A BRIEF SUMMARY OF THE STATEMENTS OF CLASS FIELD THEORY

BJORN POONEN

0. PROFINITE COMPLETIONS OF TOPOLOGICAL GROUPS

Let $G$ be a topological group. The profinite completion of $G$ is

$$\hat{G} := \lim_{\leftarrow} \frac{G}{U},$$

where $U$ ranges over the finite-index open normal subgroups of $G$. There is a natural continuous homomorphism $G \to \hat{G}$ through which every other continuous homomorphism from $G$ to a profinite group factors uniquely. If $G$ is profinite already, then $G \to \hat{G}$ is an isomorphism.

In general, $G \to \hat{G}$ need not be injective or surjective. Nevertheless, we think of $G$ as being almost isomorphic to $\hat{G}$: The finite-index open subgroups of $G$ are in bijection with those of $\hat{G}$. And finite-index open subgroups of certain Galois groups are what we are interested in.

1. LOCAL CLASS FIELD THEORY

1.1. Notation associated to a discrete valuation ring.

$\mathcal{O}$: a complete discrete valuation ring
$K := \text{Frac}(\mathcal{O})$
$v$: the valuation $K^\times \to \mathbb{Z}$
$p$: the maximal ideal of $\mathcal{O}$
$k$: the residue field $\mathcal{O}/p$
$K^s$: a fixed separable closure of $K$
$K^{ab}$: the maximal abelian extension of $K$ in $K^s$
$K^{unr}$: the maximal unramified extension of $K$ in $K^s$

$k^s$: the residue field of $K^{unr}$, so $k^s$ is a separable closure of $k$.

Equip $K$ and its subsets with the topology coming from the absolute value $|x| := \exp(-v(x))$. 

Date: December 7, 2022.
I thank David Zywina for comments. The writing of this article was supported in part by National Science Foundation grants DMS-0301280 and DMS-2101040 and Simons Foundation grants #402472 and #550033.
1.2. Local fields.

**Definition 1.1.** A nonarchimedean local field is a complete discrete-valued field $K$ as in Section 1.1 such that the residue field $k$ is finite. An archimedean local field is $\mathbb{R}$ or $\mathbb{C}$.

Facts:
- A nonarchimedean local field of characteristic 0 is isomorphic to a finite extension of $\mathbb{Q}_p$.
- A (nonarchimedean) local field of characteristic $p > 0$ is isomorphic to $\mathbb{F}_q((t))$ for some power $q$ of $p$.

1.3. The local Artin homomorphism. Let $K$ be a local field. Local class field theory says that there is a homomorphism $\theta : K^\times \to \text{Gal}(K_{ab}/K)$ that is almost an isomorphism. The homomorphism $\theta$ is called the local Artin homomorphism. It cannot be literally an isomorphism, because $\text{Gal}(K_{ab}/K)$ is a profinite group, hence compact, while $K^\times$ is not. What is true is that $\theta$ induces an isomorphism of topological groups $\hat{K}^\times \to \text{Gal}(K_{ab}/K)$.

If $K$ is archimedean, then $\theta : K^\times \to \text{Gal}(K_{ab}/K)$ is surjective and its kernel is the connected component of the identity in $K^\times$.

For the rest of Section 1.3 we assume that $K$ is nonarchimedean. Then $\theta$ is injective: The choice of a uniformizer $\pi \in \mathcal{O}$ lets us write $K^\times = \mathcal{O}^\times \pi \mathbb{Z} \simeq \mathcal{O}^\times \times \mathbb{Z}$, and $\mathcal{O}^\times$ is already profinite, so $\hat{K}^\times \simeq \mathcal{O}^\times \times \hat{\mathbb{Z}}$. Thus local class field theory says that there is an isomorphism $\mathcal{O}^\times \times \hat{\mathbb{Z}} \to \text{Gal}(K_{ab}/K)$.

More canonically, without choosing $\pi$, the two horizontal exact sequences below are almost isomorphic:

\[
\begin{array}{ccccccccc}
0 & \to & \mathcal{O}^\times & \to & K^\times & \to & \mathbb{Z} & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \text{Gal}(K_{ab}/K_{unr}) & \to & \text{Gal}(K_{ab}/K) & \to & \text{Gal}(K_{unr}/K) & \to & 0
\end{array}
\]

With the identification of the group at lower right $\text{Gal}(K_{unr}/K) \simeq \text{Gal}(k^s/k) \simeq \hat{\mathbb{Z}}$, mapping the Frobenius automorphism to $1 \in \hat{\mathbb{Z}}$, the right vertical map in (1) becomes the natural inclusion $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$. In other words, $\theta$ maps $K^\times$ isomorphically to the set of $\sigma \in \text{Gal}(K_{ab}/K)$ inducing an integer power of Frobenius on the residue field (as opposed to a $\hat{\mathbb{Z}}$-power). The bottom row of (1) is simply the profinite completion of the top row.

Also from (1), one sees that $\theta(\mathcal{O}^\times)$ is the inertia subgroup $\text{Gal}(K_{ab}/K_{unr})$ of $\text{Gal}(K_{ab}/K)$, and that $\theta$ maps any uniformizer to a Frobenius automorphism in $\text{Gal}(K_{ab}/K)$. Moreover, the descending chain $\mathcal{O}^\times \supset 1 + p \supset 1 + p^2 \supset \cdots$ is mapped isomorphically by $\theta$ to the descending chain of ramification subgroups of $\text{Gal}(K_{ab}/K)$ in the upper numbering.
1.4. **Functoriality.** Let $L$ be a finite extension of $K$. Let $N_{L/K}: L^\times \to K^\times$ be the norm map. Let $\theta_L, \theta_K$ be the local Artin homomorphisms associated to $L, K$, respectively. Let $\text{res}: \text{Gal}(L^{ab}/L) \to \text{Gal}(K^{ab}/K)$ be the homomorphism mapping an automorphism $\sigma$ of $L^{ab}$ to its restriction $\sigma|_{K^{ab}}$. Then the square

\[
\begin{array}{ccc}
L^\times & \xrightarrow{\theta_L} & \text{Gal}(L^{ab}/L) \\
\downarrow{N_{L/K}} & & \downarrow{\text{res}} \\
K^\times & \xrightarrow{\theta_K} & \text{Gal}(K^{ab}/K)
\end{array}
\]

commutes.

1.5. **Finite abelian extensions.** Because $\theta$ is almost an isomorphism, and because of Galois theory, the following sets are in bijection:

- The finite-index open subgroups of $K^\times$.
- The (finite-index) open subgroups of $\text{Gal}(K^{ab}/K)$.
- The finite abelian extensions of $K$ contained in $K^s$.

Going backwards, if $L$ is a finite abelian extension of $K$ in $K^s$, the corresponding subgroup of $K^\times$ is $N_{L/K}L^\times$. (This could be viewed as a consequence of the functoriality above.)

The composition

\[
K^\times \to \text{Gal}(K^{ab}/K) \xrightarrow{\text{res}} \text{Gal}(L/K)
\]

is surjective with kernel $N_{L/K}L^\times$, and $\mathcal{O}^\times$ maps to the inertia subgroup $I_{L/K} \leq \text{Gal}(L/K)$, and any uniformizer $\pi$ maps to a Frobenius element of $\text{Gal}(L/K)$.

### 2. Global class field theory (via ideles)

#### 2.1. Global fields.

**Definition 2.1.** A **number field** is a finite extension of $\mathbb{Q}$. A **global function field** is a finite extension of $\mathbb{F}_p(t)$ for some prime $p$, or equivalently is the function field of a geometrically integral curve over a finite field $\mathbb{F}_q$ (called the **constant field**), where $q$ is a power of some prime $p$. A **global field** is a number field or a global function field.

Throughout Sections 2 and 3, $K$ is a global field. If $v$ is a nontrivial place of $K$ (given by an absolute value on $K$), then the completion $K_v$ is a local field. If $v$ is nonarchimedean, let $\mathcal{O}_v$ be the valuation subring of $K_v$; if $v$ is archimedean, let $\mathcal{O}_v = K_v$.

#### 2.2. The adele ring.** The **adele ring** of $K$ is the restricted direct product

\[
A = A_K := \prod'_v (K_v, \mathcal{O}_v) := \left\{ (a_v) \in \prod_v K_v : a_v \in \mathcal{O}_v \text{ for all but finitely many } v \right\}.
\]

It is a topological ring: the topology is uniquely characterized by the condition that $\prod_v \mathcal{O}_v$ is open in $A$ and has the product topology. The diagonal map $K \to A$ is like $\mathbb{Z} \to \mathbb{R}$: it embeds $K$ as a discrete co-compact subgroup of $A$. 

---

3
2.3. **The idele group and idele class group.** The idele group of $K$ is

$$\mathbb{A}^\times = \prod_v (K_v^\times, \mathcal{O}_v^\times) := \left\{(a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$ 

It is a topological group: the topology is uniquely characterized by the condition that $\prod_v \mathcal{O}_v^\times$ is open in $\mathbb{A}^\times$ and has the product topology\(^1\). The diagonal map $K^\times \to \mathbb{A}^\times$ is like $\mathbb{Z}^\times \to \mathbb{R}^\times$: it embeds $K^\times$ as a discrete subgroup of $\mathbb{A}^\times$, but the quotient $C = C_K := \mathbb{A}^\times/K^\times$ is not compact. The topological group $C$ is called the **idele class group**.

2.4. **The global Artin homomorphism.** Let $K^s$ be a fixed separable closure of $K$. Let $K^{ab}$ be the maximal abelian extension of $K$ contained in $K^s$. The group $C$ plays the role in global class field theory played by $K^\times$ in local class field theory. Namely, if $K$ is a global field, there is a global Artin homomorphism

$$\theta: C \to \text{Gal}(K^{ab}/K)$$

that induces an isomorphism $\hat{C} \cong \text{Gal}(K^{ab}/K)$.

If $K$ is a number field, then $\theta$ is surjective and its kernel is the connected component of the identity in $C$.

If $K$ is a global function field with constant field $k$, then $\theta$ is injective and $\theta(C)$ equals the set of $\sigma \in \text{Gal}(K^{ab}/K)$ whose restriction in $\text{Gal}(k^s/k)$ is an integer power of the Frobenius generator.

2.5. **Functoriality.** Let $L$ be a finite extension of $K$ of degree $n$. Then $A_L \simeq A_K \otimes K \to L$ is free of rank $n$ over $A_K$, so there is a norm map $N_{L/K}: A_L \to A_K$. We write $N_{L/K}$ also for the induced homomorphism $N_{L/K}: C_L \to C_K$. Then

$$\begin{array}{ccc}
C_L & \xrightarrow{\theta_L} & \text{Gal}(L^{ab}/L) \\
N_{L/K} \downarrow & & \downarrow \text{res} \\
C_K & \xrightarrow{\theta_K} & \text{Gal}(K^{ab}/K)
\end{array}$$

commutes.

2.6. **Finite abelian extensions.** The following sets are in bijection:

- The finite-index open subgroups of $C$.
- The finite-index open subgroups of $\text{Gal}(K^{ab}/K)$.
- The finite abelian extensions of $K$ contained in $K^s$.

Going backwards, if $L$ is a finite abelian extension of $K$ in $K^s$, the corresponding subgroup of $C$ is $N_{L/K}C_L$. The composition

$$C \to \text{Gal}(K^{ab}/K) \xrightarrow{\text{res}} \text{Gal}(L/K)$$

is surjective with kernel $N_{L/K}C_L$.

---

\(^1\)Alternatively, one can use the general recipe for getting the topology on the units of a topological ring $R$: not the subspace topology on $R^\times$ as a subset of $R$ (this may fail to make the inverse map $R^\times \to R^\times$ continuous), but the subspace topology on the set of solutions to $xy = 1$ in $R \times R$ (this is what one gets if one expresses the multiplicative group scheme $\mathbb{G}_m$ as an affine variety).
2.7. Connection between the global and local Artin homomorphisms. Let \( v \) be a place of \( K \). Identify \( K_v^\times \) with a subgroup of \( \mathbb{A}^\times \) by mapping \( \alpha \in K_v^\times \) to the idele with \( \alpha \) in the \( v \)-th position and 1 in every other position. The composition \( K_v^\times \to \mathbb{A}^\times \to C \) is injective. Let \( \theta_v \) be the local Artin homomorphism for \( K_v \). Then the diagram

\[
\begin{array}{ccc}
K_v^\times & \xrightarrow{\theta_v} & \text{Gal}(K_v^{ab}/K_v) \\
\downarrow & & \downarrow \text{res} \\
C & \xrightarrow{\theta} & \text{Gal}(K^{ab}/K)
\end{array}
\]

commutes. Thus \( \theta \) determines \( \theta_v \).

Conversely, if one knows \( \theta_v \) for all \( v \), one can construct \( \theta \) as follows. Let \( L \) be a finite abelian extension of \( K \) contained in \( K_s \). Define \( \mathbb{A}^\times \to \text{Gal}(L/K) \) \((a_v) \mapsto \prod_v \theta_v(a_v)\); if \( v \) is unramified in \( L/K \), and \( a_v \in \mathcal{O}_v^\times \), then \( \theta_v(a_v) = 1 \), so all but finitely many terms in the infinite product are 1, and the product makes sense. Take the inverse limit over all possible \( L \) to get

\[
\mathbb{A}^\times \to \text{Gal}(K^{ab}/K).
\]

The idelic version of the Artin reciprocity law says that \( K^\times \) is in the kernel, so we get a homomorphism

\[
C \to \text{Gal}(K^{ab}/K),
\]

which is \( \theta \).

2.8. Moduli.

Definition 2.2. A modulus is a formal product \( m = \prod_v v^{e_v} \) where \( e_v \in \mathbb{Z}_{\geq 0} \), all but finitely many \( e_v \) equal 0, and \( e_v \in \{0, 1\} \) for real \( v \), and \( e_v = 0 \) for complex \( v \). The support \( \text{supp} m \) is the (finite) set of nonarchimedean places \( v \) such that \( e_v \neq 0 \).

If \( K \) is a number field, then a modulus can be viewed as a pair consisting of

1. an integral ideal of the ring of integers \( \mathcal{O}_K \), and
2. a subset of the real places.

If \( K \) is the function field of a smooth projective curve \( X \) over a finite field, then a modulus is the same thing as an effective divisor on \( X \).

2.9. Ray class groups and ray class fields. In this section we assume that \( K \) is a number field. Fix a modulus \( m = \prod_v v^{e_v} \). We will define a finite-index open subgroup \( U_{m,v} \subseteq \mathcal{O}_v^\times \) for each \( v \). If \( e_v = 0 \), define \( U_{m,v} := \mathcal{O}_v^\times \). If \( e_v > 0 \) and \( v \) is nonarchimedean, define \( U_{m,v} := 1 + p_v^{e_v} \), where \( p_v \) is the maximal ideal of \( \mathcal{O}_v \). If \( e_v > 0 \) and \( v \) is real, define \( U_{m,v} \) as \( \mathbb{R}_{>0} \subseteq \mathbb{R}^\times \simeq K_v^\times \). Define \( U_m := \prod_v U_{m,v} \subseteq \mathbb{A}^\times \). The image of \( U_m \) under \( \mathbb{A}^\times \to C \) is a finite-index open subgroup \( U'_m \) of \( C \) (this is equivalent to finiteness of the class number of \( K \), as we will see in Section 3.4). The corresponding finite abelian extension \( R_m \) of \( K \) is called
the ray class field of modulus \( m \), and \( R_m \) over \( K \) is unramified at all \( v \) with \( e_v = 0 \). The ray class group of modulus \( m \) is

\[
\frac{C}{U_m^\prime} = \frac{\mathbb{A}^\times}{U_{mK}^\times},
\]

which is isomorphic to \( \text{Gal}(R_m/K) \) via the global Artin homomorphism.

Every finite-index open subgroup of \( \mathbb{A}^\times \) contains \( U_m \) for some \( m \), so every finite abelian extension of \( K \) is contained in \( R_m \) for some \( m \).

3. Global class field theory (via ideals)

In this section we assume that \( K \) is a number field.

3.1. Classical ray class groups. Let \( I \) be the group of fractional ideals of \( K \), or equivalently, the free abelian group on the nonarchimedean places of \( K \). Let \( P \) be the subgroup of principal ideals. The class group is \( \text{Cl} \mathcal{O}_K := I/P \).

We now generalize to an arbitrary modulus \( m = \prod_v v^{e_v} \). Let \( I_m \) be the subgroup of fractional ideals that do not involve the primes dividing \( m \); i.e., \( I_m \) is the free abelian group on the nonarchimedean places \( v \) satisfying \( e_v = 0 \). For \( a \in K^\times \), the notation \( a \equiv 1 \pmod{\times m} \) means that \( a \in U_{m,v} \) for every \( v \) satisfying \( e_v > 0 \). The group \( P_m \subseteq I_m \) is the group of principal ideals generated by some \( a \in K^\times \) with \( a \equiv 1 \pmod{\times m} \). The classical ray class group of modulus \( m \) is \( \text{Cl}_m \mathcal{O}_K := I_m/P_m \). Section 3.4 will prove that this is isomorphic to the ray class group \( C/U_m^\prime \) defined in Section 2.9.

3.2. The classical Artin homomorphism. Let \( L/K \) be a finite abelian extension of number fields. Let \( S \) be a finite set of finite primes of \( K \) such that \( S \) contains every prime that ramifies in \( L \). Let \( I_S \) be the group of fractional ideals that do not involve the primes in \( S \). The classical Artin homomorphism is the map

\[
\Theta: I_S \to \text{Gal}(L/K)
\]

sending each prime ideal \( p \notin S \) to the Frobenius element \( \text{Frob}_p \in \text{Gal}(L/K) \).

3.3. The main theorems. The Artin reciprocity law states that there exists a modulus \( m \) (depending on \( L/K \)) with \( \text{supp} \ m = S \) such that the subgroup \( P_m \subseteq I_m = I_S \) is contained in \( \ker \Theta \). The existence theorem states that given a modulus \( m \) and group \( H \) with \( P_m \subseteq H \subseteq I_m \) there exists an abelian extension \( L \) of \( K \) unramified outside \( \text{supp} \ m \) such that the kernel of \( \Theta \) for \( L/K \) equals \( H \).

3.4. Comparison of ideal groups and idele groups. Consider the trivial modulus \( m = 1 \) (with \( e_v = 0 \) for all \( v \)). Taking the restricted direct product of the valuation maps \( v: K_v^\times \to \mathbb{Z} \) gives a surjective homomorphism

\[
\mathbb{A}^\times \to I
\]

that discards the archimedean components of its input, and its kernel is \( U_1 = \prod_v \mathcal{O}_v^\times \). Thus \( \mathbb{A}^\times/U_1 \simeq I \). If we take the quotient by the image of \( K^\times \) on both sides, we find that the ray class group \( \frac{\mathbb{A}^\times}{U_{mK}^\times} \) of modulus 1 is isomorphic to the class group \( I/P = \text{Cl} \mathcal{O}_K \). The ray class field \( R_1 \) of modulus 1 is called the Hilbert class field, which can be characterized also as the
maximal abelian extension of $K$ in $K^*$ that is unramified at all places of $K$ (including the archimedean ones). We get

$$\frac{C}{U_1} = \frac{A^\times}{U_1K^\times} \cong \frac{I}{P} = \text{Cl} \, \mathcal{O}_K \cong \text{Gal}(R_1/K).$$

This can be generalized to an arbitrary modulus $m = \prod v^{e_v}$ as follows. Let $A^m \subseteq A^\times$ be the subgroup consisting of $(a_v)$ with $(a_v)$ with $a_v \in U_{m,v}$ for every $v$ with $e_v > 0$. Let $K^m = A^m \cap K^\times$. We have an isomorphism

$$\frac{A^m}{U_m} \cong I_m.$$ 

Dividing by the image of $K^m$ on both sides gives

$$\frac{A^m}{U_mK^m} \cong \frac{I_m}{P_m}.$$ 

On the other hand, $A^\times = A^mK^\times$, so there is an isomorphism

$$\frac{A^m}{K^m} \cong \frac{A^\times}{K^\times} = C.$$ 

Dividing by the image of $U_m$ on both sides, and combining with (2), we get isomorphisms

$$\frac{C}{U'_m} = \frac{A^\times}{U_mK^\times} \cong \frac{I_m}{P_m} = \text{Cl}_m \, \mathcal{O}_K \cong \text{Gal}(R_m/K).$$

4. AN INTRODUCTION TO AN INTRODUCTION TO THE LANGLANDS PROGRAM

Let $K$ be a local or global field. Every 1-dimensional character (continuous homomorphism)

$$\text{Gal}(K^*/K) \to \mathbb{C}^\times$$

factors through $\text{Gal}(K^{ab}/K)$ and has finite image. These characters form a discrete abelian group, the Pontryagin dual of the profinite group $\text{Gal}(K^{ab}/K)$. It follows that the problem of classifying finite abelian extensions of $K$ is more or less the same as the problem of describing all these characters.

The Langlands program is an attempt to understand $\text{Gal}(K^*/K)$ more completely by describing its higher-dimensional representations: the group $\mathbb{C}^\times = \text{GL}_1(\mathbb{C})$ is replaced by $\text{GL}_n(\mathbb{C})$, or even $G(\mathbb{C})$ for other linear algebraic groups $G$. The continuous homomorphisms

$$\text{Gal}(K^*/K) \to G(\mathbb{C})$$

are conjectured to correspond to certain “automorphic” objects defined intrinsically in terms of $K$, just as class field theory gives a description of the group $\text{Gal}(K^{ab}/K)$ (which is defined in terms of extrinsic objects such as finite abelian extensions, which are initially mysterious) in terms of intrinsic objects ($K^\times$ or $C$) obtained directly from $K$.

Ultimately, the program would give information about nonabelian algebraic extensions of $K$. 

7
5. Further reading

For basics on profinite groups, see [Ser02, I.§] and [Gru86]. The latter discusses infinite Galois theory as well.

For local class field theory, see [Ser86]. For the approach to global class field theory via cohomology of ideles, see [Tat86]. For a treatment of global class field theory via ideals, see [Jan96]. All these topics are covered also in [Neu99].

For an introduction to the Langlands program, see [BG03].

References


Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

Email address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/