BASIC NUMBER THEORY: LECTURE 15

WENHAN DAI

1. Ideal prime to the conductor (continued)

The goal is to construct the following isomorphisms

$$I(\mathcal{O})/P(\mathcal{O}) \xrightarrow{\sim} I(\mathcal{O},f)/P(\mathcal{O},f) \xrightarrow{\sim} I_K(f)/P_{K,\mathbb{Z}}(f),$$

where f is the conductor of any order $\mathcal{O}$ of K. Recall the notations that $I_K(m)$ denotes the subgroup of $I(\mathcal{O}_K)$ generated by $\mathcal{O}_K$-ideals prime to m; $P_{K,\mathbb{Z}}(f)$ denotes the subgroup of $P(\mathcal{O}_K)$ generated by $\alpha\mathcal{O}_K$, where $\alpha = a \in \mathbb{Z} \bmod m\mathcal{O}_K$ and $(a,m)=1$.

We obtain the proposition below.

Proposition 1. *Let f be the conductor of an order $\mathcal{O}$.*

(1) *If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then $\mathfrak{a}\cap\mathcal{O}$ is an $\mathcal{O}$-ideal prime to f with the same norm.*
(2) *If $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal prime to f with the same norm.*
(3) *We obtain an isomorphism*

$$\begin{aligned} I_K(f) &\xrightarrow{\sim} I(\mathcal{O},f) \\ \mathfrak{a} &\longmapsto \mathfrak{a}\cap\mathcal{O} \\ \mathfrak{a}\mathcal{O}_K &\longleftarrow\!\shortmid\ \mathfrak{a} \end{aligned}$$

Proof. (1) Note that $\mathfrak{a}$ is prime to f because

$$\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a}+f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K.$$

We claim that $\mathfrak{a}\mathcal{O}_K\cap\mathcal{O} = \mathfrak{a}$, for which the "$\supseteq$" encompassment is obvious. For the converse, we have

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K\cap\mathcal{O} &= (\mathfrak{a}\mathcal{O}_K\cap\mathcal{O})(\mathfrak{a}+f\mathcal{O}) \\ &\subseteq \mathfrak{a} + f\mathcal{O}(\mathfrak{a}\mathcal{O}_K\cap\mathcal{O}) \\ &\subseteq \mathfrak{a} + f\mathfrak{a}\mathcal{O}_K \\ &\subseteq \mathfrak{a}+\mathfrak{a} = \mathfrak{a}. \end{aligned}$$

So the claim follows. By (1), the claim implies that $\mathfrak{a}$ and $\mathfrak{a}\mathcal{O}_K$ have the same norm.

(2) It suffices to show that if $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then

$$(\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K = \mathfrak{a}.$$

Date: December 8, 2020.

The "$\subseteq$" direction is obvious. For the converse, we have

$$\begin{aligned}\mathfrak{a} = \mathfrak{a}\mathcal{O} &= \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \\ &\subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + f\mathfrak{a} \\ &\subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + (\mathfrak{a} \cap \mathcal{O})\mathcal{O} \\ &\subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K.\end{aligned}$$

The second last containment is due to $f\mathfrak{a} \subseteq \mathfrak{a} \cap \mathcal{O}$.

So we have finished the proof. □

Proposition 2. *We obtain the isomorphism*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \xrightarrow{\sim} I_K(f)/P_{K,\mathbb{Z}}(f),$$

where f is the conductor of any order $\mathcal{O}$ of K.

Proof. This is equivalent to show that the image of $P(\mathcal{O}, f)$ via the natural homomorphism $\iota : I(\mathcal{O}, f) \to I_K(f)$ is exactly $P_{K,\mathbb{Z}}(f)$ (and hence, automatically, vice versa). For $\iota(P(\mathcal{O}, f)) \supseteq P_{K,\mathbb{Z}}(f)$ we have

$$\mathcal{O} = [1, fw_K], \quad \mathcal{O}_K = [1, w_K],$$

Note that $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$ if and only if $\alpha \equiv a \bmod f\mathcal{O}_K$, $a \in \mathbb{Z}$, and $(a, f) = 1$. This implies $N(\alpha) \equiv a^2 \bmod f$, and therefore $(N(\alpha), f) = 1$, with $\alpha\mathcal{O}_K \cap \mathcal{O} = \alpha\mathcal{O} \in P(\mathcal{O}, f)$.

For the converse containment, let $\alpha \in \mathcal{O}$ such that $\alpha\mathcal{O}$ is prime to f. Since $\mathcal{O} = [1, fw_K]$ we have $\alpha \equiv a \bmod fw_K$ for $a \in \mathbb{Z}$. Then $(a, f) = 1$, and so $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. This verifies the isomorphism. □

2. Global class field theory

For this section we assume K to be a number field, which is also the meaning of the word "global" in the topic.

Definition 3. A *modulus* of K is a formal product

$$\mathfrak{m} = \prod_p p^{n_p}$$

where n_p are non-negative integers and p runs through all finite and infinite primes. More explicitly,

- $n_p \geqslant 0$, and $n_p = 0$ for all but finitely many p;
- $n_p = 0$ if p is complex (as a place);
- $n_p \leqslant 1$ if p is real (as a place).

Notation 4. Let $\mathfrak{m}$ be any modulus of K.

(1) We say $\mathfrak{m} = \mathfrak{m}_\infty \cdot \mathfrak{m}_0$, where $\mathfrak{m}_\infty$ and $\mathfrak{m}_0$ denote the infinite part and finite part in the formal product respectively.
(2) Denote $I_K(\mathfrak{m})$ the group of all fractional ideals of $\mathcal{O}_K$ that are prime to $\mathfrak{m}_0$.
(3) Denote $P_{K,1}(\mathfrak{m})$ the subgroup of $I_K(\mathfrak{m})$ generated by $\alpha\mathcal{O}_K$, where α is such that $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all real infinite prime $\sigma \mid \mathfrak{m}_\infty$.

We remark that (2)(3) above are compatible with previous definitions if $\mathfrak{m} = (m)$ for some positive integer m. Also note that $P_{K,1}(\mathfrak{m})$ is automatically a subgroup of $P_{K,\mathbb{Z}}(\mathfrak{m})$.

Definition 5. A subgroup $H \subseteq I_K(\mathfrak{m})$ is called a *congruence subgroup for* $\mathfrak{m}$ if $P_{K,1}(\mathfrak{m}) \subseteq H$. The quotient $I_K(\mathfrak{m})/H$ is called the *generalized ideal class group* for $\mathfrak{m}$.

Now let L/K be a finite *abelian* extension. Suppose a modulus of K is divisible by any ramified prime. Recall that we have the Artin map for L/K

$$\Phi_{L/K} : I_K \longrightarrow \mathrm{Gal}(L/K), \quad \mathfrak{p} \longmapsto \left(\frac{L/K}{\mathfrak{p}}\right).$$

Here comes the main theorem of the global class field theory.

Theorem 6 (Artin reciprocity)**.** *Consider the following generalized Artin map for L/K and $\mathfrak{m}$, say*

$$\Phi_{L/K,\mathfrak{m}} = \Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K), \quad \mathfrak{p} \longmapsto \left(\frac{L/K}{\mathfrak{p}}\right).$$

Then

(1) $\Phi_{\mathfrak{m}}$ *is surjective.*
(2) *If the exponents of finite primes of* $\mathfrak{m}$ *are sufficiently large, then* $\ker \Phi_{\mathfrak{m}}$ *is a congruence subgroup of* $I_K(\mathfrak{m})$.

Remark 7. We paraphrase Theorem 6 into natural language.

(1) Since $\Phi_{\mathfrak{m}}$ is surjective, we see any finite abelian extension L/K (or equivalently, $\mathrm{Gal}(L/K)$) is overdetermined by fractional ideals of K. Also, it admits an avoidance over finitely many (finite or infinite) primes, i.e. L can be ramified over finitely many places. Moreover, if L is ramified at an infinite prime, then this prime must be real.

The group $I_K(\mathfrak{m})$ is determined by some of its congruence subgroup for the following reason. Suppose H is a congruence subgroup of two moduli $\mathfrak{m}, \mathfrak{m}'$, then $P_{K,1}(\mathfrak{m}) \subseteq I_K(\mathfrak{m}')$ and $P_{K,1}(\mathfrak{m}') \subseteq I_K(\mathfrak{m})$ at the same time. Thus $\mathfrak{m}_0'$ and $\mathfrak{m}_0$ has the same divisors, because there will never be a prime $\mathfrak{p}$ such that $\mathfrak{p} \mid \mathfrak{m}$ and $\mathfrak{p} \nmid \mathfrak{m}'$. So $I_K(\mathfrak{m}) = I_K(\mathfrak{m}')$.

(2) If $\mathfrak{m}$ is sufficiently divisible, then $\ker(\Phi_{\mathfrak{m}})$ determines an abelian Galois group $\mathrm{Gal}(L/K)$. Namely, the primes that are away from a sufficiently divisible moduli and split completely classifies finite abelian extensions of a number field.

Theorem 8 (Conductor)**.** *There exists a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that*

(1) *a prime ramifies in L if and only if it divides $\mathfrak{f}$, and*
(2) *if $\mathfrak{m}$ is a modulus such that all ramified primes dividing $\mathfrak{m}$, then* $\ker(\Phi_{\mathfrak{m}})$ *is a congruence subgroup if and only if $\mathfrak{f} \mid \mathfrak{m}$.*

Namely, there is a smallest modulus

We note by Theorem 6(2) that the more divisible the modulus $\mathfrak{m}$ is, the more likely it is that $\ker \Phi_{\mathfrak{m}}$ will be a congruence subgroup. Also, due to Theorem 8, there actually exists a minimal modulus $\mathfrak{f}$ such that $\ker(\Phi_{\mathfrak{f}})$ is exactly divisible, and it dominates the ramification primes. One should be careful about that $\mathfrak{f}$ is not simply the product with exponent 1 of ramified primes.

Example 9. Denote the mth root of unity $\zeta_m = \exp(2\pi i/m)$ for any integer $m \in \mathbb{N}$. Then the image of $m\mathbb{Z}$ in $I_{\mathbb{Q}}(m)$ is the congruence subgroup. Moreover, the conductor is $f(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = m$, such that

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

On the other hand, Kronecker-Weber theorem states that any abelian extension L of $\mathbb{Q}$ is contained in some cyclic extension $\mathbb{Q}(\zeta_n)$ for some n. Here n is also called the conductor of L in some sense.[1]

Fix a modulus $\mathfrak{m}$. We have see above that whenever a congruence subgroup H can be written as $\ker \Phi_{\mathfrak{m}}$ for some $\mathfrak{m}$, it will uniquely determine $\mathrm{Gal}(L/K)$, and hence the finite abelian extension L. The following theorem completes the theory of classification by providing the existence.

Theorem 10 (Existence)**.** *Suppose $H \subseteq I_K(\mathfrak{m})$ is a congruence subgroup. Then there is a unique abelian extension L/K whose ramified primes divide $\mathfrak{m}$ such that $H = \ker(\Phi_{\mathfrak{m}})$.*

Corollary 11. *Let L/K and M/K be abelian extensions such that $L \subseteq M$. Then there exists a modulus $\mathfrak{m}$ divided by all primes ramified in either L or M, such that*

$$P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{M/K,\mathfrak{m}}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}}).$$

Proof. We have $K \subseteq L \subseteq M$. Because of Theorem 10, we can choose $\mathfrak{m}$ to be divided by all primes ramified in M and such that $\ker(\Phi_{M/K,\mathfrak{m}})$ is a congruence subgroup. This shows that

$$P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{M/K,\mathfrak{m}}) \subseteq I_K(\mathfrak{m}).$$

On the other hand, we obtain a restriction map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ such that the diagram

$$\begin{tikzcd} I_K(\mathfrak{m}) \arrow[r, "\Phi_{M/K,\mathfrak{m}}"] \arrow[dr, "\Phi_{L/K,\mathfrak{m}}"'] & \mathrm{Gal}(M/K) \arrow[d, "\mathrm{res}"] \\ & \mathrm{Gal}(L/K) \end{tikzcd}$$

commutes. It shows that $\ker(\Phi_{L/K,\mathfrak{m}}) \supseteq \ker(\Phi_{M/K,\mathfrak{m}})$. Given M, the uniqueness of L follows from Theorem 10 easily. $\square$

We summarize that

- The goal of global class field theory is to classify all finite abelian extensions of K.
- Combining Theorem 6 and 10, we have seen that the finite abelian extensions are in one-to-one correspondence with congruence subgroups of $I_K(\mathfrak{m})$ for some fixed modulus $\mathfrak{m}$.
- The process of choosing $\mathfrak{m}$ can be understood as that of determining the ramification picture of L. Once L is given, we can take the conductor $\mathfrak{f}$ of L by Theorem 8. For $\mathfrak{m}$ divided by $\mathfrak{f}$, L will not vary; it still satisfies the condition provided by $\mathfrak{m}$.

[1]Caution: we will see in the next lecture that, by our definition, the conductor of this cyclotomic extension is $n\infty$.

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn