MINT 2024 – Class field theory

Lectures by Tamás Szamuely
Notes by Davide Lombardo

Any mistakes are the fault of the scribe

September 20, 2024

Contents

Chapter 1

Class Field Theory I

Two problems in Hilbert's famous list are related to class field theory: one is solved by one of the main theorems of CFT, and the other is largely open. The one that is solved is related to *reciprocity laws*, which will be our starting point.

1.1 Reciprocity laws

1.1.1 Quadratic reciprocity

Recall the definition of the classical Legendre symbol: for p a prime and $a \in \mathbb{Z}$ prime to p, we define

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ if the equation } x^2 = a \text{ has solutions modulo p} \\ -1, \text{ otherwise} \end{cases}$$

For $p > 2$, a result of Euler gives $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$.

Theorem 1.1.1.1 (Quadratic reciprocity, Gauss)**.** *For all pairs of distinct odd primes a, b we have*

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

There are also two so-called *subsidiary laws*,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

One can consider two generalisations: replacing $\mathbb{Z}$ with the ring of integers of a number field, or replacing squares with higher powers.

1.1.2 Hilbert's reinterpretation

Consider the completions of $\mathbb{Q}$, namely $\mathbb{Q}_p$ for every prime p and $\mathbb{Q}_\infty = \mathbb{R}$.

Definition 1.1.2.1 (Hilbert symbol)**.** Let $a, b \in \mathbb{Q}_p \setminus \{0\}$, where p is a prime or ∞. We define

$$(a,b)_p = \begin{cases} 1, \text{ if the equation } x^2 = ay^2 + bz^2 \text{ has a non-trivial solution in } \mathbb{Q}_p^3 \\ -1, \text{ otherwise} \end{cases}$$

A solution (x, y, z) is non-trivial if it is different from $(0, 0, 0)$ (so, equivalently, we are asking for a $\mathbb{Q}_p$-rational point on the projective quadric with equation $x^2 = ay^2 + bz^2$).

Remark 1.1.2.2. We have the reinterpretation

$(a,b)_p = 1 \iff b$ is a norm for the extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}_p \iff a$ is a norm for the extension $\mathbb{Q}(\sqrt{b})/\mathbb{Q}_p$.

This is immediate to see by manipulating the equation in the definition of the Hilbert symbol.

Assume $p \neq 2, \infty$ and let a, b be integers. There is an explicit formula for the Hilbert symbol:

$$\begin{aligned}(a,b)_p &= \overline{[(-1)^{v_p(a)v_p(b)}a^{v_p(b)}b^{-v_p(a)}]}^{(p-1)/2} \\ &= (-1)^{(p-1)/2\cdot v_p(a)\cdot v_p(b)} \cdot \left(\frac{a}{p}\right)^{v_p(b)} \cdot \left(\frac{b}{p}\right)^{-v_p(a)},\end{aligned}$$

where the bar denotes reduction modulo p and the second equality follows from Euler's criterion. In particular, if $p \nmid a$, $(a,b) = \left(\frac{a}{p}\right)^{v_p(b)}$. There are also more complicated formulas for $p = 2$ and ∞.

Remark 1.1.2.3. Note that the minus sign in the exponent of $\left(\frac{b}{p}\right)$ does not matter, because $\left(\frac{b}{p}\right) = \pm 1$. We write the formula in this way with a view towards later generalisations.

Theorem 1.1.2.4 (Hilbert's reciprocity law)**.** *For all $a, b \in \mathbb{Z} \setminus \{0\}$ (or even $\mathbb{Q}^\times$), we have*

$$\prod_p (a,b)_p = 1.$$

Remark 1.1.2.5. If a, b are integers and $p \nmid 2ab$, then $(a,b)_p = 1$. Moreover, if a, b are both odd, then $(a,b)_2 = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$. Using these formulas, Hilbert's reciprocity law implies quadratic reciprocity.

An advantage of this formulation is that it generalises nicely to number fields, simply replacing $\mathbb{Q}_p$ with the completions $K_\mathfrak{p}$ of the number field K.

Problem 1.1.2.6 (Hilbert's 9th problem)**.** *Generalise this picture to arbitrary n-th powers and arbitrary number fields.*

1.1.3 Direct attempt at a generalisation

Assume now that $K/\mathbb{Q}$ is a finite extension such that $\mu_n \subset K$. In particular, if $n > 2$, the field K cannot be embedded in the real numbers.

We shall define, for every prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, a Hilbert symbol $(a,b)_\mathfrak{p} \in \mu_n$. It will satisfy

$$\prod_\mathfrak{p} (a,b)_\mathfrak{p} = 1 \quad \forall a, b \in K^\times.$$

For $n = 2$, the product includes the 'infinite factors' corresponding to completions isomorphic to $\mathbb{R}$; otherwise, we ignore the infinite places.

In the next lecture, we will make sense of the definitions of the following objects and check their properties.

For $\mathfrak{p} \nmid n$, and $\mathfrak{p} \neq \infty$ if $n = 2$, we set

$$(a,b)_\mathfrak{p} = \overline{(-1)^{v_p(a)v_p(b)}a^{v_p(b)}b^{-v_p(a)}}^{(q-1)/n},$$

where $q = |\mathcal{O}_K/\mathfrak{p}|$ and we identify $(\mathcal{O}_K/\mathfrak{p})^\times$ with μ_{q-1} via the inverse of the reduction map modulo $\mathfrak{p}$. In particular, if $\mathfrak{p} \nmid (a)$,

$$(a,b)_\mathfrak{p} = \left(\overline{a^{(q-1)/n}}\right)^{v_p(b)}.$$

Let now $b \in \mathfrak{p}$ be an element with $v_\mathfrak{p}(b) = 1$ and define

$$\left(\frac{a}{\mathfrak{p}}\right) := (a,b)_\mathfrak{p}.$$

By the formula above, this definition does not depend on the choice of b. With this definition, $\left(\frac{a}{\mathfrak{p}}\right)$ is the unique n-th root of unity congruent to $a^{(q-1)/n}$ modulo $\mathfrak{p}$. In particular, $\left(\frac{a}{\mathfrak{p}}\right) = 1$ if and only if the equation $x^n \equiv a \pmod{\mathfrak{p}}$ has solutions. We will show:

$(a,b)_\mathfrak{p} = 1 \Leftrightarrow b$ is a norm for the extension $K_\mathfrak{p}(\sqrt[n]{a})/K_\mathfrak{p} \Leftrightarrow a$ is a norm for the extension $K_\mathfrak{p}(\sqrt[n]{b})/K_\mathfrak{p}$.

Finally, we will show that $(a,b)_\mathfrak{p}$ is bi-multiplicative and anti-commutative.

1.2 Review of group cohomology

Let G be a group and A be a left G-module (that is, an abelian group equipped with a left action of G; yet equivalently, a left $\mathbb{Z}[G]$-module). We say that A is **trivial** if G acts trivially, i.e.,

$$\sigma a = a \quad \forall \sigma \in G, \forall a \in A.$$

Notice that, if $\mathbb{Z}$ is the trivial G-module, we have

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = A^G := \{a \in A : \sigma = a \quad \forall \sigma \in G\} : \tag{1.2.0.1}$$

such a homomorphism is determined by the image of 1, and since the G-action on $\mathbb{Z}$ is trivial and the homomorphism is G-equivariant, the image also has to be fixed by G.

Definition 1.2.0.2. We set

$$\mathrm{H}^i(G, A) := \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

The $\mathrm{H}^i(G, -)$ are covariant functors from the category of G-modules to the category of abelian groups. They are also the right derived functors of the functor of invariants $A \mapsto A^G$ (this follows from the identification, given by Equation (1.2.0.1), between the functors $A \mapsto A^G$ and $A \mapsto \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$). Given a short exact sequence

$$0 \to A \to B \to C \to 0$$

of G-modules, there exists an associated long exact sequence

$$\cdots \to \mathrm{H}^i(G, A) \to \mathrm{H}^i(G, B) \to \mathrm{H}^i(G, C) \to \mathrm{H}^{i+1}(G, A) \to \cdots$$

starting from $\mathrm{H}^0(G, A) = A^G$.

To compute $\mathrm{H}^i(G, A)$, one uses explicit resolutions of $\mathbb{Z}$.

Construction 1.2.0.3. *Consider $\mathbb{Z}[G^{i+1}]$ as a $\mathbb{Z}[G]$-module via*

$$\sigma \cdot (\sigma_0, \ldots, \sigma_i) = (\sigma\sigma_0, \ldots, \sigma\sigma_i).$$

These are free $\mathbb{Z}[G]$-modules. For $i > 0$, define a connecting map

$$\delta_i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$$

by $\delta_i = \sum_j (-1)^j s^i_j$, where

$$s^i_j : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$$

sends $(\sigma_0, \ldots, \sigma_i)$ to $(\sigma_0, \ldots, \sigma_{j-1}, \sigma_{j+1}, \ldots, \sigma_i)$.

We get a projective resolution of $\mathbb{Z}$,

$$\cdots \xrightarrow{\delta_2} \mathbb{Z}[G^2] \xrightarrow{\delta_1} \mathbb{Z}[G] \xrightarrow{\delta_0} \mathbb{Z} \to 0.$$

Terminology. *We call*

- $\mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A)$ *the i-cochains;*
- $\ker \delta_i$ *the i-cocycles;*
- $\mathrm{im}\, \delta_{i+1}$ *the i-coboundaries.*

This is not quite the construction one uses in practice. In $\mathbb{Z}[G^{i+1}]$, consider the basis

$$[\sigma_1, \ldots, \sigma_i] := (1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \ldots \sigma_i).$$

These elements freely generate $\mathbb{Z}[G^{i+1}]$ over $\mathbb{Z}[G]$, so we may identify i-cochains with functions $[\sigma_1, \ldots, \sigma_i] \mapsto a_{\sigma_1, \ldots, \sigma_i}$. In this basis, the maps δ_i become

$$a_{\sigma_1, \ldots, \sigma_i} \mapsto \sigma_1 a_{2, \ldots, \sigma_i} + \sum_{j=1}^{i} (-1)^j a_{\sigma_1, \ldots, \sigma_j\sigma_{j+1}, \ldots, \sigma_i} + (-1)^{i+1} a_{\sigma_1, \ldots, \sigma_{i-1}}.$$

Example 1.2.0.4. A 1-cocycle is a function $\sigma \mapsto a_\sigma$ satisfying $a_{\sigma_1\sigma_2} = \sigma_1 a_{\sigma_2} + a_{\sigma_1}$. It is a 1-coboundary if there exists $a \in A$ such that $a_\sigma = \sigma a - a$ for all $\sigma \in G$. In the special case when G acts trivially, $\mathrm{H}^1(G, A) = \mathrm{Hom}(G, A)$ (homomorphisms in the category of groups).

An interesting special case is when G is finite and cyclic, say generated by an element σ of order n. For a G-module A, define

$$N: \begin{array}{ccc} A & \to & A \\ a & \mapsto & \sum_{i=0}^{n-1} \sigma^i a \end{array} \quad \text{and} \quad \sigma - 1: \begin{array}{ccc} A & \to & A \\ a & \mapsto & \sigma a - a. \end{array}$$

If $A = \mathbb{Z}[G]$, then these maps give rise to the resolution

$$\cdots \xrightarrow{\mathbb{Z}} [G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\sigma\mapsto 1} \mathbb{Z} \to 0.$$

The existence of this resolution implies

$$\mathrm{H}^{2i+1}(G, A) = {}_N A/(\sigma - 1)A, \quad \mathrm{H}^{2i+2}(G, A) = A^G/NA,$$

where ${}_N A$ denotes the kernel of N.

If $H < G$ is a subgroup, there are maps

$$\mathrm{Res} : \mathrm{H}^i(G, A) \to \mathrm{H}^i(H, A) \quad \text{restriction}$$

$$\mathrm{Inf} : \mathrm{H}^i(G/H, A^H) \to \mathrm{H}^i(G, A) \quad \text{inflation (if } H \triangleleft G)$$

At the level of cocycles, these are the obvious maps. If A, B, C are G-modules, equipped with a map of G-modules $A \times B \to C$, there are cup-product maps

$$\mathrm{H}^i(G, A) \times \mathrm{H}^j(G, B) \to \mathrm{H}^{i+j}(G, C)$$

that are functorial, $\mathbb{Z}$-bilinear, and satisfy $a \cup b = (-1)^j b \cup a$.

If $G = \varprojlim_i G_i$ is a pro-finite group (inverse limit of finite groups), we say that A is a continuous G-module if $\forall a \in A$ the subgroup $G_a = \{\sigma \in G : \sigma \cdot a = a\}$ is open in G. One then defines

$$\mathrm{H}^i(G, A) = \varinjlim_j \mathrm{H}^i(G/U_j, A^{U_j}),$$

where $U_j = \ker(G \to G_j)$ and the maps in the direct limit are inflations.

Remark 1.2.0.5. One can show that $\mathrm{H}^i(G, A)$ is always a torsion abelian group (for $i > 0$) and $\mathrm{H}^i(G, V) = 0$ when V is a $\mathbb{Q}$-vector space (the second part can be deduced from the first by a classical argument: $\mathrm{H}^i(G, V)$ is finite, say of order n. Multiplication by n is an automorphism, because it is on V, and also the zero map, because it is on G. The only group for which the zero map is an automorphism is the trivial group).

Consider the case where K is a field, K_s is a separable closure of K, and $G = \mathrm{Gal}(K_s/K)$. We know that in this case $G = \varprojlim_{L/K \text{ finite Galois}, L \subseteq K_s} \mathrm{Gal}(L/K)$. We then write for simplicity $\mathrm{H}^i(K, A) := \mathrm{H}^i(G, A)$.

Theorem 1.2.0.6 (Hilbert's Theorem 90)**.** *If L/K is a finite Galois extension, we have*

$$\mathrm{H}^1(\mathrm{Gal}(L/K), L^\times) = 0,$$

and therefore also $\mathrm{H}^1(K, K_s^\times) = 0$.

Corollary 1.2.0.7. *If m is invertible in K, there exists a canonical isomorphism*

$$K^\times/K^{\times m} \xrightarrow{\sim} \mathrm{H}^1(K, \mu_m).$$

Proof. Consider the short exact sequence of Galois modules $1 \to \mu_m \to K_s^\times \xrightarrow{x\mapsto x^m} K_s^\times \to 1$. The associated long exact sequence in cohomology gives

$$\mathrm{H}^0(K, K_s^\times)^m \to \mathrm{H}^0(K, K_s^\times) \to H^1(K, \mu_m) \to H^1(K, K_s^\times) \to 0.$$

Since $H^1(K, K_s^\times) = 0$ by Hilbert 90, the claim follows. Note that the isomorphism is induced by

$$a \in K^\times \mapsto \left[\sigma \mapsto \frac{\sigma \sqrt[m]{a}}{\sqrt[m]{a}}\right].$$

□

Finally, $H^2(K, K_s^\times)$ is called the Brauer group of K and denoted by $\mathrm{Br}(K)$. Its elements correspond to finite-dimensional division algebras over K with centre K.

1.3 Back to the construction of $(a,b)_p$

The key to the construction is the following theorem of Hasse:

Theorem 1.3.0.1 (Hasse)**.** *Let K be a number field and let $\mathfrak{p}$ be a finite prime of $\mathcal{O}_K$. There is a canonical isomorphism* $\mathrm{inv} : \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$.

Sketch of proof. Note that $K_\mathfrak{p}$ is a finite extension of $\mathbb{Q}_p$. We describe the construction of the invariant map. Let $K_\mathfrak{p}^{\mathrm{nr}}$ be the maximal unramified extension of $K_\mathfrak{p}$. One first proves that $\mathrm{Br}(K_\mathfrak{p}^{\mathrm{nr}}) = 0$. It follows that

$$\mathrm{Br}(K_\mathfrak{p}) = \mathrm{H}^2(K_\mathfrak{p}, K_{\mathfrak{p},s}^\times) \cong \mathrm{H}^2\left(\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{nr}}/K_\mathfrak{p}), \left(K_\mathfrak{p}^{\mathrm{nr}}\right)^\times\right).$$

Denote by Γ the group $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{nr}}/K_\mathfrak{p})$. We have a valuation map $v : \left(K_\mathfrak{p}^{\mathrm{nr}}\right)^\times \to \mathbb{Z}$, which induces

$$\mathrm{H}^2\left(\Gamma, \left(K_\mathfrak{p}^{\mathrm{nr}}\right)^\times\right) \to \mathrm{H}^2(\Gamma, \mathbb{Z}) \cong \mathrm{H}^1(\Gamma, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}.$$

Here we have used $\mathrm{H}^2(\Gamma, \mathbb{Z}) \cong \mathrm{H}^1(\Gamma, \mathbb{Q}/\mathbb{Z})$, which comes from considering the sequence of trivial Γ-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 :$$

a segment of the long exact sequence in cohomology is

$$0 = \mathrm{H}^1(\Gamma, \mathbb{Q}) \to \mathrm{H}^1(\Gamma, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(\Gamma, \mathbb{Z}) \to \mathrm{H}^2(\Gamma, \mathbb{Q}) = 0,$$

where the zeroes come from the fact that $\mathbb{Q}$ is a $\mathbb{Q}$-vector space (see Remark 1.2.0.5). □

Construction 1.3.0.2. *Fix a primitive m-th root of unity $\omega \in \mu_m$. By Kummer theory, we have an isomorphism*

$$\delta_p : K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times m} \xrightarrow{\sim} \mathrm{H}^1(K_\mathfrak{p}, \mu_m).$$

Given $a, b \in K_\mathfrak{p}^\times$, we can consider

$$\delta_p(a) \cup \delta_p(b) \in \mathrm{H}^2(K_\mathfrak{p}, \mu_m^{\otimes 2}).$$

Since μ_m is contained in $K_\mathfrak{p}$, we can choose an isomorphism $\mu_m^{\otimes 2} \cong \mu_m$. The isomorphism does depend on the choice of ω: we send $\omega \otimes \omega \mapsto \omega$. This isomorphism then induces $\mathrm{H}^2(K_\mathfrak{p}, \mu_m^{\otimes 2}) \xrightarrow{\sim} \mathrm{H}^2(K_\mathfrak{p}, \mu_m)$.

The long exact sequence in cohomology associated with

$$1 \to \mu_m \to K_\mathfrak{p}^\times \xrightarrow{x \mapsto x^m} K_\mathfrak{p}^\times \to 1$$

gives, using Hilbert 90, an isomorphism

$$\mathrm{H}^2(K_\mathfrak{p}, \mu_m) \cong {}_m\,\mathrm{Br}(K_\mathfrak{p}).$$

Finally composing with the invariant map, we get $\mathrm{H}^2(K_\mathfrak{p}, \mu_m) \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$.

Definition 1.3.0.3. We set

$$(a,b)_p := \omega^{\mathrm{inv}(\delta_p(a) \cup \delta_p(b))}.$$

One checks that the two choices of ω we have made (one in the construction of the isomorphism $\mu_m^{\otimes 2} \cong \mu_m$, the other here, as the basis of the exponentiation) cancel out, so that this definition is independent of the choice of ω.

Remark 1.3.0.4.

1. If $a, b \in K^\times$, one can use $\delta : K^\times / K^{\times m} \xrightarrow{\sim} H^1(K, \mu_m)$ to construct $\delta(a) \cup \delta(b) \in \mathrm{H}^2(K, \mu_m^{\otimes 2})$, and $\delta_p(a) \cup \delta_p(b)$ is obtained by restriction to $\mathrm{Gal}(K_{\mathfrak{p},s}/K_\mathfrak{p}) \subseteq \mathrm{Gal}(K_s/K)$. (There is a subtlety here: the subgroup $\mathrm{Gal}(K_{\mathfrak{p},s}/K_\mathfrak{p})$ is only defined up to conjugacy, but cohomology is insensitive to conjugation.)

2. Classically, $\delta(a) \cup \delta(b)$ is the class in $\mathrm{Br}(K)$ of the cyclic algebra

$$\langle x, y \mid x^m = a, y^m = b, xy = \omega yx \rangle.$$

1.4 The theorem of Brauer-Hasse-Noether and Albert

The following is a crucial result in global class field theory. It is one of the two theorems that we will take for granted in this course.

Theorem 1.4.0.1 (Brauer-Hasse-Noether, Albert)**.** *Let K be any number field. The sequence*

$$0 \to \operatorname{Br} K \to \bigoplus_{\mathfrak{p}} \operatorname{Br} K_{\mathfrak{p}} \xrightarrow{\sum \operatorname{inv}_{\mathfrak{p}}} \mathbb{Q}/\mathbb{Z} \to 0 \tag{1.4.0.2}$$

is exact, where the arrow $\operatorname{Br} K \to \bigoplus_{\mathfrak{p}} \operatorname{Br} K_{\mathfrak{p}}$ is given by the sum of the restrictions to the local Galois groups.

Since K is arbitrary and the sum ranges over all the places of K, we also have to consider the archimedean completions $K_{\mathfrak{p}} = \mathbb{R}$ or $\mathbb{C}$. In the complex case the invariant map is trivial; in the real case it is induced by $\operatorname{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \cong \frac{\frac{1}{2}\mathbb{Z}}{\mathbb{Z}} \hookrightarrow \mathbb{Q}/\mathbb{Z}$. In the cohomological interpretation, the isomorphism is easy to prove using the fact $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ is cyclic of order 2. In the interpretation via central simple algebras, a theorem of Frobenius shows that the only non-trivial central division algebra over $\mathbb{R}$ is given by the Hamilton quaternions.

Here already the fact that the second map in Equation (1.4.0.2) lands in the direct sum, and not the direct product, of the local Brauer groups, is nontrivial.

A crucial observation is that, in the case $\mu_m \subset K$, the fact that the sequence is a complex is equivalent to the fact that

$$\prod_{\mathfrak{p}} (a, b)_{\mathfrak{p}} = 1,$$

i.e. the general reciprocity law we were looking for! One implication is clear from our work up to now. The other uses the nontrivial fact that, when $\mu_m \subset K$, every class in $\operatorname{Br} K$ is of the form $\delta(a) \cup \delta(b)$ or, in other words, that every central simple algebra over the number field K is cyclic.

The proof of the reciprocity law is not easy; it ultimately relies on explicit computations of Hilbert symbols trivialized by a cyclotomic extension. In 2017 Dustin Clausen announced a new, more conceptual approach, based on difficult K-theoretic constructions.

Chapter 2

Class Field Theory II

Let K be a finite extension of $\mathbb{Q}_p$, let $m = [K : \mathbb{Q}_p]$ and write v for the valuation of K. Recall that

$$K^\times \cong U_K \times \mathbb{Z} \cong U_K^{(1)} \times \mu_{q-1} \times \mathbb{Z},$$

where $\mathbb{Z}$ corresponds to the valuation, U_K is the group of units of the ring of integers, and $U_K^{(1)}$ is the *Einseinheitengruppe*

$$\{u = 1 + a : v(a) > 0\}.$$

Fact. $U_K^{(1)} \cong \mathbb{Z}_p^m \times F$, where F is a finite cyclic p-group and (as above) $m = [K : \mathbb{Q}_p]$. A consequence of this decomposition is that U_K is a profinite group, but $K^\times$ is not, because of the $\mathbb{Z}$ component. The profinite completion of $K^\times$ is defined as

$$\widehat{K^\times} := \varprojlim_{[K^\times : U] < \infty} K^\times / U \cong U_K \times \widehat{\mathbb{Z}}.$$

The main facts of local class field theory are encapsulated in the following result:

Theorem 2.0.0.1. *There exists a canonical homomorphism*

$$\rho_K : K^\times \to G_K^{\mathrm{ab}},$$

inducing an isomorphism of topological groups $\widehat{K^\times} \to G_K^{\mathrm{ab}}$. *Here* $G_K = \mathrm{Gal}(\overline{K}/K)$, *and for a profinite group* G, *the symbol* G^{ab} *denotes the maximal abelian profinite quotient of* G.

Definition 2.0.0.2. The map ρ_K is called the **reciprocity map**.

2.1 Construction of ρ_K via the Hilbert symbol

Fix $n \in \mathbb{Z}_{>0}$. We know that $\mathrm{H}^1(K, \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cont}}(G_K, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cont}}(G_K^{\mathrm{ab}}, \mathbb{Z}/n\mathbb{Z})$. There is also the Kummer map,

$$\delta : K^\times \to \mathrm{H}^1(K, \mu_n),$$

inducing $K^\times / K^{\times n} \cong \mathrm{H}^1(K, \mu_n)$, and the cup product

$$\mathrm{H}^1(K, \mathbb{Z}/n\mathbb{Z}) \times \mathrm{H}^1(K, \mu_n) \xrightarrow{\cup} \mathrm{H}^2(K, \mu_n) \cong {}_n\,\mathrm{Br}(K) \xrightarrow[\sim]{\mathrm{inv}} \mathbb{Z}/n\mathbb{Z}.$$

Theorem 2.1.0.1 (Special case of local Tate duality)**.** *This is a perfect pairing of finite abelian groups.*

Remark 2.1.0.2. Tate duality holds more generally for every finite G_K-module A. Setting $A^* := \mathrm{Hom}(A, \overline{K}^\times)$, the statement is that the cup-product

$$\mathrm{H}^1(K, A) \times \mathrm{H}^1(K, A^*) \to \mathrm{H}^2(K, \overline{K}^\times) = \mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite abelian groups. Notice that, in the previous application of Tate duality, we had a fixed n, so instead of $\overline{K}^\times$ we had μ_n.

Remark 2.1.0.3. Tate's original proof relied on local class field theory. There is also a Grothendieck-style proof by Serre and Tate in Serre's book *Cohomologie galoisienne* [Ser94], which ensures that our arguments are not circular.

Local Tate duality is the second theorem we will take as given, together with the exact sequence of Theorem 1.4.0.1. The proof of local Tate duality is not as hard as that of the theorem of Albert and Brauer-Hasse-Noether.

There is a chain of isomorphisms

$$K^\times/K^{\times n} \xrightarrow[\text{Kummer}]{\sim} \mathrm{H}^1(K,\mu_n) \xrightarrow[\text{Tate}]{\sim} \mathrm{Hom}(\mathrm{H}^1(K,\mathbb{Z}/n\mathbb{Z}),\mathbb{Z}/n\mathbb{Z}) \\ \cong \mathrm{Hom}(\mathrm{Hom}(G_K,\mathbb{Z}/n\mathbb{Z})),\mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\mathrm{Hom}(G_K^{\mathrm{ab}},\mathbb{Z}/n\mathbb{Z})),\mathbb{Z}/n\mathbb{Z}) \cong G_K^{\mathrm{ab}}/n.$$

In the last isomorphism, we have used duality for finite abelian group, which we can do since the finiteness is part of the statement of local Tate duality. By passing to the limit in n,

$$\widehat{K^\times} \cong \varprojlim_n K^\times/K^{\times n} \cong \varprojlim_n G_K^{\mathrm{ab}}/n \cong G_K^{\mathrm{ab}},$$

where the first isomorphism follows from the fact that the subgroups of the form $K^{\times n}$ are cofinal in the finite-index subgroups of $K^\times$, and the last isomorphism follows from the fact that G_K^{ab} is already profinite, and so profinite completion acts trivially on it. The map ρ_K is obtained as the composite

$$K^\times \to \widehat{K^\times} \xrightarrow{\sim} G_K^{\mathrm{ab}}.$$

Now let L/K be a finite abelian extension. The composition

$$\rho_{L/K} : K^\times \xrightarrow[\sim]{\rho_K} G_K^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(L/K)$$

is surjective, and we have:

Theorem 2.1.0.4. *The kernel of $\rho_{L/K}$ is $N_{L/K}(L^\times) \subset K^\times$. We then get an isomorphism*

$$K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Sketch of proof. We note at the outset that the argument will use no arithmetic, and works for arbitrary fields. See the book of Gille–Szamuely [GS17] for details.

Assume first that $\mathrm{Gal}(L/K) =: G$ is cyclic of order n. Denote by $\chi : G \to \mathbb{Z}/n\mathbb{Z}$ an isomorphism, inducing a surjective character (denoted by the same symbol) $\chi : G_K \to \mathbb{Z}/n\mathbb{Z}$. Then $\mathrm{Gal}(L/K) \cong G_K^{\mathrm{ab}}/\ker(\chi)$. One checks that the diagram

$$\begin{array}{ccccc} \mathrm{H}^1(K,\mathbb{Z}/n\mathbb{Z}) \times \mathrm{H}^1(K,\mu_m) & \xrightarrow{\cup} & \mathrm{H}^2(K,\mu) & \xrightarrow{\cong} & {}_n\,\mathrm{Br}(K) \\ \downarrow{\scriptstyle d} & & \uparrow{\scriptstyle \delta} & & \downarrow \\ \mathrm{H}^2(K,\mathbb{Z}) \quad \times \quad \mathrm{H}^0(K,\overline{K}^\times) & \xrightarrow{\cup} & \mathrm{H}^2(K,\mu) & \xrightarrow{\cong} & \mathrm{Br}(K) \end{array} \tag{2.1.0.5}$$

commutes, that is, $d\psi \cup a = \psi \cup \delta a$ for $\psi \in \mathrm{H}^1(K,\mathbb{Z}/n\mathbb{Z})$ and $a \in K = \mathrm{H}^0(K,\overline{K}^\times)$. The periodicity of cohomology of cyclic groups gives

$$\mathrm{H}^2(G,L^\times) \cong (L^\times)^G/N(L^\times) = K^\times/N_{L/K}(L^\times),$$

and one checks that this map is induced by

$$K^\times \cong H^0(K,\overline{K}^\times) \xrightarrow{\cup d\chi} \mathrm{H}^2(G,L^\times).$$

Upshot. $\chi \cup \delta a = 0 \Leftrightarrow d\chi \cup a = 0 \Leftrightarrow a \in N_{L/K}(L^\times)$, which (by our construction of the reciprocity map as $\mathrm{inv}\,(\chi \cup \delta(a))$) gives the theorem in the cyclic case.

For the general case, decompose $\mathrm{Gal}(L/K) = \bigoplus_{i=1}^r \mathrm{Gal}(L_i/K)$ where the L_i/K are cyclic and linearly disjoint, and reduce to the cyclic case. □

2.2 Special case: L/K finite unramified

Denote by λ the residue field of L and by κ the residue field of K. One knows that there is an isomorphism

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(\lambda/\kappa) \cong \mathbb{Z}/n\mathbb{Z}.$$

The Frobenius automorphism $\mathrm{Frob} : x \mapsto x^q$ of $\mathrm{Gal}(\lambda/\kappa)$ corresponds, under this isomorphism, to an element $F \in \mathrm{Gal}(L/K)$, also called the Frobenius.

Proposition 2.2.0.1. *We have*

$$\rho_{L/K}(a) = F^{v(a)}$$

for all $a \in K^\times$. In particular, $\rho_{L/K}(a) = 1$ if and only if $v(a) = 0$, and by Theorem 2.1.0.4 we see that this is also equivalent to $a \in N_{L/K}(L^\times)$. Another important special case is $v(a) = 1$, in which case $\rho_{L/K}(a) = F$ is a generator of $\mathrm{Gal}(L/K)$.

Proof. Let χ be a character of $\mathrm{Gal}(L/K)$. By construction of the reciprocity map, we have

$$\chi(\rho_{L/K}(a)) = \mathrm{inv}\,(\chi \cup \delta(a))$$

and by Diagram (2.1.0.5) we have

$$\mathrm{inv}\,(\chi \cup \delta(a)) = \mathrm{inv}(d\chi \cup a).$$

We now need to recall the definition of the invariant map. Recall that, in the unramified case, we had

$$\begin{array}{ccccccccc}
\mathrm{H}^2(G,\mathbb{Z}) \times H^0(G,L^\times) & \xrightarrow{\cup} & H^2(G,L^\times) & \xrightarrow{v} & \mathrm{H}^2(K,\mathbb{Z}) & \mathrm{H}^1(K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow[\sim]{d^{-1}} & \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\chi\mapsto\chi(F)} \mathbb{Z}/n\mathbb{Z} \\
\downarrow{\scriptstyle v} & & & & \nearrow & & & & \\
\mathrm{H}^2(G,\mathbb{Z}) \times H^0(G,\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(G,\mathbb{Z}) & & & & & &
\end{array}$$

where d is the connecting map in the long exact sequence induced by $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Inspection of this diagram gives

$$\chi(\rho_{L/K}(a)) = \chi(F^{v(a)}).$$

Since this holds for all χ, we obtain as desired $\rho_{L/K}(a) = F^{v(a)}$.

□

2.3 Back to the Hilbert symbol

Suppose $\mu_n \subset K^\times$. We defined, for $a, b \in K^\times$,

$$(a,b)_K := \omega^{\mathrm{inv}(\delta(a)\cup\delta(b))},$$

where ω is a fixed primitive n-th root of unity. Identifying μ_n with $\mathbb{Z}/n\mathbb{Z}$ by sending ω to 1, we have a correspondence

$$\delta(a) \in \mathrm{H}^1(K,\mu_n) \leftrightarrow \chi_a \in \mathrm{H}^1(K,\mathbb{Z}/n\mathbb{Z}),$$

where – writing $L = K(\sqrt[n]{a})$ – one has

$$\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Corollary 2.3.0.1. *If $|\kappa| = q$, $(n,q) = 1$, then*

$$(a,b)_K = \left[(-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)}\right]^{\frac{q-1}{n}},$$

*where $\bar{c}$ is the image of c in the residue field κ, and we identify $\kappa^\times \xrightarrow{\sim} \mu_{q-1}$. The expression $(-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)}$ is called the **tame symbol**.*

Proof. Fix $\pi \in K^\times$ of valuation 1. Using anti-commutativity and bi-multiplicativity of $(a,b)_K$ and $(u,u)_K = 1$ if u is a unit, we are reduced to proving

$$(u,\pi)_K = \overline{u}^{\frac{q-1}{n}}$$

for every unit u. As we have already discussed, the left-hand side is

$$\mathrm{inv}(\chi_u \cup \delta(\pi)) = \chi_u(\rho_{L/K}(\pi)) = \chi_u(F) \equiv \overline{\frac{\sqrt[n]{u}^q}{\sqrt[n]{u}}} = \overline{u^{(q-1)/n}}.$$

□

We have thus completely described the Hilbert symbol! Another interesting consequence is:

Corollary 2.3.0.2. *We have a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_K & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \rho_K} & & \downarrow & & \\ 1 & \longrightarrow & I_K^{\mathrm{ab}} & \longrightarrow & G_K^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \widehat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

where I_K^{ab} is the inertia subgroup.

Proof. The corollary follows from the fact that, for all $u \in U_K$, the automorphism $\rho_K(u)$ maps to 0 in every finite quotient of $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ (and is therefore 0 in $\widehat{\mathbb{Z}}$). □

Remark 2.3.0.3. The units U_K have a descending filtration

$$U_K \supset U_K^{(1)} \supset U_K^{(2)} \supset U_K^{(3)} \supset \cdots \supset U_K^{(i)} \supset \cdots$$

where $U_K^{(i)} = \{1 + a \in U_K : v(a) \geq i\}$. Via the reciprocity map, it corresponds to the filtration of G_K^{ab} by ramification subgroups in the upper numbering.

We conclude our discussion of local class field theory by the *existence theorem*.

Theorem 2.3.0.4. *Every finite index subgroup H of $K^\times$ is of the form $N_{L/K}(L^\times)$ for some finite abelian extension L/K.*

Proof. Suppose $H \subset K^\times$ is of finite index. Consider

$$K^\times/H \cong \widehat{K^\times}/\widehat{H} \xrightarrow[\rho_K]{\sim} \mathrm{Gal}(L/K)$$

for some L. The composition is $\rho_{L/K}$. From the properties of the reciprocity map already established,

$$H = \ker(\rho_{L/K}) = N_{L/K}(L^\times).$$

□

Remark 2.3.0.5. If K is a local field of characteristic $p > 0$ (i.e., a finite extension of $\mathbb{F}_q((t))$, $q = p^r$), all statements remain true, but the proof we gave only works for the prime-to-p part. One needs a separate local duality theorem to address the p-part.

Moreover, recall that finite-index subgroups of $\mathbb{Q}_p^\times$ (or more generally $K^\times$ for K a p-adic field) are automatically open. This is no longer true in positive characteristic, and the profinite completion $\widehat{K^\times}$ should be taken over *open* subgroups of finite index. Likewise, the positive characteristic version of the existence theorem holds for open subgroups of finite index.

Chapter 3

Class Field Theory III

3.1 Global class field theory: construction of the reciprocity map

Let $K/\mathbb{Q}$ be a finite extension and let $\Omega = \Omega_f \cup \Omega_\infty$ be the set of places of K, where Ω_f (resp. Ω_∞) is the set of finite (resp. Archimedean) places. For every $v \in \Omega_K$ there is a corresponding completion K_v,

$$K_v = \begin{cases} \text{finite extension of some } \mathbb{Q}_p, \text{ if } v \in \Omega_f \\ \mathbb{R} \\ \mathbb{C} \end{cases}$$

For v finite, denote $\mathcal{O}_v^\times$ the group of units of $\mathcal{O}_{K_v}$. Historically, global class field theory was proven first, and local class field theory was deduced as a consequence. Later, Hasse and Chevalley noticed that it was possible to package together the local reciprocity maps to give the global one. This is the approach that we take.

Definition 3.1.0.1 (Chevalley)**.** The **idèle group** of K is

$$I_K := \{(a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all but finitely many places } v\},$$

equipped with the *restricted product topology*. A basis of open neighbourhoods of 1 for this topology is

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v^\times,$$

where S is a finite subset of Ω_K containing Ω_∞ and $U_v \subset K_v^\times$ is open. One can prove that I_K is a locally compact topological group, and there is a diagonal embedding $K^\times \hookrightarrow I_K$ which sends a to the constant sequence $(a)_{v \in \Omega}$.

Definition 3.1.0.2. The **idèle class group** of K is

$$C_K = I_K / K^\times.$$

It is equipped with the quotient topology and is therefore locally compact. It is also Hausdorff, because the image of $K^\times$ in I_K is discrete.

Notation 3.1.0.3. Let $G_K := \mathrm{Gal}(\overline{K}/K)$, G_K^{ab} be its maximal abelian quotient, and let $G_{K_v}, G_{K_v}^{\mathrm{ab}}$ be defined similarly. For every v, there is a **canonical** embedding of $G_{K_v}^{\mathrm{ab}}$ in G_K^{ab}: at the level of G_K, the embedding is only defined up to conjugacy, but this problem disappears in the abelianisation.

For $v \in \Omega_f$, we have defined

$$\rho_{K_v} : K_v^\times \to G_{K_v}^{\mathrm{ab}} \subset G_K^{\mathrm{ab}}.$$

If $K_v = \mathbb{R}$, set

$$\begin{array}{rccc} \rho_{K_v} : & \mathbb{R}^\times & \to & \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \\ & a & \mapsto & \tau^{(1-\mathrm{sign}(a))/2}, \end{array}$$

where τ is complex conjugation (in other words, ρ_{K_v} sends $\mathbb{R}_{>0}$ to the trivial element and $\mathbb{R}_{<0}$ to complex conjugation). If $K_v = \mathbb{C}$, we simply take ρ_v to be the trivial map. Define

$$\begin{array}{rccc} \tilde{\rho_K}: & I_K & \to & G_K^{\mathrm{ab}} \\ & (a_v) & \mapsto & \prod_v \rho_{K_v}(a_v). \end{array}$$

This makes sense, because a_v is a unit for all but finitely many v, and $\rho_{K_v}(a_v)$ is trivial in every finite unramified extension. More precisely: in order for this element to make sense, it has to induce a well-defined automorphism for every finite abelian extension L/K. Such an extension is unramified at all but finitely many places. If we throw away the places that ramify in L and the places at which (a_v) is not a unit, the remaining $\rho_{K_v}(a_v)$ are trivial on L.

Theorem 3.1.0.4 (Artin, global reciprocity law)**.** *The composite*

$$K^\times \to I_K \xrightarrow{\tilde{\rho_K}} G_K^{\mathrm{ab}}$$

is trivial.

Proof. Let $\chi \in \mathrm{H}^1(K, \mathbb{Q}/\mathbb{Z})$ be a character of G_K^{ab}. It induces $\chi_v \in \mathrm{H}^1(K_v, \mathbb{Q}/\mathbb{Z})$ for each v. Let $a \in K^\times$. We will prove that $\chi(\tilde{\rho_K}(a))$ is zero for every χ, which implies that $\tilde{\rho_K}(a)$ itself is zero. Recall the connecting map $d : \mathrm{H}^1(K, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(K, \mathbb{Z})$. We have

$$d\chi \cup a \in \mathrm{H}^2(K, \overline{K}^\times) = \mathrm{Br}(K).$$

We now invoke part of the Brauer-Hasse-Noether theorem, namely the fact that

$$\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}_v(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$$

is a complex. We obtain

$$0 = \sum_v \mathrm{inv}_v(d\chi_v \cup a) = \sum_v \chi_v(\rho_{K_v}(a)) = \chi(\tilde{\rho_K}(a)),$$

which is what we had to show. □

Thus, $\tilde{\rho_K}$ factors via $K^\times$, hence induces a **global reciprocity map** $\rho_K : C_K \to G_K^{\mathrm{ab}}$. We now discuss its main properties.

Theorem A.

1. *ρ_K induces an isomorphism $\widehat{C_K} \to G_K^{\mathrm{ab}}$ of topological groups, where*

$$\widehat{C_K} := \varprojlim_{\substack{U \, open \\ [C_K : U] < \infty}} C_K/U.$$

2. *$\ker \rho_K$ is the connected component of $1 \in C_K$.*

Theorem B. *Let L/K be a finite abelian extension and $\rho_{L/K}$ be the composition $C_K \to G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$. Then $\rho_{L/K}$ is surjective, and we have*

$$\ker(\rho_{L/K}) = N_{L/K}(C_L),$$

where $N_{L/K}$ is induced by the local norms L_w/K_v.

Corollary 3.1.0.5. *The open subgroups of finite index in C_K are of the form $N_{L/K}(C_L)$ for L/K abelian.*

Corollary 3.1.0.6. *We have*

$$\ker \rho_K = \bigcap_{L/K \ finite \ abelian} N_{L/K}(C_L).$$

Remark 3.1.0.7. Corollary 3.1.0.5 (the *global existence theorem*) can be proven directly using the corresponding local result and some standard facts from algebraic number theory. The combination of Corollary 3.1.0.5 and Theorem B then implies Theorem A (1).

To derive Theorem A (2) from A (1) one first proves that if C_K^0 denotes the connected component of 1 in C_K, the quotient C_K/C_K^0 is compact. It is also totally disconnected and hence profinite; in fact, it is the maximal profinite quotient of C_K. On the other hand, C_K^0 is contained in every open subgroup of C_K (this is true in any topological group), so Theorem A (2) follows.

We now turn to the proof of Theorem B. For the surjectivity we need a special case of Chebotarev's density theorem:

Theorem 3.1.0.8. *Let L/K be a finite abelian extension of number fields and let $G = \mathrm{Gal}(L/K)$. Given $g \in G$, there exist infinitely many places $v \in \Omega_K$, unramified in L, such that $F_v = g$, where F_v is the Frobenius of v. (In fact, they have Dirichlet density $1/\#G$. For us, it is enough to know that there exists one such place.)*

Chebotarev implies the surjectivity in Theorem B: every element g of $\mathrm{Gal}(L/K)$ is of the form $g = \mathrm{Frob}_v$ for some v, and it suffices to take the idèle $a = (1, 1, \ldots, 1, \pi_v, 1, \ldots)$, where π_v is a uniformiser at v. By definition, the reciprocity map takes to $\prod_{w \neq v} \rho_w(1) \cdot \rho_v(\pi_v) = \mathrm{Id} \cdot \mathrm{Frob}_v = g$.

Remark 3.1.0.9. Chebotarev's theorem is analytic in nature. One can give completely algebraic proofs of all the main theorems of class field theory, but Chebotarev's theorem remains a crucial tool when proving refinements or generalisations.

Now for the computation of the kernel in Theorem B. First write $\mathrm{Gal}(L/K) \cong \prod_{i=1}^r \mathrm{Gal}(L_i/K) \cong \prod \mathbb{Z}/p_i^{r_i}\mathbb{Z}$ as a product of finite cyclic group of prime-power order and $L \supset L_i \supset K$. We have

$$C_K/N_{L/K}(C_L) \cong \prod_i C_K/N_{L_i/K}(C_{L_i}),$$

so we can reduce to the case where $G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/p^r\mathbb{Z}$. By cyclicity of G and periodicity of cohomology,

$$K^\times/N_{L/K}(L^\times) \cong \mathrm{H}^2(G, L^\times) = \mathrm{Br}(L/K)$$

and

$$I_K/N_{L/K}(I_L) \cong \bigoplus_{v \in \Omega_K} K_v^\times/N_{L_w/K_v}(L_w^\times) \cong \bigoplus_v \mathrm{Br}(L_w/K_v).$$

When writing the first isomorphism $I_K/N_{L/K}(I_L) \cong \bigoplus_{v \in \Omega_K} K_v^\times/N_{L_w/K_v}(L_w^\times)$, we use the fact that in an unramified extension every unit is a norm to land in the direct sum (as opposed to the direct product).

Now consider the map $C_K/N_{L/K}(C_L) \to \mathrm{Gal}(L/K)$. We will show that the source and target groups have the same order (which, together with the surjectivity already established, gives the desired isomorphism). We have

$$C_K/N_{L/K}(C_L) = \mathrm{coker}\left(K^\times/N_{L/K}(L^\times) \to I_K/N_{L/K}(I_L)\right) \cong \mathrm{coker}\left(\mathrm{Br}(L/K) \to \bigoplus_v \mathrm{Br}(L_w/K_v)\right).$$

By Albert-Brauer-Hasse-Noether (Theorem 1.4.0.1), using that $\mathrm{Br}(L/K)$ injects in $\mathbb{Q}/\mathbb{Z}$, this cokernel is a cyclic subgroup of order equal to the maximum of $|\mathrm{Br}(L_w/K_v)| = \max[L_w : K_v] = [L : K]$. The last equality follows again from Chebotarev, which (applied to a generator of the cyclic group G) gives the existence of an inert place, for which $[L_w : K_v] = \#G$.

Remark 3.1.0.10. We have relied heavily on the Albert-Brauer-Hasse-Noether theorem. However, we have not used the complete statement: we only needed the fact that the sequence is a complex and the description of the cokernel of the sum of the invariant maps. We have not used injectivity on the left (the so-called *Hasse principle*), which – while very important in itself – does not enter into the proofs of the main theorems of global class field theory.

Remark 3.1.0.11. For global fields of positive characteristic the statement of Theorem B remains true with the same proof (which is in fact simpler because the Brauer–Hasse–Noether theorem has a simpler proof in this case – see e.g. the book by Gille–Szamuely [GS17]). Theorem A holds with the following modification: the reciprocity map is injective with cokernel $\widehat{\mathbb{Z}}/\mathbb{Z}$. It is the existence theorem (Corollary 3.1.0.5) whose proof is more difficult for subgroups of index divisible by the characteristic (see the book of Artin–Tate [AT09]).

3.2 Applications

Definition 3.2.0.1. The Hilbert class field H_K of K is the maximal abelian extension of K in which every $v \in \Omega_f$ is unramified and every real place v is completely split.

When v is a real place, define $\mathcal{O}_{K_v}^\times$ to be $\mathbb{R}^\times$. We know that $\prod_v \rho_K(\mathcal{O}_{K_v}^\times)$ has trivial image in $\mathrm{Gal}(H_K/K)$ (this is the usual fact that units have trivial image in an unramified extension). It follows that $\rho_{H_K/K}$ factors through $\left(I_K/\prod_v \mathcal{O}_{K_v}^\times\right)/\mathrm{Im}(K^\times) \cong \mathrm{Cl}_K$. This induces an isomorphism

$$\mathrm{Cl}_K \cong \mathrm{Gal}(H_K/K),$$

and in particular the latter is finite, a fact which is far from trivial.

3.2.1 Generalisation: class fields

The following definitions are due to Weber (originally formulated in the language of generalised class groups rather than idèles).

Definition 3.2.1.1. A **module** is a finite formal product $\mathfrak{m} = \prod_{v\in\Omega_K} v^{n_v}$, where each n_v is a non-negative integer and all but finitely many n_v are equal to zero. If $n_v = 0$ for all Archimedean places, $\mathfrak{m}$ is simply an ideal. Put

$$U_v^{(0)} = \begin{cases} \mathcal{O}_{K_v}^\times, \text{ if } v \text{ is finite} \\ \mathbb{R}^\times, \text{ if } v \text{ is real} \\ \mathbb{C}^\times, \text{ if } v \text{ is complex.} \end{cases}$$

and, for $n_v > 0$,

$$U_v^{(n_v)} = \begin{cases} \{1 + a : v(a) \geq n_v\} \subset \mathcal{O}_{K_v}^\times, \text{ if } v \text{ is finite} \\ \mathbb{R}_{>0}, \text{ if } v \text{ is real} \\ \mathbb{C}^\times, \text{ if } v \text{ is real} \end{cases}$$

Let $I_K^{\mathfrak{m}}$ be the subgroup of I_K given by $\prod_v U_v^{(n_v)}$. Let $C_K^{\mathfrak{m}}$ be its image in C_K.

The following lemma is an easy consequence of the definition of the topology of C_K.

Lemma 3.2.1.2. *The open subgroups of finite index in C_K are precisely those that contain some $C_K^{\mathfrak{m}}$.*

Definition 3.2.1.3. Let $K^{\mathfrak{m}}/K$ be the finite abelian extension whose Galois group $\mathrm{Gal}(K^{\mathfrak{m}}/K)$ is isomorphic to $C_K/C_K^{\mathfrak{m}}$. It is called the **ray class field** (Strahlklassenkörper) associated with $\mathfrak{m}$.

The lemma then implies:

Corollary 3.2.1.4. *Every finite abelian extension is contained in some ray class field $K^{\mathfrak{m}}$ and the maximal abelian extension is the union of all ray class fields.*

Ray class fields give information on the ramification properties of abelian extensions.

Definition 3.2.1.5. For L/K finite abelian, the **conductor** of L is

$$\mathfrak{f} := \gcd\{\mathfrak{m} : L \subset K^{\mathfrak{m}}\},$$

for the obvious divisibility relation on modules ($\mathfrak{m} \mid \mathfrak{m}'$ if and only if $n_v \leq n_v'$ for all v, where n_v, n_v' are the exponents defining the modules $\mathfrak{m}, \mathfrak{m}'$ respectively).

The following is not hard to prove.

Proposition 3.2.1.6. *A finite v ramifies in L if and only if $v \mid \mathfrak{f}$. More is true: define the local conductor of L_w/K_v by*

$$\mathfrak{f}_v := \{n : \rho_{L_w/K_v}(U_{K_v}^{(n)}) = \{1\}\} \quad \text{if } v \text{ is finite,}$$

and for infinite v set

$$\mathfrak{f}_v = \begin{cases} 0, \text{ if } L_w = K_v \\ 1, \text{ if } L_w = \mathbb{C}, K_v = \mathbb{R}. \end{cases}$$

Then $\mathfrak{f} = \prod_{v\in\Omega_K} v^{f_v}$.

Remark 3.2.1.7.

1. The case of trivial $\mathfrak{m}$ (all exponents equal to 0) corresponds to the Hilbert class field.
2. A more classical approach: for $\mathfrak{m} = \prod v^{n_v}$, define

$$J_K^{\mathfrak{m}} := \left\{ \prod_v n^{r_v} : r_v = 0 \text{ if } n_v \neq 0 \right\}$$

as the group of fractional ideals prime to $\mathfrak{m}$ and $P_K^{\mathfrak{m}}$ as the subgroup

$$P_K^{\mathfrak{m}} = \{\text{principal fraction ideals } (a) \text{ with } a \in U_v^{n_v} \quad \forall v \text{ such that } n_v > 0\}.$$

One checks that there is a canonical isomorphism $C_K/C_K^{\mathfrak{m}} \xrightarrow{\sim} J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$.

3.2.2 Explicit ray class fields

There are two classical cases for which explicit generators of ray class fields are known. They gave the motivation for Weber to introduce the general notion of class fields and thereby initiate the development of class field theory.

The rational field $K = \mathbb{Q}$

All modules are of the form $m \cdot \infty^r$, where $r \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{Z}$. Through local computations, one can prove[1] that $K^{m\infty} = \mathbb{Q}(\zeta_m)$. In particular, since the maximal abelian extension is the union of all ray class fields, we obtain that the maximal abelian extension of $\mathbb{Q}$ is $\mathbb{Q}(\mu) = \bigcup_n \mathbb{Q}(\mu_n)$. This is the famous Kronecker-Weber theorem.

K imaginary quadratic

One knows that there exists an elliptic curve $E/\mathbb{C}$ such that $\mathrm{End}(E) \cong \mathcal{O}_K$. This elliptic curve can be defined over the field $K(j(E))$.

Theorem 3.2.2.1. *The field $K(j(E))$ is the Hilbert class field of K.*

Remark 3.2.2.2. If we choose a different elliptic curve E' with the same endomorphism ring, the j-invariant of E' is a Galois conjugate of $j(E)$.

Since K is totally imaginary, a module of K is just an ideal $\mathfrak{m}$ in $\mathcal{O}_K = \mathrm{End}(E)$.

Definition 3.2.2.3. A point $P \in E(\mathbb{C})$ is an **$\mathfrak{m}$-torsion point** if $\gamma(P) = 0$ for all $\gamma \in \mathfrak{m}$. Let $E[\mathfrak{m}]$ be the set of $\mathfrak{m}$-torsion points of E.

Choose a Weierstrass equation for E over $K(j(E))$, say $y^2 = x^3 + Ax + B$.

Definition 3.2.2.4 (Weber function)**.** A **Weber function** $h : E \to \mathbb{P}^1$ is given by

$$h(P) = \begin{cases} x(P), \text{ if } A, B \neq 0 \\ x(P)^2, \text{ if } B = 0 \Leftrightarrow j = 0 \\ x(P)^3, \text{ if } A = 0 \Leftrightarrow j = 1728 \end{cases}$$

Theorem 3.2.2.5 (Weber)**.** *The ray class field of K associated with $\mathfrak{m}$ is given by*

$$K^{\mathfrak{m}} = K(j(E), h(E[\mathfrak{m}])).$$

Corollary 3.2.2.6. *The maximal abelian extension of K is*

$$K(j(E), \{h(E[\mathfrak{m}]) : \mathfrak{m} \subset \mathcal{O}_K\}).$$

See Ghate's notes in the reference list for details.

[1] see the second exercise sheet

A very recent development

At the beginning of the 19th century, the cases $K = \mathbb{Q}$ and K imaginary quadratic were the only ones for which explicit generators of ray class fields were known. This led Hilbert to ask:

Hilbert's 12$^{\text{th}}$ problem. Find special generators for the maximal abelian extension of every number field.

Progress on Hilbert's 12th problem was very limited for over a century, until:

Theorem 3.2.2.7 (Dasgupta, Kakde (2024))**.** *Solution for Hilbert's 12th problem for K totally real.*

Recall that a number field is *totally real* if all its Archimedean places are real, and it is CM if is a totally imaginary quadratic extension of a totally real field. As a consequence of their work on the Brumer–Stark conjecture, Dasgupta and Kakde show that every ray class field $K^{\mathfrak{m}}/K$ that is CM and cyclic is generated by a "Brumer-Stark unit" (defined by Tate). The composite of these CM ray class fields is the maximal CM abelian extension $K^{\text{ab}}_{\text{CM}}$ of K. Consider now the map

$$\begin{array}{ccc} K^\times & \to & \{\pm 1\}^n \\ a & \mapsto & (\operatorname{sign}\sigma_1(a), \dots, \operatorname{sign}\sigma_n(a)), \end{array}$$

where $\sigma_1, \dots, \sigma_n$ are the embeddings of K into $\mathbb{R}$. Choose $\alpha_1, \dots, \alpha_n = -1 \in K$ whose images give a $\mathbb{Z}/2\mathbb{Z}$-basis of $\{\pm 1\}^n$. Then

$$K^{\text{ab}} = K^{\text{ab}}_{\text{CM}}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{n-1}}),$$

which implies that K^{ab} is generated by Brumer-Stark units and $\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{n-1}}$. This may be considered a solution to Hilbert's 12th problem, in the sense that Dasgupta had previously shown that there are explicitly computable p-adic integral formulas for the Brumer-Stark units – hence, in a sense, Brumer-Stark units are (as in the classical case) special values of interesting analytic special functions.

Bibliography

[AT09] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2017.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.