Notes on Class Field Theory

Abhiram Kumar

Contents

1 Introduction

Class field theory is one of the most important achievements of Algebraic Number Theory in the 20th century. It deals with the classification of abelian extensions of local and global fields purely in terms of the arithmetic of the base field. The Kronecker-Weber theorem accomplishes this over the rational numbers. It states that an abelian extension of the rational numbers is always contained in a cyclotomic extension (field obtained by adjoining a root of unity to the rationals).
Another important question that class field theory deals with is the decomposition of prime ideals in abelian extensions. The quadratic reciprocity law of Gauss essentially describes this in the case of quadratic extensions of the rationals. One of the central theorems of global class field theory is the Artin reciprocity law, which generalizes many of the known reciprocity laws including quadratic reciprocity.
In this note, we discuss the main results of class field theory without proofs and discuss some examples leading up to it. We also briefly review pre-requisites such as basic algebraic number theory. Our main reference is [3]. We have also used [1] and [2] for some concepts.

2 Review of ANT

For a number field K (i.e. a finite extension of $\mathbb{Q}$), we denote by $\mathcal{O}_K$, the ring of algebraic integers in K. It is known that $\mathcal{O}_K$ forms a Dedekind domain, so that any ideal of $\mathcal{O}_K$ factors uniquely into a product of prime ideals. A fractional ideal of K is an $\mathcal{O}_K$ submodule I of K such that there exists a non-zero $r \in \mathcal{O}_K$ with $rI \subset \mathcal{O}_K$. The set of all fractional ideals of K forms a group $\mathcal{I}_K$ under multiplication and the set of principal fractional ideals $\mathcal{P}_K$ forms a normal subgroup of $\mathcal{I}_K$. We can therefore form the quotient group $\mathcal{C}_K$ called the ideal class group of K. An important fact about the ideal class group is the following theorem:

Theorem 2.1. *The class group $\mathcal{C}_K$ is finite for any number field K.*

Even though the ideals of $\mathcal{O}_K$ have unique factorization into prime ideals, the elements of $\mathcal{O}_K$ might not have unique factorization into prime elements. The ideal class group $\mathcal{C}_K$ being trivial amounts to say that $\mathcal{O}_K$ is a Principal Ideal Domain (PID). A theorem about Dedekind domains says that a Dedekind domain (DD) is a PID if and only if it is a Unique Factorization Domain (UFD). The number ring $\mathcal{O}_K$ is a DD and so, in some sense, $\mathcal{C}_K$ measures the deviation of $\mathcal{O}_K$ from being a UFD.

We say that an extension L/K is abelian if it is Galois and the galois group $Gal(L/K)$ is abelian. One of the earliest theorems in class field theory is the Kronecker-Weber theorem, which describes all abelian extensions of $\mathbb{Q}$. It can be stated as the following:

Theorem 2.2. *Every abelian extension of the rational numbers is contained in a cyclotomic extension.*

A cyclotomic extension is an extension of the form $\mathbb{Q}(\zeta_n)$ where ζ_n is an n^{th} root of unity. It is natural to seek generalizations of the theorem of Kronecker-Weber to an arbitrary

number field K, instead of just $\mathbb{Q}$. This is the main goal of class field theory and it says that finite abelain extensions L of a number field K correspond to certain subgroups of something known as the idele class group, whose factor groups are isomorphic to $Gal(L/K)$.

3 Valuation Theory

3.1 Valuations

Let K be a field and $x \to |x|$ be a function from K to $\mathbb{R}$.

Definition 3.1. *The function $|x|$ is called a valuation if*

1. $|x| > 0$ *except that* $|0| = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leq |x| + |y|$

If a valuation also satisfies $|x + y| \leq \max\{|x|, |y|\}$, then it is called nonarchimedian. Otherwise it is called an archimedian valuation. An important example is the following:

Example 1. *Let R be a Dedekind ring with quotient field K and let $\mathcal{P}$ be a non-zero prime ideal in R. For a non-zero element $x \in R$, let $v_{\mathcal{P}}(x)$ denote the power to which $\mathcal{P}$ appears in the factorization of (x). Let $\mathcal{P}$ also denote the maximal ideal in the discrete valuation ring $R_{\mathcal{P}}$. We define $v_{\mathcal{P}}$ on $R_{\mathcal{P}}$ by defining $v_{\mathcal{P}}(y) = -v_{\mathcal{P}}(y^{-1})$ if $y \in K \setminus R_{\mathcal{P}}$.*
Let $P = (\pi)$ in $R_{\mathcal{P}}$ so that every non-zero element y in K can be expressed as $y = u\pi^n$ for a unit $u \in R_{\mathcal{P}}$ and some integer n. One can see that $v_{\mathcal{P}}$ satisfies the following properties:

1. *$v_{\mathcal{P}}(y)$ is an integer for each non-zero $y \in K$,*
2. *$v_{\mathcal{P}}(xy) = v_{\mathcal{P}}(x) + v_{\mathcal{P}}(y)$,*
3. *$v_{\mathcal{P}}(x + y) \geq \min\{v_{\mathcal{P}}(x), v_{\mathcal{P}}(y)\}$.*

A valuation satisfying the above three properties is called an exponential valuation on K. Note that, for any real number $c \in (0, 1)$,

$$|x| = c^{v_{\mathcal{P}}(x)}$$

defines a valuation on K. This valuation is called the $\mathcal{P}$-adic valuation on K.

Two valuations $|x|, |x|_1$ are said to be equivalent if whenever $|x| < 1$ then also $|x|_1 < 1$ for $x \in K$.

Definition 3.2. *An equivalence class of valuations on a field K is called a place (or a prime) of K.*

A theorem due to Ostrowski states the following

Theorem 3.3. *Every non-trivial absolute value on the rational numbers $\mathbb{Q}$ is equivalent to either the usual real absolute value or a p-adic absolute value for a prime p.*

Thus, for the rational numbers, the places are in one-to-one correspondence with the prime integers (if we call the eq. class of archimedian valuations the infinite prime of $\mathbb{Q}$). For a non-archimedian valuation v on K, the ring $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ is called its valuation ring. We mention Hensel's lemma below, and the valuations whose valuation ring satisfies this lemma will play a crucial role in the theory later on.
Let K be a field which is complete with respect to a nonarchimedian valuation $||$. Let $\mathcal{O}$ be the corresponding valuation ring with maximal ideal π and residue class field $\kappa = \mathcal{O}/(\pi)$.

3.2 Hensel's Lemma

An important result in valuation theory that talks about finding roots of polynomials is Hensel's lemma. Rings that satisfy this result will play a crucial role in class field theory.

Lemma 3.4. *If a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits modulo p a factorization*

$$f(x) \equiv \bar{g}(x)\bar{h}(x) \mod p$$

into relatively prime polynomials $\bar{g}, \bar{h} \in \kappa[x]$, then $f(x)$ admits a factorization

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}[x]$ such that deg(g) = deg($\bar{g}$) and $g(x) \equiv \bar{g}(x) \mod p$ and $h(x) \equiv \bar{h}(x) \mod p$.

Example 2. *Consider the polynomial $x^{p-1} - 1 \in \mathbb{Z}_p[x]$, which splits over the residue field $\mathbb{F}_p$ into distinct linear factors. By Hensel's lemma we get that $x^{p-1} - 1$ actually splits into linear factors over $\mathbb{Z}_p$. Therefore $\mathbb{Q}_p$, the field of p-adic numbers, contains all the $p-1$ roots of unity!*

Definition 3.5. *A henselian field is a field with a nonarchimedian valuation v whose valuation ring $\mathcal{O}$ satisfies Hensel's lemma. The valuation v and the valuation ring $\mathcal{O}$ are also called henselian.*

4 Moduli and Ray Class Groups

4.1 Moduli

Definition 4.1. *A modulus for K is a formal product*

$$m = \prod_p p^{n(p)}$$

taken over all primes p of K in which n(p) is a non-negative integer and $n(p) > 0$ for only a finite number of p. Furthermore, $n(p) = 0$ or 1 when p is a real infinite prime and $n(p) = 0$ when p is a complex infinite prime.

We want to generalize the notion of congruence. Let p be a real prime of K, so that K_p is isomorphic to the real field. Let $x \to x_p$ be the imbedding of K into K_p. If α and β are elements of K^*, we write

$$\alpha \equiv \beta \mod p$$

to mean α_p and β_p have the same sign.
If p is a finite prime and α and β are elements in K^* with $\alpha = \frac{a}{c}$ and $\beta = \frac{b}{d}$. Then we write,

$$\alpha \equiv \beta \mod p^n$$

if $\frac{\alpha}{\beta} = \frac{ad}{bc} \in R_p$ and this element is congruent to 1 modulo p^n.
We extend this to congruences modulo a modulus m naturally.

$$\alpha \equiv \beta \mod m$$

if

$$\alpha \equiv \beta \mod p^{n(p)}$$

for all p appearing in $m = \prod_p p^{n(p)}$.

We write $m = m_\infty m_0$ to separate the finite and infinite primes appearing in m.

4.2 Ray Class Groups

The notion of ray class groups generalizes the idea of arithmetic progression in the rational integers to algebraic integers. Let R be the ring of integers of the number field K.

Definition 4.2.

$$K_m = \{\frac{a}{b} \mid a, b \in R, aR, bR \textit{ relatively prime to } m_0\}$$

$$K_{m,1} = \{\alpha \in K_m \mid \alpha \equiv 1 \mod m\}$$

The group $K_{m,1}$ is called the "ray mod m". For a set of primes S, I^S denotes the part of the ideal class group $\mathcal{C}_K$ generated by primes outside S. We denote by I^m to mean I^S where S is the set of primes dividing m_0. In particular, I^m does not depend on the exponents of primes dividing m. Let $\mathcal{P}^*_{K,m}$ denote the subgroup of P_K (the group of principal ideals) consisting of ideals $\langle\alpha\rangle$ where $\alpha \equiv 1 \mod m$ and $\sigma(\alpha) > 0$ for every real embedding σ of K (notation, $\alpha >> 0$). The quotient $\mathcal{C}_{K,m} = \frac{\mathcal{I}_{K,m}}{\mathcal{P}_{K,m}}$ is called the ray class group of K for m and the quotient $\mathcal{C}^*_{K,m} = \frac{\mathcal{I}_{K,m}}{\mathcal{P}^*_{K,m}}$ is called the strict (narrow) class group of K for m. If we take $K = \mathbb{Q}$ and $m = m\mathbb{Z}$, we get the strict class group to be the familiar $\mathbb{Z}/m\mathbb{Z}$.
A natural question is whether these class groups are finite just like the ordinary ideal class groups of number fields. We answer this in the following proposition.

Proposition 4.3. *$\mathcal{C}^*_{K,m}$ is a finite group. In fact,*

$$\#\mathcal{C}^*_{K,m} = \frac{h_K 2^{r_1} \varphi(m)}{[\mathcal{O}^*_K : \mathcal{O}^*_{K,m}]}$$

where h_K is the class number and $\varphi(m) = \#\big(\mathcal{O}_K/m\big)^*$ and r_1 is the number of real embeddings of K.

Proof. We just give the main ingredients of the proof. Let $\mathcal{P}_K(m)$ be the set of principal fractional ideals in $\mathcal{I}_K(m)$. We have $\mathcal{I}_K(m)/\mathcal{P}_K(m) \cong \mathcal{I}_K/\mathcal{P}_K \cong \mathcal{C}_K$
Next thing to note is that $\mathcal{P}_K(m)/\mathcal{P}_K^*(m) \cong K(m)/\mathcal{O}_K^* K_m^*$ where

$$K(m) = \{\alpha \in K^* \mid \langle \alpha \rangle \in \mathcal{I}_K(m)\}$$

and

$$K_m^* = \{\alpha \in K^* \mid \alpha >> 0, \alpha \equiv 1 \mod m\}$$

Note that the map $K(m) \to \{\pm 1\}^{r_1} \big(\mathcal{O}_K/m\big)^*$ given by,

$$\alpha \mapsto (sign(\sigma_1(\alpha), sign(\sigma_2(\alpha)), \ldots, sign(\sigma_{r_1}(\alpha)))) * (\alpha + m)$$

is an epimorphism with kernel K_m^*
We then have,

$$\#\mathcal{C}_{K,m}^* = [\mathcal{I}_K(m) : \mathcal{P}_{K,m}^*] = [\mathcal{I}_K(m) : \mathcal{P}_{K,m}][\mathcal{P}_K(m) : \mathcal{P}_{K,m}^*]$$

$$= [\mathcal{I}_K(m) : \mathcal{P}_{K,m}][K(m) : K_m^*]/[\mathcal{O}_K^* K_m^* : K_m^*] = \frac{h_K 2^{r_1} \varphi(m)}{[\mathcal{O}_K^* : \mathcal{O}_{K,m}^*]}$$

□

Example 3. *Consider the quadratic field $K = \mathbb{Q}(\sqrt{3})$ and let $m = \mathcal{O}_K$. Let us compute the size of the strict (narrow) class group $\mathcal{C}_{K,m}^*$ using the above proposition. In this case, we have $r_1 = 2, h_K = 1$, and $\varphi(m) = 1$.*
We only need to compute $[\mathcal{O}_K^* : \mathcal{O}_{K,m}^*]$. By Dirichlet's unit theorem, we have,

$$\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$$

with a fundamental unit being $2 + \sqrt{3}$. Since $2 + \sqrt{3} >> 0$ we get,

$$\mathcal{O}_{K,m}^* = \langle 2 + \sqrt{3} \rangle$$

Thus, we have $[\mathcal{O}_K^* : \mathcal{O}_{K,m}^*] = 2$ and

$$\#\mathcal{C}_{K,m}^* = \frac{1 \cdot 2^2 \cdot 1}{2} = 2$$

Example 4. *Consider the imaginary quadratic field $K = \mathbb{Q}(i)$ and $m = (3)^n$. In this case, we have $r_1 = 0$ and $h_K = 1$. Let us compute $\varphi(m) = \#\big(\mathbb{Z}[i]/3^n\big)^*$.*
An element $a + ib$ of $\mathbb{Z}[i]/3^n$ is invertible if and only if there is a solution to

$$(a + ib)(c + id) = 3^n(e + if) + 1$$

where $c, d, e, f \in \mathbb{Z}$. Comparing real and imaginary parts and writing in matrix form gives

$$\begin{bmatrix} a & -b \\ a & a \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 3^e + 1 \\ 3^n f \end{bmatrix}$$

This has a solution if and only if the determinant $a^2 + b^2$ *is invertible in* $\mathbb{Z}/3^n$. *Checking for remainders of squares modulo* 3, *we get that the condition is satisfied if and only if* a *or* b *is not divisible by* 3. *So we get* $9^n - (3^{n-1})^2$ *many elements in* $\left(\mathbb{Z}[i]/3^n\right)^*$. *Therefore,* $\varphi(m) = 8 \cdot 9^{n-1}$

Again by Dirichlet's unit theorem (or just by direct computation), the units of $\mathbb{Z}[i]$ *are just* $\pm 1, \pm i$ *and the only element* $>> 0$ *among them is* 1. *Therefore by the previous proposition, the size of the ray class group is*

$$\#\mathcal{C}^*_{K,m} = \frac{1 \cdot 2^0 \cdot (8 \cdot 9^{n-1})}{4} = 2 \cdot 9^{n-1}$$

5 Abstract CFT

5.1 Tate cohomology groups

Let G be a finite group and A be a G-module. We have the following natural map:

$$N : H_0(G, A) \longrightarrow H^0(G, A)$$

defined as $N(a) = \sum_{g \in G} ga$.
The Tate-cohomology groups $\tilde{H}^n(G, A)$ are defined as follows:

- $\tilde{H}^n(G, A) = H^n(G, A)$ for $n \geq 1$
- $\tilde{H}^0(G, A) = coker(N)$
- $\tilde{H}^{-1}(G, A) = ker(N)$
- $\tilde{H}^n(G, A) = H_{-n-1}(G, A)$ for $n \leq -2$

From now on, we use Tate-cohomology groups with notation H^i instead of $\tilde{H}^i$. Let A be a continuous multiplicative G-module, where G is the Galois group $G(\bar{k}/k)$. By this we mean a multiplicative abelian group A on which the elements $\sigma \in G$ act as automorphisms on the right, $\sigma : A \to A,\ a \mapsto a^\sigma$. It must satisfy the following properties:

- $a^1 = a$
- $(ab)^\sigma = a^\sigma b^\sigma$
- $a^{\sigma\tau} = (a^\sigma)^\tau$
- $A = \bigcup_{[K:k]<\infty} A_K$

where $A_K := \{a \in A \mid a^\sigma = a,\ \forall \sigma \in G_K\}$. An important condition on the continuous G-module A is the following:
For every cyclic extension L/K, the conditions $\#H^0(G(L/K), A_L) = [L : K]$ and $\#H^{-1}(G(L/K), A_L) = 1$ are satisfied. This condition on A is called the class field axiom.
We mention Hilbert theorem 90 since it will be used later in the note.

Theorem 5.1. *For a cyclic field extension $L \mid K$, one has*

$$H^{-1}(G(L/K), L^*) = 1$$

In words, this means an element $\alpha \in L^*$ of norm 1 is of the form $\alpha = \beta^{\sigma-1}$ where $\beta \in L^*$ is some element and σ is a generator of $G(L/K)$

Definition 5.2. *A class field theory is a pair of homomorphisms $(d : G \to \tilde{\mathbb{Z}}, v : A \to \tilde{\mathbb{Z}})$, where A is a G-module satisfying the class field axiom, d is a continuous, surjective homomorphism, and v is a henselian valuation.*

5.2 The Reciprocity Map

Consider the profinite group $G = G(\bar{k}/k)$, a continuous G-module A, and a pair of homomorphisms

$$d : G \to \hat{\mathbb{Z}},\ v : A_k \to \hat{\mathbb{Z}}$$

such that d is continuous and surjective and v is henselian with respect to d.
We want to define a cannonical homomorphism

$$r_{L/K} : G(L/K) \longrightarrow A_K/N_{L/K}A_L$$

for every finite Galois extension L/K. To this end, we define

$$Frob(\tilde{L}/K) := \{\sigma \in G(\tilde{L}/K) \mid d_K(\sigma) \in \mathbb{N}\}$$

Definition 5.3. *The reciprocity map $r_{\tilde{L}/K} : Frob(\tilde{L}/K) \to A_K/N_{\tilde{L}/K}A_{\tilde{L}}$ is defined by*

$$r(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \mod N_{\tilde{L}/K}A_{\tilde{L}}$$

where Σ is the fixed field of σ and π_Σ is a prime element of A_Σ.

It is a result that the map $Frob(\tilde{L}/K) \to G(L/K)$ is a surjection and hence we get

Proposition 5.4. *For every finite Galois extension L/K, there is a cannoical homomorphism*

$$r_{L/K} : G(L/K) \longrightarrow A_K/N_{L/K}A_L$$

given by

$$r_{L/K}(\sigma) = N_{\Sigma/K}(\pi_\Sigma) \mod N_{L/K}A_L$$

This homomorphism is called the reciprocity homomorphism of L/K.

The main theorem of abstract CFT then is that this map is an isomorphism if we restrict it to the abelianization $G(L/K)^{ab}$.

Theorem 5.5. *For every finite galois extension L/K, the reciprocity homomorphism*

$$r_{L/K} : G(L/K)^{ab} \longrightarrow A_K/N_{L/K}A_L$$

is an isomorphism.

5.3 The Herbrand Quotient

One has to verify the class field axiom for the G-module A in order to apply the theorems of abstract class field theory. An excellent tool for this is what is called the Herbrand Quotient. Let G be a finite cyclic group of order n, let σ be a generator, and A a G-module. We can form the two groups $H^0(G, A)$ and $H^{-1}(G, A)$. The Herbrand Quotient of A is defined to be

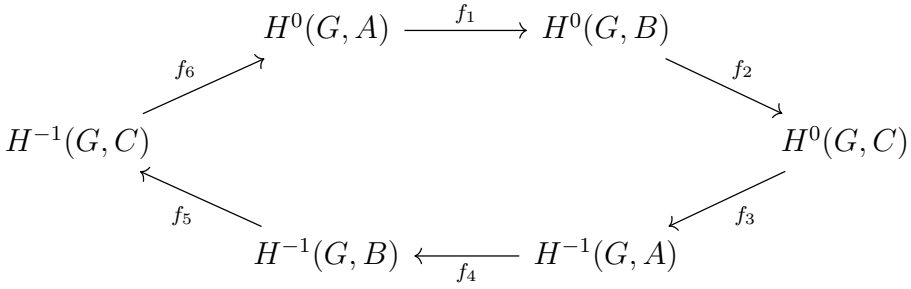
$$h(G, A) = \frac{\#H^0(G, A)}{\#H^{-1}(G, A)}$$

An important property of the Herbrand quotient is the multiplicativity.

Proposition 5.6. *If* $1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$ *is an exact sequence of* G*-modules, then one has*

$$h(G,B) = h(G,A)h(G,C)$$

Proof. Consider the exact hexagon



(1)

Let n_i be the size of the image of f_i. By exactness, we get the following:

$$\#H^0(G,A) = n_6n_1, \qquad \#H^0(G,B) = n_1n_2 \qquad \#H^0(G,C) = n_2n_3$$

$$\#H^{-1}(G,A) = n_3n_4, \qquad \#H^{-1}(G,B) = n_4n_5 \qquad \#H^{-1}(G,C) = n_5n_6$$

Therefore, $h(G,A)h(G,C) = \frac{n_6n_1}{n_3n_4} \times \frac{n_2n_3}{n_5n_6} = \frac{n_1n_2}{n_4n_5} = h(G,B)$ □

This fact is used to show that the class field axiom holds in concrete situations such as the following theorem.

6 Local CFT

We are now going to apply the abstract theory to the concrete situation of a local field k. In this setting, we have $G = Gal(\bar{k}/k), A = \bar{k}^*$ and for a finite extension K/k, we have $A_K = K^*$. We describe the Tate-cohomology groups in this situation:

Theorem 6.1. *For a cyclic extension of local fields* L/K*, we have*

$$\#H^0(G(L/K), L^*) = [L:K]$$

and

$$\#H^{-1}(G(L/K), L^*) = 1$$

Proof. The Hilbert's Theorem 90 gives the result for H^{-1}. Let $G = G(L \mid K)$. See [3] for the proof that $\#H^0(G(L/K), L^*) = [L:K]$ □

Consider the maximal unramified extension $\tilde{k}/k$. We have the following isomorphisms: $Gal(\tilde{k}/k) \cong Gal(\tilde{\kappa}/\kappa) \cong \tilde{\mathbb{Z}}$. Therefore, we obtain a continuous surjective homomorphism $d : Gal(\bar{k}/k) \to \tilde{\mathbb{Z}}$. We take $v : a \to \tilde{\mathbb{Z}}$ to be the usual normalized exponential valuation, which is henselian with respect to d. Therefore the pair (d, v) is a class field theory. The main theorem of abstract CFT (thm 3.4) applied to this gives the following:

Theorem 6.2. *For every finite Galois extension of local fields, we have a cannonical isomorphism*

$$r_{L/K} : G(L/K)^{ab} \longrightarrow K^*/N_{L/K}L^*$$

The above theorem is called the local reciprocity law. Inverting $r_{L/K}$ gives the "local notm residue symbol"

$$(., L/K) \to Gal(L/K)^{ab}$$

which is surjective with kernel $N_{L/K}L^*$.

The local reciprocity law gives a classification of the abelian extensions of a local field K.

Theorem 6.3. *The rule $L \mapsto N_{L/K}L^*$ gives a 1-1 correspondence between the finite abelian extensions of a local field K and the open subgroups $\mathcal{N} = N_{L/K}L^*$ of finite index in K^*.*
Moreover, the following hold:
$L_1 \subset L_2 \iff \mathcal{N}_{L_2} \subset \mathcal{N}_{L_1}$
$\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$
$\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$

7 Global CFT

7.1 Ideles and Idele classes

The role played by the multiplicative group of the base field in the local theory is played by the idele class group in the global theory.
Let K be a number field. An adele of K is a family $\alpha = (\alpha_p)$ of elements $\alpha_p \in K_p$ where p runs through all primes of K, and α_p is integral for all but finitely many p. The set of all adeles form a ring, denoted by $\mathbb{A}_K$. The idele group of K is defined as the unit group of $\mathbb{A}_K$. Therefore an idele is a family

$$\alpha = (\alpha_p)$$

where $\alpha_p \in K_p^*$ where α_p is a unit in the ring $\mathcal{O}_p$ of integers of K_p, for all but finitely many p. The set of all ideles of K is denoted by I_K

Definition 7.1. *The elements of the subgroup K^* of I_K are called principal ideles and the quotient group*

$$C_K = I_K/K^*$$

is called the idele class group of K.

7.2 Artin Reciprocity

We had the class field axiom in the local case satisfied by L^*. In the global case, it is satisfied by the idele class group C_K.

Theorem 7.2. *If $L \mid K$ is a cyclic extension of algebraic number fields, then*

$$\#H^0(G(L/K), C_L) = [L : k], \qquad \#H^{-1}(G(L/K), C_L) = 1$$

We now state the central theorem of global class field theory, known as the Artin reciprocity law:

Theorem 7.3. *For every Galois extension L/K of finite algebraic number fields, we have a canonical isomorphism*

$$r_{L|K} : G(L/K)^{ab} \to C_K/N_{L/K}C_L$$

As in the local theory, the reciprocity law provides a classification of all abelian extensions of a number field K. In order to do this, it is important to view C_K as a topological group. The topology on C_K is the natural one induced by valuations of all the completions K_p. The "existence theorem" of global theory is the following:

Theorem 7.4. *The map*

$$L \mapsto \mathcal{N}_L = N_{L/K}C_L$$

is a 1-1 correspondence between the finite abelian extensions L/K and the closed subgroups of finite index in C_K. Moreover, we have
$L_1 \subset L_2 \iff \mathcal{N}_{L_2} \subset \mathcal{N}_{L_1}$
$\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$
$\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$.
The field L/K corresponding to the subgroup $\mathcal{N}$ of C_K is called the class field of $\mathcal{N}$. It satisfies

$$G(L/K) \cong C_K/\mathcal{N}$$

Note that the above theorem classifies abelian extensions of a number field K purely in terms of the arithmetic of K, namely the idele class group C_K.

Definition 7.5. *The class field K^m/K for the congruence subgroup C_K^m is called the ray class field* mod m

The Galois group of the ray class field is canonically isomorphic to the ray class group mod m,

$$G(K^m \mid K) \cong C_K/C_K^m.$$

The closed subgroups of finite index in C_K are precisely those subgroups containing a congruence subgroup C_K^m and therefore we get the following result:

Proposition 7.6. *Every finite abelian extension L/K is contained in a ray class field $K^m \mid K$.*

We saw earlier in the note that the Kronecker-Weber theorem classified all abelian number fields as subfields of cyclotomic fields. The above proposition is then a generalization of this fact because ray class fields of $\mathbb{Q}$ are precisely the cyclotomic fields.

References

[1] Gerald J Janusz. *Algebraic number fields*, volume 7. American Mathematical Soc., 1996.

[2] Daniel A Marcus and Emanuele Sacco. *Number fields*, volume 1995. Springer, 1977.

[3] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.