BASIC NUMBER THEORY: LECTURE 7

WENHAN DAI

1. Proof of the cubic reciprocity (continued)

We resume on referring to the textbook [IR82] by Ireland and Rosen.[1]

Proposition 1 ([Prop 8.3.4, IR82]). *Let $p \equiv 1 \bmod 3$ be a prime and χ be a cubic character, i.e. $\chi^3 = \epsilon$. Assume $J(\chi, \chi) = a + b\omega$, then*

$$b \equiv 0 \bmod 3, \quad a \equiv -1 \bmod 3.$$

Proof. By taking $n = 3$ in Proposition 8 of Lecture 6,

$$g(\chi)^3 = pJ(\chi, \chi) = p(a + b\omega).$$

Since $p \equiv 1 \bmod 3$,

$$a + b\omega \equiv g(\chi)^3 \equiv \sum_{t \in \mathbb{F}_p^\times} \chi(t)^3 \zeta^{3t} = \sum_{t \in \mathbb{F}_p^\times} \zeta^{3t} = -1 \bmod 3.$$

Similarly, $a + b\overline{\omega} \equiv g(\overline{\chi})^3 \equiv -1 \bmod 3$. Then $a \equiv -1 \bmod 3$ and $b \equiv 0 \bmod 3$. □

For a prime $\pi \in \mathbb{Z}[\omega]$, define (with $p = N(\pi)$) that

$$\chi_\pi = \left(\frac{\cdot}{\pi}\right)_3 : \mathbb{F}_p^\times \to \{1, \omega, \omega^2\} \subseteq \mathbb{C}^\times.$$

Lemma 2. *For any prime $\pi \in \mathbb{Z}[\omega]$,*

$$J(\chi_\pi, \chi_\pi) = \pi.$$

Proof. Apply Proposition 6 of Lecture 6 to get $J(\chi_\pi, \chi_\pi) = \sqrt{p}$. By Proposition 1, $J(\chi_\pi, \chi_\pi)$ is primary. As $p = \pi\overline{\pi}$, one must choose a square root of p. Hence $J(\chi_\pi, \chi_\pi) = \pi$ or $\overline{\pi}$. On the other hand,

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &= \sum_{t \in \mathbb{F}_p^\times} \chi_\pi(t)\chi_\pi(1-t) \\ &\equiv \sum_{x \in \mathbb{F}_p} x^{\frac{p-1}{3}} (1-x)^{\frac{p-1}{3}} \equiv 0 \bmod \pi. \end{aligned}$$

This forces $J(\chi_\pi, \chi_\pi)$ to equal π. □

Using the character theory, the cubic reciprocity can be computed explicitly.

Theorem 3 (Reformulated cubic reciprocity). *Let $q \equiv 2 \bmod 3$ be a rational prime. Take another prime $\pi \in \mathbb{Z}[\omega]$. Then*

$$\chi_q(\pi) = \chi_\pi(q).$$

Date: October 23, 2020.

[1] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, Berlin, Heidelberg, and New York, 1982.

Proof. A priori we have $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi) = p\pi$ due to Lemma 2, for some $p \equiv 1 \bmod 3$. Recall that for $q \equiv 2 \bmod 3$, it keeps inert in $\mathbb{Z}[\omega]$, and the diagram commutes:

$$\begin{tikzcd} \mathbb{Z}/q\mathbb{Z} \arrow[r, hook] \arrow[d, "\sim"'] & \mathbb{Z}[\omega]/q\mathbb{Z}[\omega] \arrow[d, "\sim"] \\ \mathbb{F}_q \arrow[r, hook] & \mathbb{F}_{q^2}. \end{tikzcd}$$

It is natural to consider the power q^2-1, say

$$g(\chi_\pi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}} \equiv \chi_q(p\pi) \bmod q.$$

As $3 \mid N(q)-1$, we obtain $\chi_q(p) = 1$. Thus,

$$\chi_q(p\pi) = \chi_q(p)\chi_q(\pi) = \chi_q(\pi).$$

Also,

$$\begin{aligned} g(\chi_\pi)^{q^2} &= \left(\sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta^t\right)^{q^2} \\ &\equiv \sum_{t\in\mathbb{F}_p} \chi_\pi(t)^{q^2}\zeta^{q^2 t} \bmod q \\ &= \sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta^{q^2 t} = g_{q^2}(\chi_\pi). \end{aligned}$$

Furthermore, $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Then

$$\chi_\pi(q) = g(\chi_\pi)^{q^2-1} \equiv \chi_q(\pi) \bmod q.$$

This is sufficient to show that $\chi_\pi(q) = \chi_q(\pi)$. Hence the cubic reciprocity holds. $\square$

2. Story on number fields

Recall that a *number field* K is a finite extension of $\mathbb{Q}$. Denote $d = [K:\mathbb{Q}]$ the degree of K. Note that $K/\mathbb{Q}$ is always separable yet not necessarily Galois. (This is essentially because $\mathbb{Q}$ is a perfect field.)

Definition 4. The *ring of integers of* K, denoted by $\mathcal{O}_K$, is the integral closure of $\mathbb{Z}$ in K; equivalently, it consists of the elements of K whose minimal polynomial is monic and lies in $\mathbb{Z}[X]$.

Proposition 5. (1) *$\mathcal{O}_K$ is a subring of K such that* $\operatorname{Frac}(\mathcal{O}_K) = K$.
(2) *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank d.*

Proof. (1) is apparent by definition. We prove (2) as follows. Since $K/\mathbb{Q}$ is separable, there is a non-degenerate trace pairing

$$\begin{aligned} \operatorname{Tr}: K\times K &\longrightarrow \mathbb{Q} \\ (a,b) &\longmapsto \operatorname{Tr}_{K/\mathbb{Q}}(ab). \end{aligned}$$

Choose a basis $e_1,\ldots,e_d$ of $K/\mathbb{Q}$. With respect to this (perfect) trace pairing, one can take the dual basis $e_1^*,\ldots,e_d^*$. Fix a sufficiently divisible integer n such that $\{ne_1,\ldots,ne_d\} \subseteq \mathcal{O}_K$ and replace $e_1,\ldots,e_d$ by $ne_1,\ldots,ne_d$. Correspondingly, the dual basis is also replaced with

$n^{-1}e_1^*, \dots, n^{-1}e_d^*$. Thanks to this argument, one may assume without loss of generality that $e_i \in \mathcal{O}_K$ for all i. Then

$$\bigoplus_{i=1}^{d} \mathbb{Z}e_i \subseteq \mathcal{O}_K.$$

Conversely, for each $a \in \mathcal{O}_K$, there is another $\mathbb{Q}$-linear combination with respect to the dual basis: $a = \sum_{i=1}^{d} a_i e_i^*$ for $a_i \in \mathbb{Q}$. Then $\mathrm{Tr}(a, e_j) = \mathrm{Tr}_{K/\mathbb{Q}}(ae_j) = a_j \in \mathbb{Z}$ by definition of the trace. Hence

$$\bigoplus_{i=1}^{d} \mathbb{Z}e_i \supseteq \mathcal{O}_K.$$

So $\mathcal{O}_K$ is a free abelian group, namely a free $\mathbb{Z}$-module, of rank d. □

Definition 6. A ring R is a *Dedekind domain* if

(1) R is a noetherian domain,
(2) R is integrally closed, and
(3) every nonzero prime ideal of R is maximal.[2]

The following theorems explain the motivation to introduce the definition of Dedekind domains. A priori the unique decomposition of elements into primes as that in $\mathbb{Z}$ cannot be generalized to a similar statement for free $\mathbb{Z}$-modules of finite rank. Hence we only require the unique decomposition to hold for prime ideals in $\mathcal{O}_K$.

Theorem 7. *If R is a Dedekind domain, then every nonzero ideal $\mathfrak{a} \subseteq R$ can be written as $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are prime ideals and the decomposition is unique up to order.*

Theorem 8. *Let K be a number field. Then*

(1) *$\mathcal{O}_K$ is a Dedekind domain.*
(2) *For each nonzero prime ideal $\mathfrak{p}$, the quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite field.*

Proof. Recall that a finite integral domain is always a field. Also note that (2) implies (1). So it suffices to show that for any nonzero ideal I of $\mathcal{O}_K$, $|\mathcal{O}_K/I| < \infty$. Choose $0 \neq a \in I$ with its monic minimal polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ of $\mathbb{Q}$-coefficients. It turns out that $a_0 \in \mathbb{Z}$ for $a \in \mathcal{O}_K$.[3] And

$$a_0 = -(a^n + a_{n-1}a^{n-1} + \dots + a_1 a) \in I.$$

We deduce that $0 \neq a_0 \in I \cap \mathbb{Z}$. Hence $(a_0) \subseteq I$ and $|\mathcal{O}_K/(a_0)| < \infty$ (more precisely, there is a basis of $\mathcal{O}_K/(a_0)$ consisting of at most $n-2$ elements). In particular, $|\mathcal{O}_K/I| < \infty$. □

3. Ramification theory

Setup. Suppose L/K is a finite extension (again, not necessarily Galois) of number fields. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. By Theorem 7, $\mathfrak{p}$ admits a unique decomposition in L, written as $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$ with $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$, where $\mathfrak{q}_i$'s are mutually distinct prime ideals. Hence $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{q}_i$ is a finite extension of finite fields.

[2] In commutative algebra, this condition is written as $\operatorname{Krull\,dim} R = 1$.

[3] This is because a_0 equals the norm of a, which will be discussed later.

Definition 9. In the decomposition $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$ above, define $e_i = e(\mathfrak{q}_i|\mathfrak{p})$ to be the *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$. Also define $f_i = f(\mathfrak{q}_i|\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ to be the *inertia degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$.

Theorem 10. *We always obtain the relation*

$$\sum_{i=1}^{g} e_i f_i = d.$$

Proof. By assumption, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a free $\mathcal{O}_K/\mathfrak{p}$-module of rank d, and by the Chinese remainder theorem,

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \bigoplus_{i=1}^{g} \mathcal{O}_L/\mathfrak{q}_i^{e_i}\mathcal{O}_L, \quad \mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j} = \mathcal{O}_L \text{ for } i \neq j.$$

Thus,

$$|\mathcal{O}_L/\mathfrak{q}_i^{e_i}\mathcal{O}_L| = |\mathcal{O}_L/\mathfrak{q}_i\mathcal{O}_L|^{e_i} = |\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K|^{f_i e_i} = N(\mathfrak{p})^{f_i e_i}.$$

On the other hand,

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K|^d = N(\mathfrak{p})^d.$$

So the equality holds by comparison. ☐

Theorem 11. *Assume that L/K is finite Galois of degree d. Then*

(1) *The group* $\mathrm{Gal}(L/K)$ *acts on the set* $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_g\}$ *transitively.*

(2) *There are integers e, f such that*

$$e(\mathfrak{q}_i \mid \mathfrak{p}) = e, \quad f(\mathfrak{q}_i \mid \mathfrak{p}) = f, \quad i = 1, \ldots, g.$$

Moreover, by Theorem 10,

$$efg = d.$$

Proof. Note immediately that (2) is implied by (1). So we tackle with (1) only. Suppose the Galois action is not transitive. Then there exists $\mathfrak{q}_1, \mathfrak{q}_2$ such that for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{q}_1) \neq \mathfrak{q}_2$. Choose $a \in \mathfrak{q}_2 \setminus \bigcup_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{q}_1)$. Then

$$N_{L/K}(a) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(a) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma^{-1}(a) \notin \mathfrak{q}_1.$$

This forces $N_{L/K}(a) \in \mathfrak{q}_2$, contradicting with $N_{L/K}(a) \in \mathfrak{q}_2 \cap \mathcal{O}_K = \mathfrak{p} = \mathfrak{q}_1 \cap \mathcal{O}_K$. ☐

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