BASIC NUMBER THEORY: LECTURE 11

WENHAN DAI

1. Ramification theory

Let L/K be a finite Galois extension of number fields. For a prime $\mathfrak{p} \subseteq \mathcal{O}_K$, let $\mathfrak{q} \subseteq \mathcal{O}_L$ be the prime lying above $\mathfrak{p}$. Recall that we have defined the decomposition group $D(\mathfrak{q} \mid \mathfrak{p})$ and the inertia group $I(\mathfrak{q} \mid \mathfrak{p})$. We obtain

$$|\operatorname{Gal}(L/K)| = [L : K] = efg, \quad |D(\mathfrak{q} \mid \mathfrak{p})| = ef, \quad |I(\mathfrak{q} \mid \mathfrak{p})| = e.$$

Let K' be a subextension of L/K and $\mathfrak{p}'$ be a prime of K' above $\mathfrak{p}$. Then

$$D(\mathfrak{q} \mid \mathfrak{p}') = D(\mathfrak{q} \mid \mathfrak{p}) \cap \operatorname{Gal}(L/K'), \quad I(\mathfrak{q} \mid \mathfrak{p}') = I(\mathfrak{q} \mid \mathfrak{p}) \cap \operatorname{Gal}(L/K').$$

Definition 1. Fix a finite Galois extension L/K.

(1) The *decomposition field*, denoted by L_D, is the intermediate field fixed by $D(\mathfrak{q} \mid \mathfrak{p})$.
(2) The *inertia field*, denoted by L_I, is the intermediate field fixed by $I(\mathfrak{q} \mid \mathfrak{p})$.

$$\begin{tikzcd} L \arrow[d, dash, "e"] \arrow[d, dash, bend right, "I(\mathfrak{q}|\mathfrak{p})"'] \arrow[dd, dash, bend left, "D(\mathfrak{q}|\mathfrak{p})"] \\ L_I \arrow[d, dash, "f"'] \\ L_D \arrow[d, dash, "g"'] \\ K \end{tikzcd}$$

Proposition 2. *Keep the same setups as above.*

(1) $K' \subseteq L_D$ *if and only if* $e(\mathfrak{p}' \mid \mathfrak{p}) = f(\mathfrak{p}' \mid \mathfrak{p}) = 1$, *namely* $\mathfrak{p}$ *splits completely in* K'; $K' \supseteq L_D$ *if and only if* $\mathfrak{q}$ *is the only prime above* $\mathfrak{p}'$.
(2) $K' \subseteq L_I$ *if and only if* $e(\mathfrak{p}' \mid \mathfrak{p}) = 1$, *namely* $\mathfrak{p}$ *unramifies in* K'; $K' \supseteq L_I$ *if and only if* $\mathfrak{q}$ *is totally ramified over* $\mathfrak{p}'$.

Theorem 3. *Let L/K and M/K be finite extensions of number fields. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. Then $\mathfrak{p}$ unramifies (resp. splits completely) in L and M if and only if $\mathfrak{p}$ unramifies (resp. splits completely) in LM.*

Proof. The ($\Leftarrow$) direction is easy by Proposition 2. As for ($\Rightarrow$), let N be the Galois closure over LM/K. Choose an arbitrary prime $\mathfrak{q} \subseteq \mathcal{O}_N$ above $\mathfrak{p}$. If $\mathfrak{p}$ is unramified in both L and M, then $L, M \subseteq N_I$ by Proposition 2, and hence $LM \subseteq N_I$. So that $\mathfrak{p}$ is unramified in LM. Similarly, suppose $L, M \subseteq N_D$, then $LM \subseteq N_D$. Thus $\mathfrak{p}$ splits completely in LM. $\square$

Date: November 10, 2020.

Proof of Proposition 2. We work on (1) only, and the proof of (2) follows by similar argument. We obtain

$$\begin{aligned} & e(\mathfrak{p}' \mid \mathfrak{p}) = f(\mathfrak{p}' \mid \mathfrak{p}) = 1, \\ \Longleftrightarrow\ & D(\mathfrak{p}' \mid \mathfrak{p}) = I(\mathfrak{p}' \mid \mathfrak{p}) = \{e\}, \\ \Longleftrightarrow\ & e(\mathfrak{q} \mid \mathfrak{p}) = e,\ f(\mathfrak{q} \mid \mathfrak{p}) = f, \\ \Longleftrightarrow\ & D(\mathfrak{q} \mid \mathfrak{p}') = D(\mathfrak{q} \mid \mathfrak{p}),\ I(\mathfrak{q} \mid \mathfrak{p}') = I(\mathfrak{q} \mid \mathfrak{p}), \\ \Longleftrightarrow\ & D(\mathfrak{q} \mid \mathfrak{p}) \subseteq \mathrm{Gal}(L/K'), \\ \Longleftrightarrow\ & K' \subseteq L_D. \end{aligned}$$

□

2. Genus field (continued)

Let K be an imaginary quadratic field and L be the Hilbert class field of K.

Theorem 4. *Denote μ the number of primes dividing d_K. Let $p_1, \dots, p_r$ be all odd primes dividing d_K. Then*

(1) *The genus field of K is the maximal unramified extension of K which is an abelian extension of $\mathbb{Q}$.*
(2) *The genus field $M = K(\sqrt{p_1^*}, \dots, \sqrt{p_r^*})$.*
(3) *The number of genera of discriminant d_K equals*

$$2^{\mu-1} = |C(\mathcal{O}_K)/C(\mathcal{O}_K)^2| = |\,\mathrm{Gal}(M/K)|.$$

(4) *The principal genus consists of square classes, i.e. the image of elements in $C(d_K)^2$.*

Lemma 5. *Let L, M be two abelian extensions of a number field K. Fix $\mathfrak{p} \subseteq \mathcal{O}_K$ an odd prime. Then*

(1) *$\mathfrak{p}$ is unramified in LM if and only if $\mathfrak{p}$ is unramified in both L and M respectively.*
(2) *If $\mathfrak{p}$ is unramified in LM, then the natural group homomorphism*

$$\begin{aligned} \mathrm{Gal}(LM/K) &\longrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \\ \left(\frac{LM/K}{\mathfrak{p}}\right) &\longmapsto \left(\left(\frac{L/K}{\mathfrak{p}}\right), \left(\frac{M/K}{\mathfrak{p}}\right)\right) \end{aligned}$$

is injective.

Lemma 6. *Fix $a \in \mathbb{Z}$. The field extension $K(\sqrt{a})$ is unramified over K if and only if a can be chosen such that $a \equiv 1 \bmod 4$ and $a \mid d_K$.*

Proof. Suppose $a \equiv 1 \bmod 4$ and $a \mid d_K$. Then write $d_K = ab$ with $(a, b) = 1$. Note that $\sqrt{d_K} \in K$, so that $K(\sqrt{a}) = K(\sqrt{b})$. If $\mathfrak{p} \nmid 2$ then $\mathfrak{p} \nmid 2a$ or $\mathfrak{p} \nmid 2b$. By Lemma 3 in Lecture 10 $\mathfrak{p}$ is unramified. On the other hand, 2 unramifies in $\mathbb{Q}(\sqrt{a})$ and 2 is either unramified or totally ramified in K. Consequently, if $\mathfrak{p} \mid 2$, then $\mathfrak{p}$ is unramified. This shows that $K(\sqrt{a})$ is unramified over K. The converse direction is left as an exercise. □

Last time we have proved Theorem 4(1).

Proof of Theorem 4(2). As $\mathrm{Gal}(M/K) \simeq C(\mathcal{O}_K)/C(\mathcal{O}_K)^2$, we see M is a compositum of quadratic extensions of K. Also, $\mathrm{Gal}(M/\mathbb{Q})$ is generated by $\mathrm{Gal}(M/K)$ and τ, where τ is the complex conjugation. Hence

$$\mathrm{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^m$$

for some m. It follows that

$$\begin{aligned} M &= \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m}) = K(\sqrt{a_1}, \dots, \sqrt{a_m}) \\ &\subseteq K(\sqrt{p_1^*}, \dots, \sqrt{p_r^*}) \\ &= \mathbb{Q}(\sqrt{d_K}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}) =: M^* \end{aligned}$$

where $a_1, \dots, a_m \in \mathbb{Z}$ and $a_i \equiv 1 \bmod 4$, $a_i \mid d_K$ (so that each a_i is a product of some p_j^*'s). Note that M^* is an abelian extension of $\mathbb{Q}$. In particular, M^* is abelian an unramified over K. As M is the genus field, by Theorem 4(1) it is maximal among the unramified abelian extensions of $\mathbb{Q}$, we have $M^* \subseteq M$, and hence $M^* = M$. $\square$

To prove (3), we have

$$[M^* : \mathbb{Q}] = 2^r = 2^\mu, \quad |C(\mathcal{O}_K)/C(\mathcal{O}_K)^2| = 2^{\mu-1}.$$

If $d_K \equiv 1 \bmod 4$ then $M^* = M = \mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_r^*})$. If $d_K = -4n$ for $n > 0$, then

$$M = M^* = \begin{cases} \mathbb{Q}(\sqrt{-1}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}) & n \equiv 1 \bmod 4, \\ \mathbb{Q}(\sqrt{-2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}) & n \equiv 2 \bmod 8, \\ \mathbb{Q}(\sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}) & n \equiv 6 \bmod 8. \end{cases}$$

To describe the image of Galois groups under the map with genera classes as the target, the Artin map is in need. Denote $K_i = K(\sqrt{p_i^*})$. The Artin reciprocity map has a post-composition

$$\left(\frac{M/K}{\cdot}\right) : I_K \to \mathrm{Gal}(M/K) \to \prod_{i=1}^r \mathrm{Gal}(K_i/K) \simeq \{\pm 1\}^r$$

where M is the genus field of K. It induces

$$\Phi_K : I_K \longrightarrow \{\pm 1\}^r.$$

Claim: for each fractional ideal $\mathfrak{a} \subseteq \mathcal{O}_K$,

$$\Phi_K(\mathfrak{a}) = \left(\left(\frac{N(\mathfrak{a})}{p_1}\right), \dots, \left(\frac{N(\mathfrak{a})}{p_r}\right) \right).$$

For this, it suffices to show for each $\mathfrak{p} \subseteq \mathcal{O}_K$ prime that

$$\left(\frac{K_i/K}{\mathfrak{p}}\right)(\sqrt{p_i^*}) = \left(\frac{N(\mathfrak{p})}{\mathfrak{p}}\right)\sqrt{p_i^*}$$

for $i = 1, \dots, r$. Suppose $\mathfrak{p} \nmid 2$ and $\mathfrak{q} \mid \mathfrak{p}$. Then

$$\left(\frac{K_i/K}{\mathfrak{p}}\right)(\sqrt{p_i^*}) \equiv (\sqrt{p_i^*})^{N(\mathfrak{p})} = (p_i^*)^{\frac{N(\mathfrak{p})-1}{2}} \sqrt{p_i^*} \bmod \mathfrak{q}.$$

If $N(\mathfrak{p}) = p$, then

$$(p_i^*)^{\frac{N(\mathfrak{p})-1}{2}} \equiv \left(\frac{p_i^*}{p}\right) = \left(\frac{p}{p_i^*}\right)$$

by quadratic reciprocity as $p_i^* \equiv 1 \bmod 4$. Otherwise $N(\mathfrak{p}) = p^2$, and then

$$(p_i^*)^{\frac{N(\mathfrak{p})-1}{2}} \equiv \left(\frac{p^2}{p_i^*}\right) = \left(\frac{p}{p_i^*}\right)^2 = 1.$$

This almost finishes the proof of (3). The remaining details are omitted.

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