BASIC NUMBER THEORY: LECTURE 9

WENHAN DAI

Hilbert class field (continued)

Let L/K be a finite Galois extension and $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime that is unramified in L. Let $\mathfrak{q} \subseteq \mathcal{O}_L$ be an ideal lying above $\mathfrak{p}$. Recall that the Artin symbol is a unique element of $\mathrm{Gal}(L/K)$ such that for each $\alpha \in \mathcal{O}_L$,

$$\left(\frac{L/K}{\mathfrak{q}}\right)(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{q}.$$

It enjoys the following basic properties.

Corollary 1. *Resume the same notation as before.*

(1) *For each $\sigma \in \mathrm{Gal}(L/K)$,*

$$\left(\frac{L/K}{\sigma(\mathfrak{q})}\right) = \sigma\left(\frac{L/K}{\mathfrak{q}}\right)\sigma^{-1}.$$

(2) *The order of $\left(\frac{L/K}{\mathfrak{q}}\right)$ is the inertia degree $f(\mathfrak{q} \mid \mathfrak{p})$.*[1]

(3) *The prime $\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{q}}\right) = 1$.*

By Corollary 1(1), if L/K is abelian, then the artin symbol $\left(\frac{L/K}{\mathfrak{q}}\right)$ is independent of the choice of the prime $\mathfrak{q}$ above $\mathfrak{p}$. In this case, we denote it by $\left(\frac{L/K}{\mathfrak{p}}\right)$ if no confusion arises. The reader must be careful on the definition that $\mathfrak{p}$ must be unramified.

Example 2. Let $K = \mathbb{Q}(\sqrt{-3})$ with $\mathcal{O}_K = \mathbb{Z}[\omega]$. Suppose $L = K(\sqrt[3]{2})$. It turns out that

$$\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}, \quad \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3.$$

We first check the ramification. Say $\alpha = \sqrt[3]{2}$ has a minimal polynomial $f(x) = x^3 - 2$, whose discriminant has only two prime divisors $2, 3$. Hence p is unramified in $\mathbb{Q}(\sqrt[3]{2})$ whenever $p \neq 2, 3$. On the other hand, $d_K = -3$ and thus for $p \neq 3$, p is unramified in K. Combining these, p unramifies in L when $p \neq 2, 3$. The claim on Artin symbol goes as follows. Let $\pi \nmid 2, 3$ be a prime ideal in $\mathcal{O}_K$. Then

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) = \left(\frac{2}{\pi}\right)_3 \cdot \sqrt[3]{2}.$$

To prove it, let $\mathfrak{q} \subseteq \mathcal{O}_L$ be any prime above (π). Then $\left(\frac{L/K}{\mathfrak{q}}\right) = \left(\frac{L/K}{\pi}\right)$, and by definition,

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) \equiv (\sqrt[3]{2})^{N(\pi)} \bmod \mathfrak{q}.$$

Date: November 3, 2020.

[1]Recall that for the Galois extension L/K, all inertia degrees for $\mathfrak{q}$ over $\mathfrak{p}$ are the same.

Also,

$$(\sqrt[3]{2})^{N(\pi)} = 2^{\frac{N(\pi)-1}{3}} \cdot \sqrt[3]{2} \equiv \left(\frac{2}{\pi}\right)_3 \cdot \sqrt[3]{2} \bmod \mathfrak{q}.$$

This proves the claim.

Recall that the inertia group I_K is the free abelian group generated by all finite prime ideals of K. Via quotienting by the principal ideal group P_K, we get the ideal class group $\mathrm{Cl}(\mathcal{O}_K) = I_K/P_K$.

Definition 3 (Artin reciprocity map)**.** Let L/K be the Hilbert class field (i.e. the maximal unramified abelian extension). The *Artin reciprocity map* is a group homomorphism

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K) = G_{L/K}^{\mathrm{ab}}$$

sending a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ to the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Definition 4. A finitely generated $\mathcal{O}_K$-submodule of K is called a *fractional ideal.* Among the fractional ideals, those of the form $\alpha\mathcal{O}_K$ for $\alpha \in K^\times$ are called *principal fractional ideals.*

Proposition 5.

1. *If $\mathfrak{a}$ is a nonzero fractional ideal, then there is a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$.*
2. *The set of fractional ideals is*

$$\{\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \mid \mathfrak{p}_i \text{ distinct prime ideals, } r_i \in \mathbb{Z}\}.$$

Namely, the fractional ideals admit unique prime factorizations with integral exponents.

It turns out that I_K is isomorphic to the abelian group of fractional ideals. The most important ingredient is that

Theorem 6. *The group of principal fractional ideals, denoted by P_K, is exactly the kernel of Artin reciprocity map, i.e.*

$$P_K = \ker\left(\frac{L/K}{\cdot}\right).$$

Corollary 7. *Let L be the Hilbert class field of a number field K. The following are equivalent:*

- *$\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime that splits completely in L;*
- *$\mathfrak{p}$ is a principal fractional ideal, i.e. $\mathfrak{p} \in P_K$;*
- *$\left(\frac{L/K}{\mathfrak{p}}\right) = 1$;*
- *$p \in \ker\left(\frac{L/K}{\cdot}\right)$.*

Using these results, we are ready to state the main theorem about the course topic.

Theorem 8. *Let $K = \mathbb{Q}(\sqrt{-n})$ for $n \not\equiv 3 \bmod 4$ square-free. Denote L the Hilbert class field of K. Fix $p \nmid n$ an odd prime. Then*

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$

Proof. The condition that $n \not\equiv 3 \bmod 4$ is square-free implies $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. Assume $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Then there is some principal prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $p\mathcal{O}_K = \mathfrak{p} \cdot \overline{\mathfrak{p}}$. By Corollary 7, $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ split completely in L. On the other hand, since $p \nmid 2n$ we see $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Hence $p\mathcal{O}_K$ splits completely in L.

Conversely, suppose p splits completely in L. Then it splits completely in K in particular. Let $p = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 \neq \mathfrak{p}_2$ both split completely in L. Hence $\mathfrak{p}_1, \mathfrak{p}_2$ are principal by Corollary 6. Taking $\mathfrak{p}_1 = (x + \sqrt{-n}y)$ and $\mathfrak{p}_2 = (x - \sqrt{-n}y)$ finishes the proof. □

Lemma 9. *Let K be an imaginary quadratic field and L be its Hilbert class field. Then $L/\mathbb{Q}$ is a Galois extension.*

Proof. Denote τ the complex conjugation on K. Then $\tau(K) = K$ and $\tau(L) = \tau(K)^{\mathrm{Hilb}}$. Hence $\tau(L) = L$ with $L^\tau \cap K = \mathbb{Q}$. This shows $L/\mathbb{Q}$ is Galois. □

Proposition 10. *Let K be an imaginary quadratic field and L/K a finite extension such that $L/\mathbb{Q}$ is Galois. Then*

1. *$L = K(\alpha)$ for some real algebraic integer α;*
2. *let f be the monic minimal polynomial of α as in (1) over $\mathbb{Q}$. Fix a prime number $p \nmid \operatorname{disc} f$. Then p splits completely in L if and only if $\left(\frac{d_K}{p}\right) = 1$ and $f(x) \equiv 0 \bmod p$ has an integer solution.*

Proof. (1) Note that for the complex conjugation τ on K,

$$[L : L^\tau] = 2, \quad L = KL^\tau.$$

Hence $L^\tau = \mathbb{Q}(\alpha)$ for some algebraic integer α. Note that $\tau(\alpha) = \alpha$, which implies $\alpha \in \mathbb{R}$.

(2) We already know p splits completely in K if and only if $\left(\frac{d_K}{p}\right) = 1$. If so, we say $p\mathcal{O}_K = \mathfrak{p} \cdot \overline{\mathfrak{p}}$. Moreover, p splits completely in L if and only if $\mathfrak{p}$ splits completely in L. Since $L = K(\alpha)$, we see $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$. Also, f is the monic minimal polynomial of α over K. We obtain

$$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z} \implies \overline{f} \in (\mathcal{O}_K/\mathfrak{p})[x] \simeq (\mathbb{Z}/p\mathbb{Z})[x].$$

By assumption $p \nmid \operatorname{disc} f$. Hence $\mathfrak{p} \nmid \operatorname{disc} f$ as well. Therefore, $\mathfrak{p}$ splits completely in L if and only if $\overline{f}$ splits completely in $\mathbb{F}_p[x]$; equivalently, $f \equiv 0 \bmod p$ has an integer solution.

□

Theorem 11. *Let K be an imaginary quadratic field. We have the ideal class group*

$$\mathrm{Cl}(\mathcal{O}_K) = C(\mathcal{O}_K) := I_K/P_K \simeq \mathrm{Gal}(K^{\mathrm{Hilb}}/K).$$

Moreover, let $C(d_K)$ be the class group for primitive positive definite forms of discriminant d_K. Then

$$C(\mathcal{O}_K) \simeq C(d_K).$$

The theorem above shows the coincidence of the classifications for ppdfs with discriminant d_K and fractional ideals in $\mathcal{O}_K$.

Theorem 12 (Primes of the form $p = x^2 + ny^2$)**.** *Fix a square-free integer $n > 0$ satisfying $n \not\equiv 3 \bmod 4$. Then there is a monic irreducible $f_n \in \mathbb{Z}[x]$ of degree $h(-4n) = [K^{\mathrm{Hilb}} : K]$ such that if p is an odd prime, with $p \nmid n \cdot \mathrm{disc}(f_n)$, then $p = x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$ and $f_n(x) \equiv 0 \bmod p$ has an integer solution.*

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