BASIC NUMBER THEORY: LECTURE 8

WENHAN DAI

Recap. Let L/K be a finite extension of number fields. Then $\mathcal{O}_L/\mathcal{O}_K$ is not necessarily free as a quotient of $\mathbb{Z}$-modules. However, if p is a prime of $\mathbb{Q}$, then $(\mathcal{O}_L/p\mathcal{O}_L)/(\mathcal{O}_K/p\mathcal{O}_K)$ is a vector space of dimension $d = [L : K]$. Moreover, recall that $\mathcal{O}_K$ is a Dedekind domain. Consequently, for any prime $\mathfrak{p}$ of $\mathcal{O}_K$, the localization $\mathcal{O}_{K,\mathfrak{p}}$ is a discrete valuation ring. Hence $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathcal{O}_{K,\mathfrak{p}}$ of rank d. Consequently,

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} L = K, \quad \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}, \quad \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L.^1$$

While assuming L/K is a finite Galois extension and $\mathfrak{p}$ is prime in $\mathcal{O}_K$, $\mathrm{Gal}(L/K)$ acts transitively on the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_g\}$.

1. Discriminant

Let $[K : \mathbb{Q}] = d$. Then $e_1, \ldots, e_d$ is a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Define the determinant of $K/\mathbb{Q}$ by

$$\Delta_{K/\mathbb{Q}} := \det((\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j))_{i,j}),$$

where the matrix $(\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j))_{i,j}$ is positive definite, i.e. there is $B = (\alpha_j(e_i))_{i,j}$ such that $(\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j))_{i,j} = BB^T$, where $\alpha_i : K \hookrightarrow \mathbb{C}$ for $1 \leqslant i \leqslant d$. The determinant is well-defined, i.e. $\Delta_{K/\mathbb{Q}}$ is independent of the choice of the basis.

A prime number $p \in \mathbb{Q}$ is *ramified* in K if the ramified index $e(\mathfrak{p} \mid p) > 1$ for some prime ideal $\mathfrak{p}$ lying above p.

Theorem 1. *Let p be a prime number. Then p ramifies in K if and only if $p \mid \Delta_{K/\mathbb{Q}}$.*

Proof. Recall that if the trace pairing is nondegenerate, then it corresponds to a separable field extension. More explicitly, let E/F be a finite field extension and $e_1, \ldots, e_d$ is a basis of E over F. Define the discriminant of this basis via

$$\mathrm{disc}_{E/F}(e_1, \ldots, e_d) := \det(\mathrm{Tr}_{E/F}(e_i e_j)).$$

If $F[x]/(x^m) = E$, then $m > 1$ if and only if $\mathrm{disc}_{E/F}(e_1, \ldots, e_d) = 0$.

Assume ad hoc that $p\mathcal{O}_K = \prod_{l=1}^{g} \mathfrak{q}_l^{s_l}$, so

$$\mathcal{O}_K/p\mathcal{O}_K = \bigoplus_{l=1}^{g} \mathcal{O}_K/\mathfrak{q}_l^{s_l}.$$

Date: October 27, 2020.

[1]This is due to the following fact in commutative algebra. Let S be a multiplicative subset in a commutative ring R. Denote R_S the localization with respect to S. Then the prime ideals in R_S are in a one-to-one correspondence with the prime ideals that are disjoint with S.

It turns out that the complex conjugation

$$\overline{\Delta_{K/\mathbb{Q}}} = \prod_{l=1}^{g} \mathrm{disc}_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p}(e_1, \dots, e_d).$$

And the result follows from the equality. □

Example 2. Consider a quadratic field $K = \mathbb{Q}(\sqrt{N})$, where N is square-free. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}(\sqrt{N}), & N \not\equiv 1 \bmod 4; \\ \mathbb{Z}(\frac{1+\sqrt{N}}{2}), & N \equiv 1 \bmod 4. \end{cases}$$

The generators in both cases have minimal polynomials $x^2 - N$ with discriminant $4N$ and $x^2 - x - \frac{N-1}{4}$ with discriminant N, respectively.

After choosing a square root of N in K, we take

$$\alpha = a + b\sqrt{N}, \quad \alpha' = a - b\sqrt{N}, \quad a, b \in \mathbb{Q}.$$

Then the minimal polynomial of α (or α') is read as $f(x) = x^2 - 2xa + a^2 - Nb^2$. Thus,

$$2a \in \mathbb{Z},\ a^2 - Nb^2 \in \mathbb{Z} \iff \alpha \in \mathcal{O}_K.$$

In this case, if $a \in \mathbb{Z}$ then $b \in \mathbb{Z}$; otherwise, if $a \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$, then so also does b and $N \equiv 1 \bmod 4$. It turns out that

$$d_K := \Delta_{K/\mathbb{Q}} = \begin{cases} 4N & N \not\equiv 1 \bmod 4, \\ N & N \equiv 1 \bmod 4. \end{cases}$$

Exercise 3. Resume the above notation as in Example 2. Let f be the monic minimal polynomial of α that splits completely in the separable closure of $\mathbb{Q}$ as

$$f = (x - \alpha_1) \cdots (x - \alpha_d), \quad \alpha = \alpha_1.$$

Assume $\mathcal{O}_K = \mathbb{Z}[\alpha] = \bigoplus_{i=0}^{d-1} \mathbb{Z}\alpha^i$. Denote $B = (\alpha_j^{i-1})$. Show that

$$\Delta_{K/\mathbb{Q}} = (\det B)^2 = \mathrm{disc}\, f.$$

2. Primes in quadratic reciprocity

Definition 4. Let $D \equiv 0, 1 \bmod 4$. The *Kronecker symbol* for D is defined as

$$\left(\frac{D}{2}\right) = \begin{cases} 0 & D \equiv 0 \bmod 4, \\ 1 & D \equiv 1 \bmod 8, \\ -1 & D \equiv 5 \bmod 8. \end{cases}$$

Proposition 5. *Let K be a quadratic field of discriminant d_K. Suppose* $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \alpha\}$. *Let p be a prime number of $\mathbb{Z}$. Then:*

(1) $\left(\frac{d_K}{p}\right) = 0 \iff p\mathcal{O}_K = \mathfrak{p}^2$ *for some* $\mathfrak{p}$.
(2) $\left(\frac{d_K}{p}\right) = 1 \iff p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, *where* $\alpha(\mathfrak{p}_1) = \mathfrak{p}_2$ *and* $\alpha(\mathfrak{p}_2) = \mathfrak{p}_1$.
(3) $\left(\frac{d_K}{p}\right) = -1 \iff p\mathcal{O}_K$ *is inert, i.e.* $p\mathcal{O}_K$ *is still a prime in* K.

Proof. Case (1) is clear by Theorem 1, since p divides d_K and ramifies in $\mathcal{O}_K$. We deal with (2)(3). Let f be an irreducible polynomial over $\mathcal{O}_K$. Denote L the splitting field of f. Then

$$\mathcal{O}_L \simeq \mathcal{O}_K[x]/(f(x)), \quad \mathcal{O}_L/p\mathcal{O}_L \simeq (\mathcal{O}_K/p\mathcal{O}_K)[x]/(\overline{f}(x)).$$

Suppose that $\overline{f}(x) = \prod_{i=1}^{g} \overline{f_i}(x)^{e_i}$. Let $\mathfrak{q}_i$ be the corresponding prime ideal in $\mathcal{O}_L$ of $\overline{f_i}$. Hence

$$p\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}.$$

If $\overline{\beta_i}$ is a root of $\overline{f_i}$, then $\mathfrak{q}_i = (f_i, \beta_i)$. In the case when K is a quadratic field,

$$f(x) = \begin{cases} x^2 - N & N \not\equiv 1 \bmod 4, \\ x^2 - x - \frac{N-1}{4} & N \equiv 1 \bmod 4. \end{cases}$$

For (2)(3), p is an odd prime, and f splits in $\mathbb{F}_p$ if and only if $\left(\frac{N}{p}\right) = \left(\frac{d_K}{p}\right) = 1$. The proposition follows from this. □

We briefly summarize the upshot of the proof. The first step is to kick out the ramified case by applying Theorem 1. As for the unramified case, the prime factorization of $p\mathcal{O}_K$ is very similar to the decomposition of the minimal polynomial.

Corollary 6 (cf. Theorem 1)**.** *Let K be a quadratic field of discriminant d_K, and let p be an integer prime. Then p ramifies in K if and only if p divides d_K. And p splits completely in K if and only if $\left(\frac{d_K}{p}\right) = 1$.*

3. Hilbert class field

In this section we assume K to be a number field.

Definition 7. (1) A *real* (resp. *complex*) *infinite prime* of K is a field embedding $\alpha : K \hookrightarrow \mathbb{R}$ (resp. a pair of field embedding $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$, where $\overline{\sigma}$ is the complex conjugate of σ).

(2) Let L/K be a finite extension. An infinite prime α of K is said to *ramify* in L if it is real and it extends to a complex infinite prime of L.

Example 8. Let $K/\mathbb{Q}$ be a quadratic extension. Then the infinite prime ∞ ramifies in K if and only if K is an imaginary quadratic field.

Theorem 9. *There is a finite Galois extension L/K such that*

(1) *L is unramified at finite and infinite primes and abelian (i.e. $\mathrm{Gal}(L/K)$ is an abelian group);*

(2) *any unramified abelian extension of K lies in L.*

Namely, L exists as the maximal unramified abelian extension of K.

Definition 10. The field L in Theorem 9 is called the *Hilbert class field* of K, denoted as $L = K^{\mathrm{Hilb}}$.

Now we introduce new setups. Let L/K be a finite Galois extension. Fix a prime (ideal) $\mathfrak{p}$ of $\mathcal{O}_K$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ lying above p.

Definition 11. The *decomposition group* of $\mathfrak{q}$ is

$$D_{\mathfrak{q}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

The *inertia group* of $\mathfrak{q}$ is

$$I_{\mathfrak{q}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \forall \alpha \in \mathcal{O}_L,\ \sigma(\alpha) \equiv \alpha \bmod \mathfrak{q}\}.$$

Also denote

$$\widetilde{G} := \mathrm{Gal}((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_L/\mathfrak{p})).$$

Observe that $I_{\mathfrak{q}} \subseteq \ker(D_{\mathfrak{q}} \to \widetilde{G})$. Moreover,

Proposition 12. *We obtain*

$$D_{\mathfrak{q}}/I_{\mathfrak{q}} \simeq \widetilde{G},$$

and the orders are given by

$$|D_{\mathfrak{q}}| = ef, \quad |I_{\mathfrak{q}}| = e, \quad |\widetilde{G}| = f.$$

Lemma 13. *Let L/K be a finite Galois extension. Suppose $\mathfrak{p} \subseteq \mathcal{O}_K$ is an unramified prime in L and $\mathfrak{q}$ is a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then there exists a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{q}$ for all $\alpha \in \mathcal{O}_L$.*

Proof. Since $\mathfrak{p}$ is unramified, $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_{N(\mathfrak{p})^e} = \mathbb{F}_{N(\mathfrak{p})}$, and

$$D_{\mathfrak{q}} \simeq \widetilde{G} \simeq \mathrm{Gal}((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})).$$

□

Definition 14. The Artin symbol of a prime $\mathfrak{q}$ of L relative to K is defined as

$$\left(\frac{L/K}{\mathfrak{q}}\right) := \sigma,$$

where σ is as in Lemma 13 above.

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