a torsor under its Jacobian $E$ with substraction $C \times C \to E$ carrying $(P, Q)$ to the class of the divisor $P - Q$.

The *Tate-Shafarevich group* of an abelian variety $A$ over a number field $F$ is

$$Ш(A/F) := \bigcap_v \mathrm{Ker}(H^1(G_F, A) \to H^1(G_{F_v}, A)).$$

The *Weil-Châtelet group* $\mathrm{WC}(A/F)$ is the group of isomorphism classes of $A$-torsors. It can be identified with $H^1(G_F, A)$, an $A$-torsor $M$ corresponding to the class of the crossed homomorphism $\sigma \mapsto \sigma P - P$, where $P \in M(\bar{F})$. An $A$-torsor is trivial if and only if it has rational point. Thus $Ш(A/F)$ measures the failure of the local-global principle for the existence of rational points on $A$-torsors. The Tate-Sharafevich conjecture states that $Ш(A/F)$ is finite.

**Remark 3.5.18.** For homogeneous polynomials $f$ in *two variables* of degree $\geq 2$ over a number field, a density argument shows that if $f$ has a nontrivial zero in $F_v$ for all but finitely many $v$, then $f$ is reducible in $F$ (exercise) and, if $\deg(f) \leq 4$, then $f$ has a nontrivial zero in $F$. Indeed, if $f$ is a product of two irreducible quadratic polynomials, then the density of places $v$ of $F$ such that $f$ has a nontrivial zero in $F_v$ is at most 3/4. For $d \geq 5$, there are homogeneous polynomials of degree $d$ in two variables over $\mathbb{Q}$ that have nontrivial zeroes in $\mathbb{Q}_p$ for all $p$ and in $\mathbb{R}$ but not in $\mathbb{Q}$: $(X^2 + 3Y^2)^m(X^3 - 19Y^3)$ (if $p \equiv 1 \mod 3$ the first factor has a nontrivial zero, otherwise the second factor does), $(X^2 + Y^2)^m(X^2 - 17Y^2)(X^2 + 17Y^2)$.

In particular, for $n \leq 4$, if $a \in F$ is an $n$-th power in $F_v$ for all but finitely many $v$, then $a$ is an $n$-th power in $F$. This also holds for more general $n$-th powers, with a few exceptional cases, as follows.

Let $F$ be a number field. Let $\eta_r = \zeta_{2^r} + \zeta_{2^r}^{-1}$. Then

$$\eta_{r+1}^2 = 2 + \eta_r, \quad \zeta_{2^{r+1}}\eta_{r+1} = \zeta_{2^r} + 1,$$

so that there exists a unique integer $s \geq 2$ such that $\eta_s \in F$ but $\eta_{s+1} \notin F$.

**Theorem 3.5.19** (Grunwald-Wang)**.** *Let $S$ be a finite set of places of $F$, and let $P(n, S) \subseteq F^\times$ be the subgroup consisting of $a \in F^\times$ such that $a$ is an $n$-th power in $F_v$ for all $v \notin S$. Then $P(n, S) = F^{\times n}$, except under the following conditions:*

*(1) $2^{s+1} \mid n$.*
*(2) $-1$, $2 + \eta_s$, and $-(2 + \eta_s)$ are non-squares in $F$.*
*(3) $S \supseteq S_0$, where $S_0$ is the set of places $v \mid 2$ such that $-1$, $2 + \eta_s$, and $-(2 + \eta_s)$ are non-squares in $F_v$.*

*Under these conditions, $P(n, S) = F^{\times n} \cup \eta_{s+1}^n F^{\times n}$.*

We refer to [AT, Chapter X] for a proof.

For $F = \mathbb{Q}$, we have $s = 2$ and condition (2) is satisfied. Moreover, $S_0 = \{2\}$, so the theorem implies that if $a \in \mathbb{Q}$ is an $n$-th power in $\mathbb{Q}_2$ and in $\mathbb{Q}_p$ for all but finitely many $p$, then $a$ in an $n$-th power in $\mathbb{Q}$. One cannot omit $\mathbb{Q}_2$ if $8 \mid n$:

$$16 = (1 + i)^8 = (1 - i)^8 = (\sqrt{2})^2 = (\sqrt{-2})^8$$

is an 8-th power in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$ odd (because at least one of $-1$, 2, and $-2$ is a square in $\mathbb{Q}_p$), but 16 is not an 8-th power in $\mathbb{Q}_2$ or $\mathbb{Q}$.

For $F = \mathbb{Q}(\sqrt{d})$ with $d$ a square-free integer satisfying $d \equiv -1 \mod 8$ and $d \neq -1$ (for example $d = 7$), we have $s = 2$ and condition (2) is satisfied. Since $-d$ is a square in $\mathbb{Q}_2$, $-1$ is a square in $\mathbb{Q}_2(\sqrt{d})$ and $S_0 = \emptyset$. The number 16 is an 8-th power in every $F_v$, but not an 8-th power in $F$.

## 3.6 Artin reciprocity

Let $E/F$ be a finite Galois extension of number fields and let $S$ be a finite set of maximal ideals of $\mathcal{O}_F$ containing those ramified in $E$. We have homomorphisms $\mathcal{I}_F^S \to \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)$ and $A_{E/F}^S \colon \mathcal{I}_F^S \to G^{\mathrm{ab}}$ (3.1.7), where $G = \mathrm{Gal}(E/F)$, carrying $\mathfrak{p}$ to the class of $\pi_\mathfrak{p}$ and $\mathrm{Frob}_{\mathfrak{p},E/F}$, respectively. Note that $\mathcal{I}_F^S \to \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E)$ is a surjection. We will prove the following form of Artin reciprocity.

**Theorem 3.6.1.** *The Artin homomorphism $A_{E/F}^S$ factorizes into*

$$\mathcal{I}_F^S \to \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E) \xrightarrow{\sim} G^{\mathrm{ab}}.$$

**Remark 3.6.2.** The Artin map is functorial in the following sense: For finite Galois extensions of number fields $E/F$ and $E'/F'$ and a homomorphism $\tau\colon E \to E'$ such that $\tau(F) \subseteq F'$, the diagram

$$\begin{tikzcd}
\mathcal{I}_{F'}^{S_{F'}} \arrow[r, "A_{E'/F'}"] \arrow[d, "N_{F'/F}"'] & \mathrm{Gal}(E'/F')^{\mathrm{ab}} \arrow[d] \\
\mathcal{I}_F^S \arrow[r, "A_{E/F}"] & \mathrm{Gal}(E/F)^{\mathrm{ab}}
\end{tikzcd}$$

commutes. Here the right vertical arrow is induced by the homomorphism $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$ given by restriction by $\tau$. Indeed, $\left(\frac{E'/F'}{\mathfrak{p}'}\right)|_F = \left(\frac{E/F}{\mathfrak{p}}\right)^f$, where $f = f(\mathfrak{p}'/\mathfrak{p})$ is the degree of the residue field extension.

It follows that the reciprocity isomorphism also satisfies functoriality: The diagram

$$\begin{tikzcd}
\mathbb{I}_{F'}/F'^\times N_{E'/F'}(\mathbb{I}_{E'}) \arrow[r, "\sim"] \arrow[d, "N_{F'/F}"'] & \mathrm{Gal}(E'/F')^{\mathrm{ab}} \arrow[d] \\
\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E) \arrow[r, "\sim"] & \mathrm{Gal}(E/F)^{\mathrm{ab}}
\end{tikzcd}$$

commutes.

In the rest of this section we assume that $E/F$ is an abelian extension. The general case will follow from the existence theorem (Remark 3.7.7).

**Remark 3.6.3.** It suffices to show that there exists a modulus $m$ for $F$ such that $S = \mathrm{supp}(m) \cap V_f$ and such that $A_{E/F}^S$ is trivial on $\mathcal{P}_F(m)$. Indeed, since $A_{E/F}^S$ is trivial on $N_{E/F}(\mathcal{I}_E(m))$, this implies that $A^m_{E/F}$ factorizes into

$$\begin{tikzcd}
\mathcal{I}_F(m) \arrow[r] \arrow[d] & \mathcal{I}_F(m)/\mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m)) \arrow[d, "\simeq"] & \\
\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_F) \arrow[r, "\psi"] & \mathbb{I}_F/F^\times U_{F,m}N_{E/F}(\mathbb{I}_F) \arrow[r, "\phi"] & G.
\end{tikzcd}$$

By the surjectivity of $A^S_{E/F}$ (Corollary 3.3.8), $\psi\phi$ is a surjection. By the first inequality,

$$\#\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_F) \le \#G.$$

Therefore, $\psi\phi$ is an isomorphism.

We omit the superscript from the notation and write $A_{E/F}$ when no confusion arises.

**Example 3.6.4.** Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\zeta_n)$, $m = ((n), 1)$. Then $A_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \colon \mathcal{I}^m_{\mathbb{Q}} \to G = (\mathbb{Z}/n\mathbb{Z})^\times$ carries $p$ to $p$ mod $n$ for primes $p \nmid n$, hence is trivial on $\mathcal{P}_{\mathbb{Q}}(m)$.

**Remark 3.6.5.** We have the following reductions.

(1) Let $K/F$ be a finite extension. Then we have a commutative diagram

$$\begin{tikzcd}
\mathcal{I}^{S_K}_K \arrow[r, "A^{S_K}_{EK/K}"] \arrow[d, "N_{K/F}"'] & \mathrm{Gal}(EK/K) \arrow[d, hook] \\
\mathcal{I}^S_F \arrow[r, "A^S_{E/F}"] & \mathrm{Gal}(E/F).
\end{tikzcd}$$

Since $N_{E/F}(\mathcal{P}_K(m_K)) \subseteq \mathcal{P}_F(m)$, if $A_{E/F}$ is trivial on $\mathcal{P}_F(m)$, then $A_{EK/K}$ is trivial on $\mathcal{P}_K(m_K)$. Here $m_K = (\mathfrak{a}\mathcal{O}_K, (m_{w|_F})_w)$ for $m = (\mathfrak{a}, (m_v)_v)$.

(2) Let $F \subseteq E' \subseteq E$. Then $A^S_{E'/F}$ is the composite

$$\mathcal{I}^S_F \xrightarrow{A^S_{E/F}} \mathrm{Gal}(E/F) \to \mathrm{Gal}(E'/F).$$

Thus if $A_{E/F}$ is trivial on $\mathcal{P}_F(m)$, then $A_{E'/F}$ is trivial on $\mathcal{P}_F(m)$ as well.

(3) Let $G = \prod_i G_i$. Then the $i$-th component of $A^S_{E/F}$ is $A^S_{E_i/F}$, where $E_i = E^{\prod_{j\neq i} G_j}$. Thus if $A^S_{E_i/F}$ is trivial on $\mathcal{P}_F(m_i)$, then $A^S_{E/F}$ is trivial on $\mathcal{P}_F(m)$, where $m_v = \max_i m_{i,v}$.

By (1), (2) and Example 3.6.4, $A_{E/F}$ is trivial on $\mathcal{P}_F(m)$ for $m = (n\mathcal{O}_F, 1)$ if $E \subseteq F(\zeta_n)$.

By (3), we may assume that $E/F$ is a cyclic extension. For $v \notin S$, $U_v \subseteq N_{E/F}(\mathbb{I}_E)$. Thus we can take $m$ so that $U_{F,m} \subseteq N_{E/F}(\mathbb{I}_E)$. By the second inequality, $\#\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_F) = \#G$, so that $\mathrm{Ker}(A^m_{E/F})$ and $\mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m_E))$ have the same index in $\mathcal{I}_F(m)$. Therefore, $\mathrm{Ker}(A^m_{E/F}) \supseteq \mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m_E))$ if and only if $\mathrm{Ker}(A^m_{E/F}) \subseteq \mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m_E))$. Let $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_r^{\alpha_r} \in \mathrm{Ker}(A^m_{E/F})$. We want $\mathfrak{a} \in \mathcal{P}_F(m)N_{E/F}(\mathcal{I}_E(m_E))$. The strategy, roughly speaking, is to reduce to the known case of an extension contained in a cyclotomic extension, by the commutative diagram in (1) applied backwards. The actual proof will consist of constructing one $K_i$ for each $\mathfrak{p}_i$. We need the following lemma.

**Lemma 3.6.6.** *Let $E/F$ be a finite cyclic extension of number fields of degree $d$. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$ and let $t$ be a rational integer in $\mathfrak{p}$. Then there exist an integer $n$ prime to $t$ and $\tau \in \mathrm{Gal}(F(\zeta_n)/F)$ of order a multiple of $d$ such that $E \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, $\mathrm{Frob}_{\mathfrak{p},F(\zeta_n)/F}$ has order a multiple of $d$, and $\langle \mathrm{Frob}_{\mathfrak{p},F(\zeta_n)/F}\rangle \cap \langle \tau \rangle = \{1\}$.*

Note that $(n,t) = 1$ implies that the prime factors of $t$ are unramified in $\mathbb{Q}(\zeta_n)$, so that $\mathfrak{p}$ is unramified in $F(\zeta_n)$. Moreover, $E \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ implies $E \cap F(\zeta_n) = F$, $F \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$,

$$\mathrm{Gal}(E(\zeta_n)/E) \simeq \mathrm{Gal}(F(\zeta_n)/F) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times,$$

and $\mathrm{Gal}(E(\zeta_n)/F) \simeq \mathrm{Gal}(E/F) \times \mathrm{Gal}(F(\zeta_n)/F)$.

The proof of Lemma 3.6.6 makes use of the following technical lemma, which we leave as an exercise.

**Lemma 3.6.7.** *Let $a > 1$, $d > 0$ be integers and let $s$ be a multiple of $a$. Then there exist an integer $n$ prime to $s$ and $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ of order a multiple of $d$, such that the image $\bar{a}$ of $a$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ has order a multiple of $d$, and $\langle \bar{a} \rangle \cap \langle b \rangle = \{1\}$.*

*Proof of Lemma 3.6.6.* We apply the lemma to $a = N\mathfrak{p}$ and $s$ the product of $at$ with all rational primes ramified in $E$. Since no rational prime ramifies in $E \cap \mathbb{Q}(\zeta_n)$, we have $E \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. (Recall that $\mathbb{Q}$ has no nontrivial extension unramified at every $p$ by the bound $\sqrt{|\Delta_K|} \geq (\frac{\pi}{4})^{d/2} d^d/d!$ [N, Proposition III.2.14] for every number field $K$ of degree $d$.) Then $\mathrm{Frob}_{\mathfrak{p},F(\zeta_n)/F}$ corresponds to $\bar{a}$. We take $\tau \in \mathrm{Gal}(F(\zeta_n)/F)$ to be the element corresponding to $b$. □

Applying Lemma 3.6.6 successively to $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, we obtain pairwise coprime integers $n_1, \dots, n_r$, prime to $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and to maximal ideals in the support of $m$, and $\tau_i \in \mathrm{Gal}(F(\zeta_{n_i})/F)$. Let $g$ be a generator of $G$ and let $K_i \subseteq E(\zeta_{n_i})$ be the subfield fixed by $(g, \tau_i)$ and $\mathrm{Frob}_{\mathfrak{p}_i,E(\zeta_{n_i})/F} = (\mathrm{Frob}_{\mathfrak{p}_i,E/F}, \mathrm{Frob}_{\mathfrak{p}_i,F(\zeta_{n_i})/F})$. Note that $\mathfrak{p}_i$ splits in $K_i$. We have $E(\zeta_{n_i}) = K_i(\zeta_{n_i})$, so that $EK_i$ is contained in $K_i(\zeta_{n_i})$. Indeed, for $h = (g,\tau_i)^\alpha (\mathrm{Frob}_{\mathfrak{p}_i,E/F}, \mathrm{Frob}_{\mathfrak{p}_i,F(\zeta_{n_i})/F})^\beta \in \mathrm{Gal}(E(\zeta_{n_i})/K_i)$, if $h$ fixes $\zeta_{n_i}$, then $\tau_i^\alpha \mathrm{Frob}^\beta_{\mathfrak{p}_i,F(\zeta_{n_i})/F} = 1$, so that $\tau_i^\alpha = \mathrm{Frob}^\beta_{\mathfrak{p}_i,F(\zeta_{n_i})/F} = 1$. It follows that $\alpha$ and $\beta$ are multiples of $d$, so that $h = 1$.

Let $K = K_1 \cdots K_r$. We have $E \cap K = F$, so that $\mathrm{Gal}(EK/K) \xrightarrow{\sim} \mathrm{Gal}(E/F)$. Indeed $\mathrm{Gal}(E(\zeta_{n_1}, \dots, \zeta_{n_r})/F) \simeq \mathrm{Gal}(E/F) \times (\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times$. Since $K$ is fixed by $(g, \tau_1, \dots, \tau_r)$, $E \cap K$ is fixed by $g$.

Let $A_{E/F}(\mathfrak{p}_i^{\alpha_i}) = g^{\beta_i}$, $\beta_i \in \mathbb{Z}$. Then $1 = A_{E/F}(\mathfrak{a}) = g^{\sum_i \beta_i}$. We may assume $\sum_i \beta_i = 0$. We have a commutative diagram

$$\begin{tikzcd}
\mathcal{I}_K^{S'_K} \arrow[r, "A_{EK/K}"] \arrow[d, "N_{K/F}"'] & \mathrm{Gal}(EK/K) \arrow[d, "\simeq"] \\
\mathcal{I}_F^{S'} \arrow[r, "A_{E/F}"] & \mathrm{Gal}(E/F).
\end{tikzcd}$$

Here $S' \supseteq S$) and contains all maximal ideals dividing one of the $n_i$'s. Let $\tilde{g}$ be the generator of $\mathrm{Gal}(EK/K)$ of image $g$. By the surjectivity of $A_{EK/K}$, there exists

$\tilde{\mathfrak{b}} \in \mathcal{I}_K^{S_K}$ such that $A_{EK/K}(\tilde{\mathfrak{b}}) = \tilde{g}$. Then $A_{E/F}(\mathfrak{b}) = g$, where $\mathfrak{b} = N_{K/F}(\tilde{\mathfrak{b}})$. Since $\mathfrak{p}_i$ splits in $K_i$, it is a norm from $K_i$ to $F$, so that there exists $\mathfrak{c}_i \in \mathcal{I}_{K_i}^{S_{K_i}}$ such that $N_{K_i/F}(\mathfrak{c}_i) = \mathfrak{p}_i^{\alpha_i}\mathfrak{b}^{-\beta_i}$, so that $A_{E/F}(N_{K_i/F}(\mathfrak{c}_i)) = 1$. By the analogue of the above diagram for $K_i$, we get $A_{EK_i/K_i}(\mathfrak{c}_i) = 1$. Since $EK_i$ is contained in $K_i(\zeta_{n_i})$, there exists $\mu_i \geq m_{K_i}$ and $\mathfrak{d}_i \in \mathcal{I}_{EK_i}(\mu_i)$, $x_i \in \mathcal{P}_{K_i}(\mu_i)$ such that $\mathfrak{c}_i = (x_i)N_{EK_i/K_i}(\mathfrak{d}_i)$. Therefore,

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{\alpha_i}\mathfrak{b}^{-\beta_i} = \prod_i N_{K_i/F}(\mathfrak{c}_i) = \prod_i (N_{K_i/F}(x_i))N_{EK_i/F}(\mathfrak{d}_i) = (y)N_{E/F}(\mathfrak{e}),$$

where $y = \prod_i N_{K_i/F}(x_i) \in \mathcal{P}_F(m)$, and $\mathfrak{e} = \prod_i N_{EK_i/E}(\mathfrak{d}_i) \in \mathcal{I}_E(m)$.

This finishes the proof of Artin reciprocity for abelian extensions.

## 3.7 Existence theorem

Let $F$ be a number field. We say that an open subgroup of $\mathbb{I}_F$ containing $\mathbb{F}^\times$ is *normic* if it is of the form $\mathcal{N}_E = F^\times N_{E/F}(\mathbb{I}_E)$ for some finite abelian extending $E/F$. The goal of this section is to prove Theorem 3.1.19, namely that every open subgroup of $\mathbb{I}_F$ containing $F^\times$ is normic. The strategy of the proof is to reduce to a Kummer extension, where the class field can be constructed directly.

**Lemma 3.7.1.** *If $\mathcal{N}$ is normic and $\mathcal{N}' \supset \mathcal{N}$, then $\mathcal{N}'$ is normic.*

*Proof.* We have $\mathcal{N} = \mathcal{N}_E$, $E/F$ finite abelian. This induces a commutative diagram

$$\begin{tikzcd}
\mathbb{I}_F^\times/\mathcal{N}_E \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(E/F) \arrow[d] \\
\mathbb{I}_F^\times/\mathcal{N}' \arrow[r, "\sim"] & \mathrm{Gal}(E'/F),
\end{tikzcd}$$

where $F \subseteq E' \subseteq E$. It is clear that the lower horizontal arrow is the Artin isomorphism for $E'$. □

**Lemma 3.7.2.** *Let $K/F$ be a finite abelian extension and let $\mathcal{N}$ be an open subgroup of $\mathbb{I}_F$ containing $F^\times$. If $\mathcal{N}' = N_{K/F}^{-1}(\mathcal{N}) \subseteq \mathbb{I}_K$ is normic, then $\mathcal{N}$ is normic.*

*Proof.* We have $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = K$ such that each $F_{i+1}/F_i$ is cyclic. We may assume that $K/F$ is acyclic.

We have $\mathcal{N}' = \mathcal{N}_{L/K}$, $L/K$ finite abelian. Let us show that $L/F$ is a Galois extension. Let $\sigma$ be an $F$-embedding of $L$ into a separable closure of $K$. Then $\sigma K = K$ and $\sigma\mathcal{N}' = \mathcal{N}'$. But by functoriality, $\sigma\mathcal{N}_{L/K} = \mathcal{N}_{\sigma L/K}$. Thus $L = \sigma L$.

Next we show that $L/F$ is an abelian extension. We use the fact that for an exact sequence of groups $1 \to A \to G \to C \to 1$ with $A$ abelian and $C$ cyclic, $G$ is abelian if and only if the action of $C$ on $A$ by conjugation is trivial. For $\tau \in \mathrm{Gal}(L/F)$, we have a commutative diagram

$$\begin{tikzcd}
\mathbb{I}_K/\mathcal{N}_{L/K} \arrow[r, "\sim"] \arrow[d, "\tau"'] & \mathrm{Gal}(L/K) \arrow[d] \\
\mathbb{I}_K/\mathcal{N}_{L/K} \arrow[r, "\sim"] & \mathrm{Gal}(L/K),
\end{tikzcd}$$

where the right vertical arrow is conjugation by $\tau$. For $x \in \mathbb{I}_K$, $N_{K/F}(\tau x) = N_{K/F}(x)$, so that $\tau x/x \in \mathcal{N}'$. Thus the left vertical arrow is the identity. It follows that the right vertical arrow is the identity. This finishes the proof that $L/F$ is abelian.

We have $\mathcal{N} \supseteq F^\times N_{K/F}(\mathcal{N}') = F^\times N_{L/F}(\mathbb{I}_L) = \mathcal{N}_L$. Therefore, $\mathcal{N}$ is normic by the preceding lemma. □

**Remark 3.7.3.** It suffices to show that any open subgroup $\mathcal{N} \subseteq \mathbb{I}_F$ of exponent $n$ containing $F^\times$ is normic under the assumption that $F$ contains all $n$-th roots of unity. Indeed, let $K = F(\zeta_n)$, which is an abelian extension of $F$. Then $\mathbb{I}_K/N_{K/F}^{-1}(\mathcal{N}) \to \mathbb{I}_F/\mathcal{N}$ is an injection, so that the exponent of $N_{K/F}^{-1}(\mathcal{N})$ has exponent dividing $n$. The assertion then follows from the preceding lemma. (By a more elaborate reduction we may even assume $n$ is a prime, but this does not make the proof simpler.)

Now let $F$ be a number field containing all $n$-th roots of unity and let $\mathcal{N}$ be an open subgroup of $\mathbb{I}_F$ of exponent dividing $n$ containing $F^\times$. Then $\mathcal{N}$ contains $F_v^{\times n}$ for all places $v$ of $F$. Moreover, there exists a finite set of places $S$ of $F$ containing all Archimedean places such that $U_v \in \mathcal{N}$ for all $v$ not in $S$. Since the class group $\mathcal{C}l_F$ is finite, we may enlarge $S$ so that $\mathbb{I}_F = F^\times \mathbb{I}_{F,S}$. We may further enlarge $S$ such that $S$ contains all places dividing $n$. Since $\mathcal{N} \supseteq F^\times \prod_{v\in S} F_v^{\times n} \prod_{v\notin S} U_v$, the existence theorem follows from the following theorem.

**Theorem 3.7.4.** *Let $F$ be a number field containing the $n$-th roots of unity and let $S$ be a finite set of places of $F$ containing all Archimedean places and all places dividing $n$ such that $\mathbb{I}_F = F^\times \mathbb{I}_{F,S}$. Let $\mathcal{N} = F^\times \prod_{v\in S} F_v^{\times n} \prod_{v\notin S} U_v$. Then $\mathcal{N} = \mathcal{N}_E$, where $E = F(\sqrt[n]{\mathcal{O}_{F,S}^\times})$.*

Note that $E/F$ is a finite extension. Indeed,

$$[E : F] = \#(\mathcal{O}_{F,S}^\times F^{\times n}/F^{\times n}) = \#(\mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^\times \cap F^{\times n}) = \#(\mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^{\times n}) = n^{\#S}.$$

Here in the last equality we have used the fact that $\mathcal{O}_{F,S}$ is the product of $\mu_F$ with a free abelian group of rank $\#S - 1$.

*Proof.* By Artin reciprocity, $\mathcal{N}_E \supseteq F_v^{\times n}$ for all places $v$ of $F$. Moreover, for $x \in \mathcal{O}_{F,S}^\times$ and $v \notin S$, $F(\sqrt[n]{x})/F$ is unramified at $v$. Thus $E/F$ is unramified at $v$ so that $\mathcal{N}_E \supseteq U_v$ for $v \notin S$. Therefore, $\mathcal{N}_E \supseteq \mathcal{N}$. It suffices to show $\#(\mathbb{I}_F/\mathcal{N}) = \#(\mathbb{I}_F/\mathcal{N}_E)$. We have seen

$$\#(\mathbb{I}_F/\mathcal{N}_E) = [E : F] = n^{\#S}.$$

To compute $\#(\mathbb{I}_F/\mathcal{N})$, we use the short exact sequence

$$1 \to \mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^{\times n} \xrightarrow{\phi} \prod_{v\in S} F_v^\times / \prod_{v\in S} F_v^{\times n} \xrightarrow{\psi} \mathbb{I}_F/\mathcal{N} \to 1.$$

The exactness at the middle term is clear. For the surjectivity of $\psi$, we use $\mathbb{I}_F = F^\times \mathbb{I}_{F,S}$. The injectivity of $\phi$ is equivalent to $\mathcal{O}_{F,S}^\times \cap \prod_{v\in S} F_v^{\times n} = \mathcal{O}_{F,S}^{\times n}$. It is clear that $\mathcal{O}_{F,S}^\times \cap \prod_{v\in S} F_v^{\times p} \supseteq \mathcal{O}_{F,S}^{\times n}$. Conversely, for $x \in \mathcal{O}_{F,S}^\times \cap \prod_{v\in S} F_v^{\times n}$, $v$ splits in $K = F(\sqrt[n]{x})$ for $v \in S$ and $v$ is unramified in $K$ for $v \notin S$. It follows that $\mathcal{N}_K \supseteq F^\times \mathbb{I}_{F,S} = \mathbb{I}_F$, so that $\mathcal{N}_K = \mathbb{I}_F$, which is equivalent to $K = F$, namely, $x \in F^{\times n}$. Therefore, $x \in \mathcal{O}_{F,S}^{\times n}$.

Since $S$ contains all places dividing $n$, $\prod_{v\in S}|n|_v = 1$ by product formula, so that $\#(\prod_{v\in S} F_v^\times / \prod_{v\in S} F_v^{\times n}) = n^{2\#S}$ by the following lemma. It follows that

$$\#(\mathbb{I}_F/\mathcal{N}) = \#(\prod_{v\in S} F_v^\times / \prod_{v\in S} F_v^{\times n})/\#(\mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^{\times n}) = n^{\#S}.$$

□

**Lemma 3.7.5.** *Let $K$ be a local field of characteristic zero containing all $n$-th roots of unity. Then $\#(K^\times/K^{\times n}) = n^2/|n|$. Here $|\cdot|$ is the normalized absolute value.*

*Proof.* For $K = \mathbb{C}$, the equation becomes $1 = 1$. For $K = \mathbb{R}$, we have $n \leq 2$, so that the equation becomes $1 = 1$ or $2 = 2$. Assume that $K$ is ultrametric. Consider the trivial action of $G = \mathbb{Z}/n\mathbb{Z}$ on $K^\times$. Then

$$\hat{H}^0(G, K^\times) = K^\times/K^{\times n}, \quad \hat{H}^{-1}(G, K^\times) = \{x \in K^\times \mid x^n = 1\}.$$

Thus

$$\#(K^\times/K^{\times n})/n = Q(K^\times) = Q(U_K)Q(\mathbb{Z}) = nQ(U_K).$$

Finally, exp and log induce isomorphisms between $\mathfrak{m}_K^a$ and $1 + \mathfrak{m}_K^a$ for some $a \geq 1$, so that

$$Q(U_K) = Q(1 + \mathfrak{m}^a) = Q(\mathfrak{m}^a) = Q(\mathcal{O}_K) = \#(\mathcal{O}_K/n\mathcal{O}_K) = 1/|n|.$$

Here we used $\hat{H}^0(G, \mathcal{O}_K) = \mathcal{O}_K/n\mathcal{O}_K$ and $\hat{H}^{-1}(G, \mathcal{O}_K) = 0$. □

**Corollary 3.7.6.** *Let $E/F$ be a finite extension of number fields and let $K/F$ be the maximal abelian sub-extension. Then $\mathcal{N}_E = \mathcal{N}_K$.*

*Proof.* By the existence theorem, $\mathcal{N}_E = \mathcal{N}_{K'}$, $K'/F$ finite abelian. Since $\mathcal{N}_{K'} = \mathcal{N}_E \subseteq \mathcal{N}_K$, $K'$ is an extension of $K$. Every place $v$ of $F$ that admits $w \mid v$ in $E$ with $D(w/v) = 1$ satisfies $F_v^\times \subseteq \mathcal{N}_E = \mathcal{N}_{K'}$. If, in addition, $v$ is unramified in $K'$, then $v$ splits in $K'$ because $\mathrm{Frob}_v \in \mathrm{Gal}(K'/F)$ is trivial. (By the compatibility with local reciprocity that we will prove in the next section, the additional condition that $v$ is unramified in $K'$ is in fact automatic.) It follows, by Chebotarev's density theorem, that $E$ is an extension of $K'$ (exercise). Therefore, by the assumption on $K$, we have $K \simeq K'$ and $\mathcal{N}_K = \mathcal{N}_{K'} = \mathcal{N}_E$. □

**Remark 3.7.7.** Let $E/F$ be a finite Galois extension of group $G$, and let $K/F$ be the maximal abelian sub-extension as in the corollary. Then $\mathrm{Gal}(K/F)$ can be identified with $G^{\mathrm{ab}}$. The corollary, combined with Artin reciprocity for the abelian extension $K/F$, implies the general case of Artin reciprocity for $E/F$.

## Transfer

Given a group $G$ and a subgroup $H$ of finite index, the transfer homomorphism $\mathrm{Ver}\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is defined as follows. Let $G = \coprod_{r\in R} Hr$. For $g \in G$ and $r \in R$, write $rg = h_r r'$ with $h_r \in H$ and $r' \in R$. Then $\mathrm{Ver}(g[G,G])$ is $\prod_r h_r[H,H]$.

**Theorem 3.7.8.** *Let $E/F$ be a finite Galois extension of number fields and let $K$ be an intermediate field. Then the diagram*

$$\begin{tikzcd}
\mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E) \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[d, "\mathrm{Ver}"] \\
\mathbb{I}_K/K^\times N_{E/K}(\mathbb{I}_E) \arrow[r, "\sim"] & \mathrm{Gal}(E/K)^{\mathrm{ab}}
\end{tikzcd}$$

*commutes.*

*Proof.* Let $G = \mathrm{Gal}(E/F)$ and $H = \mathrm{Gal}(E/K)$. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$ unramified in $F$ and let $\mathfrak{q}$ be a lifting of $\mathfrak{p}$ to $E$. It suffices to show that $\left(\frac{E/K}{\mathfrak{p}\mathcal{O}_K}\right) = \mathrm{Ver}(\bar{\phi})$, where $\phi = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in G$ and $\bar{\phi}$ is the class of $\phi$ in $G^{\mathrm{ab}}$. Note that $\mathfrak{p}\mathcal{O}_K = \prod_{g\in\Gamma}(K \cap g\mathfrak{q})$, where $G = \coprod_{g\in\Gamma} HgD$, $D = D(\mathfrak{q}/\mathfrak{p}) = \langle\phi\rangle$ is the decomposition group. For $\mathfrak{p}' = K \cap g\mathfrak{q}$, $\mathrm{Frob}_{g\mathfrak{q}/\mathfrak{p}'} = \mathrm{Frob}_{g\mathfrak{q}/\mathfrak{p}}^{f_g} = (g\phi g^{-1})^{f_g} = g\phi^{f_g}g^{-1}$, where $f_g = f(\mathfrak{p}'/\mathfrak{p})$ is the smallest integer $i \geq 1$ such that $g\phi^i g^{-1} \in H$. Thus

$$\left(\frac{E/K}{\mathfrak{p}\mathcal{O}_K}\right) = \prod_{g\in\Gamma} g\phi^{f_g}g^{-1}[H,H].$$

This is also $\mathrm{Ver}(\bar{\phi})$, because a set of representatives of $H\backslash G$ is given by $g\phi^i$, $g \in \Gamma$, $0 \leq i \leq f_g - 1$, and $(g\phi^i)\phi = g\phi^{i+1}$ for $0 \leq i < f_g - 1$ and $(g\phi^{f_g-1})\phi = (g\phi^{f_g}g^{-1})g$. □

This compatibility with transfer implies the following principal ideal theorem for the Hilbert class field.

**Theorem 3.7.9** (principal ideal). *Let $F$ be a number field. For every ideal $\mathfrak{a}$ of $\mathcal{O}_F$, $\mathfrak{a}\mathcal{O}_{H_F}$ is principal.*

For any Galois extension $E/F$, $H_E$ is the maximal unramified abelian extension of $E$ (this characterization uses the compatibility with local reciprocity, which will be proved in the next section), hence a Galois extension of $F$.

*Proof.* Let $G = \mathrm{Gal}(H_{H_F}/F)$. Since $H_{H_F}/F$ is an unramified extension, the maximal abelian sub-extension $H_{H_F}/F$ is $H_F$. Thus $\mathrm{Gal}(H_F/F) = G^{\mathrm{ab}}$ and $\mathrm{Gal}(H_{H_F}/H_F) = [G,G]$. By the compatibility with transfer, the diagram

$$\begin{tikzcd}
\mathcal{C}l_F \arrow[r, "\sim"] \arrow[d] & G^{\mathrm{ab}} \arrow[d, "\mathrm{Ver}"] \\
\mathcal{C}l_{H_F} \arrow[r, "\sim"] & {[G,G]}
\end{tikzcd}$$

commutes. Thus, by the following theorem, the map $\mathcal{C}l_F \to \mathcal{C}l_{H_F}$ is zero. □

**Theorem 3.7.10.** *Let $G$ be a finite group. Then* $\mathrm{Ver}\colon G^{\mathrm{ab}} \to [G,G]^{\mathrm{ab}}$ *is the zero map.*

We refer the reader to [N, Theorem VI.7.6] for a proof of a generalization of this group-theoretic result.

**Remark 3.7.11.** For a number field $F$ we can form the class field tower

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots,$$

where each $F_{i+1} = H_{F_i}$ is the Hilbert class field of $H_{F_i}$. Furtwängler asked whether the class field tower is finite. Golod and Shafarevich gave examples of number fields $F$ for which the class field tower is infinite. See [CF, Chapter IX].

# 3.8 Local class field theory

## Global reciprocity on local fields

**Theorem 3.8.1.** *Let $E/F$ be a finite abelian extension of number fields. The global Artin reciprocity $\rho_{E/F}\colon \mathbb{I}_F/F^\times N_{E/F}(\mathbb{I}_E) \xrightarrow{\sim} \mathrm{Gal}(E/F)$ induces, for every place $w$ of $E$ above a place $v$ of $F$, an isomorphism*

$$F_v^\times/N_{E_w/F_v}(E_w^\times) \xrightarrow{\sim} D(w/v).$$

We start with a local analogue of the first inequality.

**Lemma 3.8.2.** *For any finite abelian extension $L/K$ of local fields of characteristic $0$, we have*

$$[K^\times : N_{L/K}(L^\times)] \leq \#\mathrm{Gal}(L/K).$$

*Proof.* Let $D = \mathrm{Gal}(L/K)$. In the cyclic case, we have seen that $\#\hat{H}^0(D, L^\times) = \#D$ in the proof of the second inequality. The general case follows from the cyclic case by the following exact sequence for a sub-extension $L'/K$:

$$L'^\times/N_{L/L'}(L^\times) \xrightarrow{N_{L'/K}} K^\times/N_{L/K}(L^\times) \to K^\times/N_{L'/K}(L'^\times) \to 1.$$

□

**Proposition 3.8.3.** $\rho_{E/F}(F_v^\times) = D(w/v)$.

This will finish the proof of the theorem. Indeed, $\rho_{E/F}(N_{E_w/F_v}(E_w^\times)) = 1$, so by the proposition, $\rho_{E/F}$ induces a surjective homomorphism $F_v^\times/N_{E_w/F_v}(E_w^\times) \to D(w/v)$, and we conclude by the inequality above.

*Proof.* Let $G = \mathrm{Gal}(E/F)$, $D = D(w/v)$, $K = E^D$. We have a commutative square

$$\begin{tikzcd}
\mathbb{I}_F/\mathcal{N}_E \arrow[r, "\rho_{E/F}", "\sim"'] \arrow[d] & G \arrow[d] \\
\mathbb{I}_F/\mathcal{N}_K \arrow[r, "\rho_{K/F}", "\sim"'] & G/D.
\end{tikzcd}$$

Since $v$ splits in $K$, $\rho_{K/F}(F_v^\times) = 1$. Thus $\rho_{E/F}(F_v^\times) \subseteq D$.

For the inverse inclusion we reduce to the case of a Kummer extension as follows. Assume that $H = \rho_{E/F}(F_v^\times) \subsetneq D$. Let $L/K$ be a sub-extension of $E^H/K$ of prime degree $p$. Then $\rho_{L/F}(F_v^\times) = 1$. Let $L' = L(\zeta_p)$ and $K' = K(\zeta_p)$. By the commutative square

$$\begin{tikzcd}
\mathbb{I}_{K'}/K'^{\times}N_{L'/K'}(\mathbb{I}_{L'}) \arrow[r, "\rho_{L'/K'}", "\sim"'] \arrow[d, "N_{K'/F}"'] & \mathrm{Gal}(L'/K') \arrow[d, hook] \\
\mathbb{I}_F/F^{\times}N_{L/F}(\mathbb{I}_L) \arrow[r, "\rho_{L/F}", "\sim"'] & \mathrm{Gal}(L/F),
\end{tikzcd}$$

we have $\rho_{L'/K'}(K'^{\times}_{v'}) = 1$, where $v' \mid w_K$, $w_K = w|_K$. By assumption, $w$ is the unique place of $w$ above $w_K$. Thus $w_L = w|_L$ is the unique place of $L$ above $w_K$, so that $p \mid [L_{w_L} : K_{w_K}] \mid [L'_{w'} : K_{w_K}]$, where $w'$ is a place above $v'$ and $w_L$. Note that $[K' : K] \mid p - 1$ is prime to $p$. To find a contradiction, it suffices to show that $v'$ splits in $L'$.

We are thus reduced to showing that if $E/F$ is an abelian extension of exponent $n$, with $F$ containing all $n$-th roots of unity, such that $F_{v_0}^\times \subseteq \mathcal{N}_E$, then $v_0$ splits in $E$. Let $S \ni v_0$ be a finite set of places of $F$ containing all Archimedean places, all places ramified in $E$, and all places dividing $n$, such that $\mathbb{I}_F = F^\times \mathbb{I}_{F,S}$. We have $\mathcal{N}_E \supseteq F^\times F_{v_0}^\times \prod_{\substack{v\in S\\ v\neq v_0}} F_v^{\times n} \prod_{v\notin S} U_v = \mathcal{N}$. Thus $E$ is contained in the class field of $\mathcal{N}$ described in following theorem applied to $T = \{v_0\}$. Since $v_0$ splits in this class field, it splits in $E$. □

**Theorem 3.8.4.** *Let $F$ be a number field containing the $n$-th roots of unity and let $S = T \coprod T'$ be a finite set of places of $F$ containing all Archimedean places and all places dividing $n$ such that $\mathbb{I}_F = F^\times \mathbb{I}_{F,S}$. Let*

$$\mathcal{N} = \prod_{v\in T} F_v^\times \prod_{v\in T'} F_v^{\times n} \prod_{v\notin S} U_v, \quad \mathcal{N}' = \prod_{v\in T'} F_v^\times \prod_{v\in T} F_v^{\times n} \prod_{v\notin S} U_v.$$

*Then $F^\times \mathcal{N} = \mathcal{N}_E$, where $E = F(\sqrt[n]{\Delta})$, $\Delta = F^\times \cap \mathcal{N}'$.*

The case $T = \emptyset$ is Theorem 3.7.4. We have seen that $E/F$ is a finite extension. Note that $v \in T$ clearly splits in $E/F$.

*Proof.* As before, by Artin reciprocity $\mathcal{N}_E \supseteq F_v^{\times n}$ for all places $v$ of $F$. For $v \notin S$, $E/F$ is unramified so that $\mathcal{N}_E \supseteq U_v$. For $v \in T$, $\mathcal{N}_E \supseteq F_v^\times$. Thus $\mathcal{N}_E \supseteq F^\times \mathcal{N}$. It suffices to show that they have the same index in $\mathbb{I}_F$.

We have

$$[\mathbb{I}_F : \mathcal{N}_E] = [E : F] = [\Delta F^{\times n} : F^{\times n}] = [\Delta : \Delta \cap F^{\times n}] = [\Delta : \mathcal{O}_{F,S}^{\times n}].$$

To compute $[\mathbb{I}_F : F^\times \mathcal{N}]$, we use the short exact sequence

$$1 \to \mathcal{O}_{F,S}^\times/\Delta' \to \prod_{v\in T'} F_v^\times/F_v^{\times n} \xrightarrow{\psi} \mathbb{I}_F/F^\times \mathcal{N} \to 1,$$

where $\Delta' = F^\times \cap \mathcal{N}$. For the surjectivity of $\psi$ we used $\mathbb{I}_F = F^\times \mathbb{I}_{F,S}$. Thus

$$[\mathbb{I}_F : F^\times \mathcal{N}] = [\prod_{v\in T'} F_v^\times : \prod_{v\in T'} F_v^{\times n}][\mathcal{O}_{F,S}^\times : \mathcal{O}_{F,S}^{\times n}]^{-1}[\Delta' : \mathcal{O}_{F,S}^{\times n}].$$

Similarly, let $E' = F(\sqrt[n]{\Delta'})$. Then $\mathcal{N}_{E'} \supseteq \mathcal{N}'$, and we have

$$[\mathbb{I}_F : \mathcal{N}_{E'}] = [\Delta' : \mathcal{O}_{F,S}^{\times n}], \quad [\mathbb{I}_F : F^\times \mathcal{N}'] = [\prod_{v \in T} F_v^\times : \prod_{v \in T'} F_v^{\times n}][\mathcal{O}_{F,S}^\times : \mathcal{O}_{F,S}^{\times n}]^{-1}[\Delta : \mathcal{O}_{F,S}^{\times n}].$$

Thus

$$[\mathbb{I}_F : \mathcal{N}_E][\mathbb{I}_F : \mathcal{N}_{E'}] = [\Delta : \mathcal{O}_{F,S}^{\times n}][\Delta' : \mathcal{O}_{F,S}^{\times n}] = [\mathbb{I}_F : F^\times \mathcal{N}][\mathbb{I}_F : F^\times \mathcal{N}'].$$

Here we have used the fact

$$[\prod_{v \in S} F_v^\times : \prod_{v \in S} F_v^{\times n}] = n^{2\#S} = [\mathcal{O}_{F,S}^\times : \mathcal{O}_{F,S}^{\times n}]^2$$

proven in Theorem 3.7.4. It follows that $[\mathbb{I}_F : \mathcal{N}_E] = [\mathbb{I}_F : F^\times \mathcal{N}]$ and $\mathcal{N}_E = F^\times \mathcal{N}$. □

## Local reciprocity and existence theorem

**Proposition 3.8.5.** *Let $L/K$ be a finite (resp. finite Galois) extension of local fields. Let $F$ be a number field and $v$ a place of $F$ with an isomorphism $\iota\colon F_v \xrightarrow{\sim} K$. Then there exist a finite (resp. finite Galois) extension $E/F$, a place $w$ of $E$ above $v$, and an isomorphism $E_w \xrightarrow{\sim} L$ extension $\iota$. Furthermore, in the Galois case, there exists an intermediate field $F'$ of $E/F$ such that $F'_{v'} = F_v$ and* $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(E/F')$, *where $v' = w|_{F'}$.*

We have seen that any local field of characteristic zero is the completion of a number field. That a finite extension of $\mathbb{Q}_p$ is the completion of a number field is a special case of the above proposition.

Note that even if $L/K$ is abelian, $E/F$ is not necessarily abelian.

*Proof.* The Archimedean case is trivial. Assume we are in the non-Archimedean case.

In the case of a finite extension, we have $L = K[X]/(f)$. By Krasner's lemma, we may assume that $f \in F[X]$. We take $E = F[X]/(f)$ and take $w$ to be the place defined by the embedding $E \hookrightarrow L$.

In the case of a finite Galois extension, $L/K$ is the splitting field of a polynomial $g \in K[X]$. Again by Krasner's lemma, we may assume that $g \in F[X]$. We take $E$ to be the splitting field of $g$ in $F$ and choose a place $w \mid v$. Then we have $E_w \simeq L$ extending $F'_{v'} \simeq K$. We get a monomorphism $D = \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/F) = G$. Finally we take $F' = F^D$, so that $\mathrm{Gal}(E/F') = D$. □

Let $L/K$ be a finite *abelian* extension of local fields of characteristic zero. By the last assertion of the proposition, there exist a finite *abelian* extension of number fields $E/F$, places $w \mid v$, and an isomorphism $E_w \simeq L$ inducing $F_v \simeq K$. We define the local reciprocity isomorphism

$$r_{L/K}\colon \mathrm{Gal}(L/K) \xrightarrow{\sim} K^\times / N_{L/K}(L^\times)$$

to be the isomorphism induced from the global reciprocity isomorphism $r_{E/F}$. We check that this definition does not depend on choices. For this, consider another set of data $E'/F'$, $w' \mid v'$, $E'_{w'} \simeq L$. Let $E''$ be the composite of $E$ and $E'$ in $L$. The embedding $E'' \to L$ induces a place $w''$ of $E''$ and an isomorphism $E''_{w''} \xrightarrow{\sim} L$ inducing $F''_{v''} \xrightarrow{\sim} K$, where $F''$ is the composite of $F$ and $F'$ in $K$ and $v'' = w''|_{E''}$. The extension $E''/F''$ is a composite of $EF''/F''$ and $E'F''/F''$, hence abelian. By the functoriality of global reciprocity, the square

$$\begin{tikzcd}
\mathrm{Gal}(E''/F'') \arrow[r, "r_{E''/F''}", "\sim"'] \arrow[d] & \mathbb{I}_{F''}/F''^{\times} N_{E''/F''}(\mathbb{I}_{E''}) \arrow[d, "N_{F''/F}"] \\
\mathrm{Gal}(E/F) \arrow[r, "r_{E/F}", "\sim"'] & \mathbb{I}_F/F^{\times} N_{E/F}(\mathbb{I}_E)
\end{tikzcd}$$

commutes. This implies that $r_{L/K}$ does not depend on choices.

We check the required properties of $r_{L/K}$. For $L/K$ unramified with $K$ non-Archimedean, the normalization $r_{L/K}(\mathrm{Frob}_{L/K}) = \pi_L N_{L/K}(L^\times)$ follows from the construction of $r_{L/K}$ via the Artin map. For *abelian* extensions $L/K$ and $L'/K'$ of local fields and an embedding $\tau\colon L \hookrightarrow L'$ such that $\tau(K) \subseteq K'$, the functoriality of $r_{L/K}$ follows from the functoriality of global reciprocity. Indeed, we construct successively number field extensions $E/F$ (abelian), $F'/F$, and $E'/F'$ (abelian, modifying $F'/F$ if necessary), giving rise to the local field extensions by completion, then $\tau(E) \subseteq E'$.

Next we prove the local existence theorem (Theorem 3.1.13), namely that every (open) subgroup $\mathcal{N} \subseteq K^\times$ of finite index equals $\mathcal{N}_L := N_{L/K}(L^\times)$ for some finite extension $L/K$. As in the global case, we reduce to the Kummer case where $\mathcal{N}$ has exponent $n$ and $K$ contains all $n$-th roots of unity. In this case, $\mathcal{N} \supseteq K^{\times n}$. We conclude by the fact that $\mathcal{N}_{K(\sqrt[n]{K^\times})} = K^{\times n}$ (Proposition 3.2.8), which is a consequence of local reciprocity and Kummer theory.

**Corollary 3.8.6.** *Let $L/K$ be a finite Galois extension of local fields of characteristic $0$ and let $K'/K$ be the maximal abelian sub-extension. Then $\mathcal{N}_L = \mathcal{N}_{K'}$.*

*Proof.* We claim that for any abelian extension $L'/K$ with $\mathcal{N}_{L/K} \subseteq \mathcal{N}_{L'/K}$, $L$ is an extension of $L'$. Assume this claim. By the existence theorem, there exists an abelian extension $L''/K$ such that $\mathcal{N}_{L''/K} = \mathcal{N}_{L/K}$. By the claim, $L$ is an extension of $L''$. But $\mathcal{N}_{L''/K} = \mathcal{N}_{L/K} \subseteq \mathcal{N}_{K'/K}$, so that $L''$ is an extension of $K'$. By the assumption on $K'$, we have $K' \simeq L''$, so that $\mathcal{N}_L = \mathcal{N}_{L''} = \mathcal{N}_{K'}$.

We prove the claim by induction on $[L : K]$. We have

$$\mathcal{N}_{L/K} \subseteq \mathcal{N}_{L'/K} \cap \mathcal{N}_{K'/K} = \mathcal{N}_{L'K'/K}.$$

Here the equality is a consequence of the existence theorem (Corollary 3.1.14). Thus

$$\mathcal{N}_{L/K'} \subseteq N_{K'/K}^{-1}(\mathcal{N}_{L/K}) \subseteq N_{K'/K}^{-1}(\mathcal{N}_{L'K'/K}) = \mathcal{N}_{L'K'/K'}.$$

Here in the equality we used the lemma below (applied to $L'K'/K$). Since $L/K$ is solvable (see the remark below), $[L : K'] < [L : K]$, and we conclude by induction hypothesis. □

**Lemma 3.8.7.** *Let $L'/K$ be a finite abelian extension of local fields of characteristic $0$ and let $K'/K$ be a sub-extension. Then $N_{K'/K}^{-1}(\mathcal{N}_{L'/K}) = \mathcal{N}_{L'/K'}$.*

*Proof.* Consider the exact sequence

$$K'^{\times}/\mathcal{N}_{L'/K'} \xrightarrow{N_{K'/K}} K^{\times}/\mathcal{N}_{L'/K} \to K^{\times}/\mathcal{N}_{K'/K} \to 1$$

that we used in the proof of the local analogue of the first inequality. Since

$$[L' : K] = [L' : K'][K' : K],$$

we have $\#(K^{\times}/\mathcal{N}_{L'/K}) = \#(K'^{\times}/\mathcal{N}_{L'/K'})\#(K^{\times}/\mathcal{N}_{K'/K})$ by reciprocity. Thus the first arrow in the exact sequence is an injection. In other words, $N_{K'/K}^{-1}(\mathcal{N}_{L'/K}) = \mathcal{N}_{L'/K'}$. □

**Remark 3.8.8** (Higher ramification groups)**.** Let $L/K$ be a finite extension of Archimedean local fields of group $G$. For $i \geq -1$, the $i$-th ramification group $G_i < G$ is the subgroup consisting of $g \in G$ acting trivially on $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$ (or equivalently, $v_L(gx - x) \geq i + 1$ for all $x \in \mathcal{O}_L$). This gives a descending filtration

$$G = G_{-1} > G_0 > G_1 > \dots .$$

of normal subgroups of $G$. Note that $G_0$ is the inertia group so that $G_{-1}/G_0 \simeq \mathrm{Gal}(k_L/k_K)$. For $i \geq 0$, $g \in G_0$ belongs to $g \in G_i$ if and only if $g\pi_L/\pi_L \in U_L^{(i)}$, because $\mathcal{O}_L = \mathcal{O}_{L^{G_0}}[\pi_L]$. Thus $g \mapsto g\pi_L/\pi_L$ gives an injection $G_i/G_{i+1} \hookrightarrow U_L^{(i)}/U_L^{(i+1)}$. It follows that $G$ is solvable. Note that $U_L^{(i)}/U_L^{(i+1)}$ is $k_L^{\times}$ for $i = 0$ and $k_L$ for $i \geq 1$. The group $G_1$ is a $p$-group and is called the wild inertia group.

Let $L/K$ be a finite Galois extension of local fields of characteristic 0 and let $K'/K$ be the maximal abelian sub-extension as in the corollary. We define

$$r_{L/K} \colon \mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} K^{\times}/N_{L/K}(L^{\times})$$

to be the isomorphism induced by $r_{K'/K}$. Functoriality of $r_{L/K}$ follows from the abelian case. This finishes the proof of local reciprocity (Theorem 3.1.5).

**Theorem 3.8.9** (Compatibility between local and global reciprocity)**.** *Let $E/F$ be a finite Galois extension of number fields and let $w$ be a place of $E$ above a place $v$ of $F$. Then the diagram*

$$\begin{tikzcd}
\mathrm{Gal}(E_w/F_v)^{\mathrm{ab}} \arrow[r, "r_{E_w/F_v}", "\sim"'] \arrow[d] & F_v^{\times}/N_{E_w/F_v}(E_w^{\times}) \arrow[d] \\
\mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[r, "r_{E/F}", "\sim"'] & \mathbb{I}_F/F^{\times}N_{E/F}(\mathbb{I}_E)
\end{tikzcd}$$

*commutes.*

*Proof.* Let $F' = E^D$, where $D = D(w/v)$, and let $v' = w|_{F'}$. Then $F_v \simeq F'_{v'}$ and the above diagram can be identified with the outer square of the diagram

$$\begin{tikzcd}
\mathrm{Gal}(E_w/F'_{v'})^{\mathrm{ab}} \arrow[r, "r_{E_w/F'_{v'}}", "\sim"'] \arrow[d, "\simeq"'] & F'^{\times}_{v'}/N_{E_w/F'_{v'}}(E_w^{\times}) \arrow[d, "\simeq"] \\
\mathrm{Gal}(E/F')^{\mathrm{ab}} \arrow[r, "r_{E/F'}", "\sim"'] \arrow[d] & \mathbb{I}_{F'}/F'^{\times}N_{E/F'}(\mathbb{I}_E) \arrow[d, "N_{F'/F}"] \\
\mathrm{Gal}(E/F)^{\mathrm{ab}} \arrow[r, "r_{E/F}", "\sim"'] & \mathbb{I}_F/F^{\times}N_{E/F}(\mathbb{I}_E)
\end{tikzcd}$$

The upper square commutes by construction: both $r_{E_w/F'_{v'}}$ and $r_{E/F'}$ can be identified with the reciprocity isomorphisms for the maximal abelian sub-extension $E'/F'$ of $E/F'$. The lower square commutes by the functoriality of global reciprocity. □

## Local construction of local reciprocity

Our construction of the local reciprocity uses global reciprocity. There are more direct constructions of local reciprocity.

We have indicated that reciprocity can be interpreted as a cup product of group cohomology. It is more convenient to state this with Tate cohomology. For any finite Galois extension $L/K$ of local fields of group $G$ and degree $d$, there is a canonical isomorphism $\mathrm{Br}_{L/K} := H^2(G, L^\times) \simeq \frac{1}{d}\mathbb{Z}/\mathbb{Z}$ and the inverse image $c_{L/K} \in H^2(G, L^\times)$ of the class of $\frac{1}{d}$ is called the *fundamental class*.

**Theorem 3.8.10.** *The homomorphism*

$$\hat{H}^{q-2}(G, \mathbb{Z}) \to \hat{H}^q(G, L^\times)$$

*defined by cup product with $c_{L/K}$ is an isomorphism for every $q \in \mathbb{Z}$.*

The case $q = 0$ gives the reciprocity isomorphism:

$$r_{L/K} \colon G^{\mathrm{ab}} = \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow[\sim]{-\cup c_{L/K}} \hat{H}^0(G, L^\times) = K^\times/N_{L/K}(L^\times).$$

For details on this approach (both local and global), we refer to [CF].

In the case where $L/K$ is a *totally ramified* finite Galois extension of non-Archimedean local fields, the reciprocity map can be made more explicit. In this case, the fundamental class is given by the short exact sequences of $G$-modules

$$1 \to U_L \to U_{\widehat{L^{\mathrm{ur}}}} \xrightarrow{\phi} U_{\widehat{L^{\mathrm{ur}}}} \to 1, \quad 1 \to U_{\widehat{L^{\mathrm{ur}}}} \to \widehat{L^{\mathrm{ur}}}^\times \xrightarrow{v_L} \mathbb{Z} \to 0,$$

where $L^{\mathrm{ur}}$ is the maximal unramified extension of $L$, and $\phi(x) = \mathrm{Frob}(x)/x$. The image of $g[G, G]$ in $\hat{H}^{-1}(G, U_{\widehat{L^{\mathrm{ur}}}})$ (or $\hat{H}^{-1}(G, U_L)$) is given by the class of $g\pi_L/\pi_L$. Thus

$$r_{L/K}(g[G, G]) = N_{\widehat{L^{\mathrm{ur}}}/\widehat{K^{\mathrm{ur}}}}(x),$$

where $x \in U_{\widehat{L^{\mathrm{ur}}}}$ is a solution to the equation $\mathrm{Frob}(x)/x = g\pi_L/\pi_L$.

Note that the short exact sequence

$$1 \to \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(\overline{k_K}/k_K) \to 1,$$

where $K^{\mathrm{ab}}$ is the maximal abelian extension of $K$ and $\mathrm{Gal}(\overline{k_K}/k_K) \simeq \hat{\mathbb{Z}}$, splits. It follows that for any finite abelian extension $L/K$ is contained in a finite abelian extension of the form $K_1K_2/K$, where $K_1/K$ is unramified and $K_2/K$ is totally ramified. For an explicit construction of the splitting, see below.

## Lubin-Tate extensions

For non-Archimedean local fields, Lubin-Tate theory solves the problem of explicit construction of abelian extensions. Let $K$ be such a field. Let $\pi$ be a uniformizer and let $q = \# k_K$.

**Definition 3.8.11.** A *Lubin-Tate polynomial* is $f(X) = X^q + a_{q-1}X^{q-1} + \cdots + a_2X^2 + \pi X \in \mathcal{O}_K[X]$ such that $v_K(a_i) \geq 1$. The $n$-th Lubin-Tate extension $L_n$ is the splitting field of the $n$-th iteration $f^{(n)}(X) = (f \circ f \circ \cdots \circ f)(X)$ of $f(X)$.

It turns out that these extensions depend on $\pi$ but not on the choice of $f$.

**Theorem 3.8.12** (Lubin-Tate)**.** *The extension $L_n/K$ is abelian and we have*

$$\mathcal{N}_{L_n/K} = U_K^{(n)} \pi^{\mathbb{Z}}.$$

Thus $L_n/K$ is a totally ramified extension of group $U_K/U_K^{(n)}$.

**Example 3.8.13.** For $K = \mathbb{Q}_p$ and $f(X) = (X+1)^p - 1$, we have $f^{(n)}(X) = (X+1)^{p^n} - 1$, so $L_n = \mathbb{Q}_p(\zeta_{p^n}) = \mathbb{Q}_p(\mathbb{Q}_p^\times[p^n])$.

In general, $L_n = K(F_f[\pi^n])$, where $F_f$ is the Lubin-Tate module associated to $f$, which is a one-dimensional formal group law equipped with an $\mathcal{O}_K$-action. The isomorphism class of $F_f$ depends only on $\pi$.

Let $L_\infty = \bigcup_n L_n$. Then $K^{\mathrm{ab}} = L_\infty K^{\mathrm{ur}}$. We get a splitting $\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \mathrm{Gal}(L_\infty/K) \times \mathrm{Gal}(K^{\mathrm{ur}}/K)$ corresponding to the splitting $\widehat{K^\times} \simeq U_K \times \pi^{\hat{\mathbb{Z}}}$ via reciprocity.

# Bibliography

[AT] E. Artin and J. Tate, *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original. MR2467155 (2009k:11001) ↑68, 79

[B1] N. Bourbaki, *Éléments de mathématique. Topologie générale*, Springer, Berlin, 2007 (French). MR0358652 (50 #11111) ↑2, 3, 5, 19

[B2] ______, *Éléments de mathématique. Intégration*, Springer, Berlin, 2007 (French). ↑16, 18

[B3] ______, *Éléments de mathématique. Algèbre commutative*, Springer, Berlin, 2007 (French). ↑9, 10, 11, 12

[B4] ______, *Éléments de mathématique. Théories spectrales*, Springer, Berlin, 2007 (French). ↑36, 37

[CF] J. W. S. Cassels and A. Fröhlich (eds.), *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, Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967. MR0215665 (35 #6500) ↑87, 92, 95

[H] P. J. Higgins, *Introduction to topological groups*, Cambridge University Press, London-New York, 1974. London Mathematical Society Lecture Note Series, No. 15. MR0360908 (50 #13355) ↑2, 5, 14, 16, 18

[I] S. Iyanaga (ed.), *The theory of numbers*, North-Holland, Amsterdam, 1975. Translated from the 1969 Japanese edition by K. Iyanaga. ↑10

[N] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859 ↑9, 10, 11, 21, 82, 86

[RV] D. Ramakrishnan and R. J. Valenza, *Fourier analysis on number fields*, Graduate Texts in Mathematics, vol. 186, Springer-Verlag, New York, 1999. MR1680912 ↑44, 68

[R] W. Rudin, *Real and complex analysis*, 3rd ed., McGraw-Hill Book Co., New York, 1987. MR924157 (88k:00002) ↑15

[S] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott; Graduate Texts in Mathematics, Vol. 42. MR0450380 (56 #8675) ↑73

[T1] J. T. Tate Jr, *Fourier analysis in number fields and Hecke's zeta-functions*, 1950. Thesis (Ph.D.)–Princeton University, reproduced in [CF]. MR2612222 ↑38

[T2] Y. Tian, *Lectures on algebraic number theory.* Notes. ↑11, 12, 26

[W] A. Weil, *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition. MR1344916 (96c:11002) ↑12, 31