GLOBAL CLASS FIELD THEORY, A VERY BRIEF SUMMARY

YIHANG ZHU

Let K be a number field. Class field theory provides understanding of the abelian extensions of K, in terms of arithmetic invariants of K itself. For simplicity, in the following we assume K is totally imaginary, i.e. it does not admit any embedding into $\mathbb{R}$.

1. Formulation using ideals

Recall: Let L/K is a finite Galois extension, $\mathfrak{p}$ a prime of K and $\mathfrak{P}$ a prime of L dividing $\mathfrak{p}$. Suppose $\mathfrak{P}$ is unramified. (Since L/K is Galois, this is a property of $\mathfrak{p}$.) Then we can define the Frobenius element $\sigma = \mathrm{Frob}_{\mathfrak{P}} = (\mathfrak{P}, L/K) \in \mathrm{Gal}(L/K)$, uniquely characterized by the condition that $\sigma(x) \equiv x^{\mathrm{N}\,\mathfrak{p}} \mod \mathfrak{P}$, for any $x \in \mathcal{O}_L$, where $\mathrm{N}\,\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$. When $\mathfrak{P}'$ is another prime of L above $\mathfrak{p}$, the elements $\mathrm{Frob}_{\mathfrak{P}}$ and $\mathrm{Frob}_{\mathfrak{P}'}$ are conjugate in $\mathrm{Gal}(L/K)$. In particular, if L/K is abelian, we define $\mathrm{Frob}_{\mathfrak{p}} = (\mathfrak{p}, L/K)$ to be $\mathrm{Frob}_{\mathfrak{P}}$ for $\mathfrak{P}$ as before. Note again that $(\mathfrak{p}, L/K)$ is well defined only for $\mathfrak{p}$ unramified in L.

Definition 1.1. A modulus of K is a formal expression $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$ and $e_i \in \mathbb{Z}_{>0}$. One may also think of $\mathfrak{m}$ as the integral ideal of $\mathcal{O}_K$ defined by the product. The notion of one modulus dividing another, and that of a prime ideal dividing a modulus, are defined in the evident way. The trivial modulus (i.e. empty product) will be denoted by 1.

Definition 1.2. Let $I_K^{\mathfrak{m}}$ be the free abelian group generated by primes of K not dividing $\mathfrak{m}$, regarded as a subgroup of the group I_K of fractional ideals of K.

Definition 1.3. For a modulus $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, let

$$K_{\equiv 1(\mathfrak{m})} = \left\{ \alpha \in K^\times | \alpha \in 1 + \mathfrak{p}_i^{e_i} \mathcal{O}_{K,(\mathfrak{p}_i)}, 1 \le i \le k \right\}.$$

Remark 1.4. $K_{\equiv 1(\mathfrak{m})}$ is a subgroup of $K^\times$. The condition $\alpha \in 1 + \mathfrak{p}_i^{e_i} \mathcal{O}_{K,(\mathfrak{p}_i)}$ is equivalent to requiring the power of $\mathfrak{p}_i$ appearing in the prime factorization of the fractional ideal $(\alpha - 1)\mathcal{O}_K$ to be $\ge e_i$.

Definition 1.5. Let $\alpha \in K_{\equiv 1(\mathfrak{m})}$, then $\alpha \mathcal{O}_K$ is a fractional ideal belonging to $I_K^{\mathfrak{m}}$, so we have a group homomorphism $K_{\equiv 1(\mathfrak{m})} \to I_K^{\mathfrak{m}}$. Let $\mathrm{Cl}_{\mathfrak{m}}$ be the cokernel, called the Ray class group of $\mathfrak{m}$.

Remark 1.6. When $\mathfrak{m} = 1$ is the trivial modulus, $\mathrm{Cl}_{\mathfrak{m}} = \mathrm{Cl}(\mathcal{O}_K)$ is the usual class group of $\mathcal{O}_K$.

Theorem 1.7. *Any ray class group* $\mathrm{Cl}_{\mathfrak{m}}$ *is finite.*

Let L/K be a finite abelian extension. Suppose $\mathfrak{m}$ is a modulus of K divisible by all the primes ramified in L. Then we can uniquely define a map $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ by mapping a prime $\mathfrak{p} \in I_K^{\mathfrak{m}}$ to $(\mathfrak{p}, L/K)$. This map is called the Artin map.

Definition 1.8. Let L/K be a finite abelian extension. We say a modulus $\mathfrak{m}$ of K is admissible for L/K if the following are satisfied:

(1) All the primes of K that are ramified in L divide $\mathfrak{m}$.
(2) The Artin map $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ factors through $\mathrm{Cl}_{\mathfrak{m}}$.

A priori there is no reason that condition (2) should be satisfied by any modulus. However we have

Theorem 1.9 (Artin reciprocity). *For any finite abelian extension L/K, there exists a modulus of K admissible for L/K. Moreover, this modulus can be chosen such that it is divisible only by the ramified primes.*

Remark 1.10. Artin reciprocity is a highly nontrivial statement, revealing relations between the Frobenius elements of various primes. It is one of the main theorems of class field theory.

Let L/K be a finite abelian extension. Let $\mathfrak{m}, \mathfrak{m}'$ be two moduli of K. It is clear from the definition that if $\mathfrak{m}$ is admissible for L/K and $\mathfrak{m}|\mathfrak{m}'$, then $\mathfrak{m}'$ is also admissible.

Definition 1.11. Let L/K be a finite abelian extension. Define the conductor $\mathfrak{f}_{L/K}$ of L/K to be the admissible modulus with minimal exponents among admissible moduli. Thus a modulus $\mathfrak{m}$ of K is admissible for L/K if and only if $\mathfrak{f}_{L/K}|\mathfrak{m}$.

Remark 1.12. By the last statement of Theorem 1.9, a prime of K is ramified in L if and only if it divides $\mathfrak{f}_{L/K}$.

Let $\mathfrak{m}$ be a modulus of K. For a finite abelian extension L/K, define $I_L^{\mathfrak{m}} := I_L^{\mathfrak{n}}$, where $\mathfrak{n}$ is the modulus of L equal to the product of all the primes of L above primes of K dividing $\mathfrak{m}$. We have a norm map $\mathrm{N}_{L/K} : I_L^{\mathfrak{m}} \to I_K^{\mathfrak{m}}$, defined by mapping a prime $\mathfrak{P}$ to $\mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, where $\mathfrak{p}$ is the prime of K under $\mathfrak{P}$ and $f(\mathfrak{P}/\mathfrak{p})$ is the degree of the residue extension.

Theorem 1.13 (Reciprocity isomorphism). *Let L/K be a finite abelian extension. Let $\mathfrak{m}$ be any admissible modulus. Then the Artin map $\mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective, with kernel equal to the image of $\mathrm{N}_{L/K}(I_L^{\mathfrak{m}})$ in $\mathrm{Cl}_{\mathfrak{m}}$. In other words, we have the following reciprocity isomorphism induced by the Artin map*

$$\mathrm{Cl}_{\mathfrak{m}} / \mathrm{N}_{L/K}(I_L^{\mathfrak{m}}) = I_K^{\mathfrak{m}} / \mathrm{N}_{L/K}(I_L^{\mathfrak{m}}) K_{\equiv 1(\mathfrak{m})} \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Theorem 1.14 (Existence theorem). *Let $\mathfrak{m}$ be any modulus of K. There exists a unique finite abelian extension L/K for which $\mathfrak{m}$ is admissible, and such that the Artin map induces an isomorphism*

$$\mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

The extension L is called the ray class field of $\mathfrak{m}$, denoted by $K_{\mathfrak{m}}$.

In the rest of this section we find equivalent ways of characterizing the ray class field of a modulus $\mathfrak{m}$. We first introduce the so-called "split prime principle", whose proof is independent of class field theory.

Definition 1.15. Let L/K be a finite Galois extension. Let $\mathrm{Spl}(L/K)$ be the set of primes of K that are split in L.

Lemma 1.16 (split prime principle). *Let $L_1/K, L_2/K$ be two finite Galois extensions. TFAE.*

(1) $L_1 \supset L_2$.
(2) $\mathrm{Spl}(L_1/K) \subset \mathrm{Spl}(L_2/K)$.
(3) *For some finite set* S *of primes of* K*, we have* $\mathrm{Spl}(L_1/K) - S \subset \mathrm{Spl}(L_2/K) - S$.

Remark 1.17. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are elementary. In (3), we can also replace S by a set of primes of density zero, for a suitable notion of density.

The following proposition characterizes the ray class field of a modulus.

Proposition 1.18. *Let* $\mathfrak{m}$ *be a modulus of* K*. The ray class field* $K_{\mathfrak{m}}/K$ *satisfies the following:*

(1) Let S *be the set of the prime divisors of* $\mathfrak{m}$*. Then* $\mathrm{Spl}(K_{\mathfrak{m}}/K) - S = \{\text{principal primes generated by elements of } K_{\equiv 1(\mathfrak{m})}\}$.
(2) For any finite abelian extension L/K*, we have* $L \subset K_{\mathfrak{m}}$ *if and only if* $\mathfrak{f}_{L'/K} | \mathfrak{m}$.

Proof. We use the following observation: Let L/K be a finite abelian extension. If $\mathfrak{p}$ is unramified in L, then $\mathfrak{p}$ is split in L if and only if $(\mathfrak{p}, L/K) = 1$.

(1) This follows from the admissibility of $\mathfrak{m}$ for $K_{\mathfrak{m}}/K$ and the injectivity of the Artin map $\mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Gal}(K_{\mathfrak{m}}/K)$.
(2) By hypothesis $\mathfrak{m}$ is admissible for $K_{\mathfrak{m}}/K$. If $L \subset K_{\mathfrak{m}}$, it is easy to check that $\mathfrak{m}$ is also admissible for any L/K, hence $\mathfrak{f}_{L/K}|\mathfrak{m}$. Conversely, suppose $\mathfrak{f}_{L/K}|\mathfrak{m}$, i.e. $\mathfrak{m}$ is admissible for L/K. We prove $L \subset K_{\mathfrak{m}}$ by proving $\mathrm{Spl}(K_{\mathfrak{m}}/K) - S \subset \mathrm{Spl}(L/K) - S$. Let $\mathfrak{p} \in \mathrm{Spl}(K_{\mathfrak{m}}/K) - S$. By (1) we have $\mathfrak{p} = \alpha\mathcal{O}_K$, for some $\alpha \in K_{\equiv 1(\mathfrak{m})}$. But then $(\mathfrak{p}, L/K) = 1$ since $\mathfrak{m}$ is admissible for L/K.

□

Remark 1.19. By Lemma 1.16, property (1) in the proposition uniquely characterizes the extension $K_{\mathfrak{m}}/K$. Obviously property (2) also uniquely characterizes $K_{\mathfrak{m}}$. We have actually proved the uniqueness of $K_{\mathfrak{m}}$ stated in Theorem 1.14. In practice, we can check if a given finite abelian extension is the ray class field of a modulus by checking (1). Note that the characterization (2) can also be stated as: A modulus $\mathfrak{m}$ is admissible for a finite abelian extension L/K if and only if $L \subset K_{\mathfrak{m}}$.

Remark 1.20. The conductor of $K_{\mathfrak{m}}/K$ need not be equal to $\mathfrak{m}$ in general.

Example 1.21. Take $\mathfrak{m} = 1$ to be the trivial modulus. Since $\mathfrak{m}$ is admissible for $K_{\mathfrak{m}}/K$, we see that $K_{\mathfrak{m}}/K$ is unramified everywhere. Moreover, if L/K is a finite abelian extension unramified everywhere, then $\mathfrak{f}_{L/K} = 1$. Hence by characterization (2), $L \subset K_{\mathfrak{m}}$. Thus $K_{\mathfrak{m}}$ is the maximal unramified finite abelian extension, i.e. the Hilbert class field H of K. The reciprocity isomorphism in Theorem 1.14 reads: $\mathrm{Cl}(\mathcal{O}_K) \xrightarrow{\sim} \mathrm{Gal}(H/K)$.

Example 1.22. Take $K = \mathbb{Q}$. Since $\mathbb{Q}$ is not totally imaginary, we need to modify our theory slightly. Now a modulus is either a positive integer m or a formal product of m with the symbol ∞. In the former case all the definitions are the same. If $\mathfrak{m} = m\infty$, define $\mathbb{Q}_{\equiv 1(\mathfrak{m})} := \{\alpha \in \mathbb{Q}_{\equiv 1(m)} | \alpha > 0\}$, $I_{\mathbb{Q}}^{\mathfrak{m}} := I_{\mathbb{Q}}^{m}$, $\mathrm{Cl}_{\mathfrak{m}} = I_{\mathbb{Q}}^{\mathfrak{m}}/\mathbb{Q}_{\equiv 1(\mathfrak{m})}$. We have $\mathrm{Cl}_m \cong (\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$, $\mathrm{Cl}_{m\infty} = \mathbb{Z}/m\mathbb{Z}$. Let $L/\mathbb{Q}$ be a finite abelian extension, we say $\mathfrak{m} = m\infty$ is admissible for L/K if all the primes not dividing m are unramified in L, and the map $I_{\mathbb{Q}}^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ factors through $\mathrm{Cl}_{\mathfrak{m}}$. We say $\mathfrak{m} = m$ is admissible for L/K, if all the primes not dividing m are unramified in L, and the place ∞ is also unramified in L (i.e. the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$ extends to an embedding $L \hookrightarrow \mathbb{R}$), and the map $I_{\mathbb{Q}}^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ factors through $\mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$. Then the main theorems 1.9, 1.13, 1.14 remain true. (In the last statement of Theorem 1.9, we interpret "ramified primes" as also including ∞ if $L/\mathbb{Q}$ is ramified at ∞.)

The ray class fields are just the cyclotomic fields. We have $\mathbb{Q}_{m\infty} = \mathbb{Q}(\zeta_m), \mathbb{Q}_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) = \mathbb{Q}_{m\infty} \cap \mathbb{R}$. The reciprocity isomorphisms for these are just the usual isomorphisms:

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}),$$

$$(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m + \zeta_m^{-1})/\mathbb{Q}).$$

Let $L/\mathbb{Q}$ be any finite abelian extension. We have $L \subset \mathbb{Q}_{\mathfrak{f}_{L/\mathbb{Q}}}$. This statement is the classical Kronecker-Weber theorem.

2. Formulation using ideles

Let K be a totally imaginary number field. Define $J_{K,\infty} := \prod_\sigma \mathbb{C}^\times$, where σ runs through a set of representatives of the set of embeddings $K \hookrightarrow \mathbb{C}$ modulo complex conjugation. $J_{K,\infty}$ is a topological group with the natural product topology.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. It gives rise to a discrete valuation $v_\mathfrak{p} : K^\times \to \mathbb{Z}$, sending α to the exponent of $\mathfrak{p}$ appearing in the prime factorization of the fractional ideal $\alpha\mathcal{O}_K$. Choose a real number $0 < \epsilon < 1$, we define an absolute value $|\cdot|_\mathfrak{p}$ on K, setting $|\alpha| = \epsilon^{v_\mathfrak{p}(\alpha)}$ for $\alpha \neq 0$ and $|0| = 0$. Usually we take $\epsilon = \#\mathcal{O}_K/\mathfrak{p}$, but this is not essential. We can take the completion of K with respect to this absolute value, to get a field $K_\mathfrak{p}$.[1] The discrete valuation $v_\mathfrak{p}$ extends to a discrete valuation on $K_\mathfrak{p}$. Define $\mathcal{O}_\mathfrak{p} = \{\alpha \in K_\mathfrak{p} | v_\mathfrak{p}(\alpha) \geq 0\}$.

Consider the abelian group $\prod_\mathfrak{p} K_\mathfrak{p}^\times$, where $\mathfrak{p}$ runs through all the prime ideals of $\mathcal{O}_K$. Consider its subgroup $J_K^\infty := \left\{(x_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p}^\times | x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times \text{ a.a. } \mathfrak{p}\right\}$. Here "a.a." means "for almost all", i.e. except for finitely many. We can define a topology on J_K^∞ by claiming that open sets are of the form $\prod_{\mathfrak{p}\in S} V_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_\mathfrak{p}^\times$, where S is a finite set of primes, and $V_\mathfrak{p}$ is an open subset of $\mathcal{O}_\mathfrak{p}^\times$ (the latter equipped with the topology defined by $|\cdot|_\mathfrak{p}$.)

Exercise 2.1. Check that this defines a topology on J_K^∞, and J_K^∞ is a topological group. (namely, multiplication and inversion are continuous.)

Let $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ be a modulus of K, define $U_\mathfrak{m}^\infty := \prod_{\mathfrak{p}\nmid \mathfrak{m}} \mathcal{O}_\mathfrak{p}^\times \times \prod_{i=1}^k (1+\mathfrak{p}_i^{e_i}\mathcal{O}_{\mathfrak{p}_i})$. This is a subgroup of J_K^∞. When $\mathfrak{m}$ varies, $U_\mathfrak{m}^\infty$ form a basis of open neighborhoods of $1 \in J_K^\infty$.

Define $J_K := J_{K,\infty} \times J_K^\infty$, equipped with the product topology. It is a topological group, called the group of ideles[2] of K. We have a diagonal embedding $K^\times \hookrightarrow J_K$. The image is a discrete subgroup, and the quotient $J_K/K^\times$, called the idele class group, is a Hausdorff locally compact topological group.

[1] Define the distance between $\alpha, \beta \in K$ to be $|\alpha - \beta|$, then $K_\mathfrak{p}$ is just the completion of the metric space K.

[2] The concept and the terminology "idèles" were introduced by Chevalley. "Idèles" was meant to be the abbreviation of "éléments idéal"

We have a group homomorphism

$$\mathrm{ideal} : J_K \to I_K, x = (x_\sigma, x_\mathfrak{p}) \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}.$$

Let L/K be a finite Galois extension. For any prime $\mathfrak{P}$ of L over $\mathfrak{p}$ of K, the field extension $L_\mathfrak{P}/K_\mathfrak{p}$ is finite Galois, of degree $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$. We define the homomorphism

$$\mathrm{N}_{L/K} : J_L^\infty \to J_K^\infty, (x_\mathfrak{P})_\mathfrak{P} \mapsto (\prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} x_\mathfrak{P})_\mathfrak{p}.$$

Since K is by assumption totally imaginary, the complex embeddings of K and those of L are in bijection. We define $\mathrm{N}_{L/K} : J_{L,\infty} \to J_{K,\infty}$ to be the natural isomorphism. Combining these two maps we define $\mathrm{N}_{L/K} : J_L \to J_K$. Let K^{ab} be the maximal abelian extension of K (inside a fixed algebraic closure). We equip $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the profinite topology. The following is the main theorem of the class field theory of K, formulated in the idelic language.

Theorem 2.2. *There exists a canonical homomorphism $\Psi_K : J_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. It is surjective and continuous, and satisfies the following.*

1. *(Artin reciprocity) Ψ_K is trivial on the image of the diagonal embedding $K^\times \hookrightarrow J_K$.*
2. *Let L/K be a finite abelian extension. Let $\Psi_{L/K} : J_K \to \mathrm{Gal}(L/K)$ be the composition of Ψ_K with the natural map $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$. Let $\mathfrak{m}$ be the modulus equal to the product of the primes of K ramified in L. For any $x \in J_K$ with $\mathrm{ideal}(x) \in I_K^\mathfrak{m}$, we have $\Psi_{L/K}(x) = (\mathrm{ideal}(x), L/K)$.*
3. *(Reciprocity isomorphism) Let L/K be a finite abelian extension. $\Psi_{L/K}$ induces an isomorphism $J_K/K^\times \mathrm{N}_{L/K}(J_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.*
4. *(Existence theorem) Any open subgroup of finite index of $J_K/K^\times$ arises as the kernel of $\psi_{L/K}$ for a unique finite abelian extension L/K.*

Remark 2.3. From (2) we easily see that $\Psi_K : J_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is trivial on $J_{K,\infty}$. Thus statements (1)-(3) remain true if we replace J_K by J_K^∞. The role $J_{K,\infty}$ plays in the theory is that it gives the correct topology on J_K for (4) to hold. In fact, $K^\times$ is dense in J_K^∞, so the only open subgroup of $J_K^\infty/K^\times$ is itself, and we don't get the analogous statement to (4) if we only work with J_K^∞. Moreover, when K is not necessarily totally imaginary, we need $J_{K,\infty}$ to control the ramification of the real embeddings.

We conclude with a discussion of the ray class fields in the idelic language. Let $\mathfrak{m}$ be a modulus of K. Let $U_\mathfrak{m} = J_{K,\infty} \times U_\mathfrak{m}^\infty = J_{K,\infty} \times \prod_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{O}_\mathfrak{p}^\times \times \prod_{i=1}^k (1+\mathfrak{p}_i^{e_i}\mathcal{O}_{\mathfrak{p}_i})$. It is a subgroup of J_K. The image of $U_\mathfrak{m}$ in $J_K/K^\times$ is an open subgroup of finite index. In fact the map $\mathrm{ideal} : J_K \to I_K$ induces an isomorphism $J_K/K^\times U_\mathfrak{m} \xrightarrow{\sim} \mathrm{Cl}_\mathfrak{m}$. The ray class field $J_\mathfrak{m}$ is the field corresponding to the image of $U_\mathfrak{m}$ in $J_K/K^\times$ via (4) in Theorem 2.2.