BASIC NUMBER THEORY: LECTURE 16

WENHAN DAI

1. Class field theory and reciprocity

We are to introduce the famous Kronecker-Weber theorem. Before this, recall the example for cyclotomic field $\mathbb{Q}(\zeta_n)$. We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

of order $\varphi(n)$. On the other hand, also recall that for the genus field M of $\mathbb{Q}$ we have $\mathrm{Gal}(M/\mathbb{Q}) \simeq \{\pm 1\}^\mu$. In fact, $\varphi(n)$ is a power of 2 if and only if $n = 2^k p_1 \cdots p_t$, where $p_1, \dots, p_t$ are distinct Fermat primes, i.e. $p_k = 2^{r_k} + 1$ for some integer $r_k \in \mathbb{N}$ for $k = 1, \dots, t$.[1] By definition we have the conductor $\mathfrak{m} = n\infty$ of $\mathbb{Q}(\zeta_n)$, and $\ker(\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q},\mathfrak{m}}) = P_{\mathbb{Q},1}(\mathfrak{m})$. It says that $\mathbb{Q}(\zeta_n)$ is the Hilbert class field of $\mathbb{Q}$. This phenomenon indicates the following big theorem.

Theorem 1 (Kronecker-Weber)**.** *$L/\mathbb{Q}$ is an abelian extension if and only if $L \subseteq \mathbb{Q}(\zeta_n)$ for some n.*

Proof. The "if" part is obvious as $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group, and hence its quotient groups are abelian as well. The "only if" part is due to the argument above: there is a modulus $\mathfrak{m} = n\infty$ such that $\ker(\Phi_{L/\mathbb{Q},\mathfrak{m}}) \supseteq P_{\mathbb{Q},1}(\mathfrak{m})$. Hence $L \subseteq \mathbb{Q}(\zeta_n)$. □

2. Higher reciprocity law

2.1. nth power of Legendre symbol.

Let K be a number field containing $\zeta_n = e^{2\pi i/n}$. Suppose $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal such that $\mathfrak{p} + n\mathcal{O}_K = \mathcal{O}_K$. Let $\alpha \in \mathcal{O}_K$ be an element such that $\alpha \notin \mathfrak{p}$.

Lemma 2. *We have $n \mid N(\mathfrak{p}) - 1$.*

Proof. As $\mathfrak{p}$ is coprime to n, $1, \zeta_n, \dots, \zeta_n^{n-1}$ are distinct modulo $\mathfrak{p}$. Note that $(\mathcal{O}_K/\mathfrak{p})^\times$ is cyclic of order $N(\mathfrak{p}) - 1$, and $\{1, \zeta_n, \dots, \zeta_n^{n-1}\}$ is a subgroup of order n. This proves $n \mid N(\mathfrak{p}) - 1$. □

By the lemma, we deduce

- Fermat's little theorem: $\alpha^{N(\mathfrak{p})-1} \equiv 1 \bmod \mathfrak{p}$ for $\alpha \in \mathcal{O}_K$ and $\alpha \notin \mathfrak{p}$.

Date: December 18, 2020.

[1] It turns out that the equilateral polygons with p edges, where p is a Fermat prime, can be drawn with ruler and compasses. Gauss had specified the case when $p = 17$. In fact,

$$\cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{\sqrt{17}}{6} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}},$$

which consists square roots only.

- Moreover, for some $0 \leqslant m \leqslant n-1$,
$$\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \zeta_n^m \bmod \mathfrak{p}.$$

Definition 3. Define the nth power of Legendre symbol by
$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n := \zeta_n^m$$
for α and m above. Let $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal prime to n and α. Then it admits a unique factorization $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ and
$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n := \prod_{i=1}^{r} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n^{n_i}.$$

Notation 4. By abuse of notation as before, we also denote
$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \longrightarrow \mu_n, \quad \mathfrak{p} \longmapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_n$$
as the nth power of Legendre symbol.

Previously, we have seen that for an odd prime q,
$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}, \quad [q] \longmapsto \left(\frac{p^*}{q}\right)_2$$
is constructed using the quadratic reciprocity. Conversely, if the character χ exists, and $\chi' : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ is another nontrivial character, then $\chi = \chi'$. This observation can be summarized as that

- the quadratic reciprocity law is equivalent to the existence of $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$.

Using this philosophy, we can construct:

Theorem 5 (Weak reciprocity). *For $0 \neq \alpha \in \mathcal{O}_K$, let $L = K(\sqrt[n]{\alpha})$. Then we obtain a natural (injective) group homomorphism*
$$\mathrm{Gal}(L/K) \longrightarrow \mu_n, \quad \sigma \longmapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}.$$
Assume $\mathfrak{m}$ is a modulus divisible by all primes containing $n\alpha$, and assume $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup. Then the diagram commutes:
$$\begin{tikzcd} I_K(\mathfrak{m}) \arrow[r, "\Phi_{L/K,\mathfrak{m}}"] \arrow[dr, "\left(\frac{\alpha}{\cdot}\right)_n"'] & \mathrm{Gal}(L/K) \arrow[d, hook] \\ & \mu_n. \end{tikzcd}$$

Proof. Fix an arbitrary $\mathfrak{p} \in I_K(\mathfrak{m})$. Then
$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) \equiv (\sqrt[n]{\alpha})^{N(\mathfrak{p})} \equiv (\alpha^{\frac{N(\mathfrak{p})-1}{n}}) \cdot \sqrt[n]{\alpha} \bmod \mathfrak{p}.$$
On the other hand,
$$\frac{\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{p}.$$
So the diagram commutes. $\square$

Theorem 6 (Quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Proof. It suffices to show the existence of character χ. By Hilbert class field theory we have the tower

$$\begin{tikzcd}
\mathbb{Q}(\mu_p) \arrow[d, dash, "(\mathbb{Z}/p\mathbb{Z})^\times"'] \\
K \arrow[d, dash, "\{\pm 1\}"] \\
\mathbb{Q}
\end{tikzcd}$$

Given the fact that p is the only finite prime ramifies in $\mathbb{Q}(\mu_p)$, we see p is the only finite prime ramifies in K. This shows that $2 \nmid d_K$, and $K = \mathbb{Q}(\sqrt{p^*})$. Consider the modulus (in fact the conductor) $\mathfrak{m} = p\infty$ of $\mathbb{Q}(\mu_p)$. The post-composite of Artin reciprocity map $\Phi_{\mathbb{Q}(\mu_p)/\mathbb{Q},p\infty}$ gives a natural quotient

$$\begin{array}{rcl}
I_{\mathbb{Q}}(p\infty) \xrightarrow{\Phi_{\mathbb{Q}(\mu_p)/\mathbb{Q},p\infty}} \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) & \xrightarrow{\simeq} & (\mathbb{Z}/p\mathbb{Z})^\times \\
q \longmapsto & & [q].
\end{array}$$

Now take $\alpha = p^*$ in the definition of Legendre symbol, we have a commutative diagram

$$\begin{tikzcd}
I_{\mathbb{Q}}(p\infty) \arrow[r, "\Phi_{p\infty}"] \arrow[ddr, "\left(\frac{p^*}{\cdot}\right)_2"'] & \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \arrow[r, "\simeq"] \arrow[d] & (\mathbb{Z}/p\mathbb{Z})^\times \\
& \mathrm{Gal}(K/\mathbb{Q}) \arrow[d] & \\
& \{\pm 1\} &
\end{tikzcd}$$

We check that for any prime ideal $\mathfrak{P} \mid q$ in $\mathcal{O}_{\mathbb{Q}(\mu_p)}$,

$$\left(\frac{\mathbb{Q}(\mu_p)/\mathbb{Q}}{q}\right)(\zeta_p) \equiv \zeta_p^q \bmod \mathfrak{P},$$

thus,

$$\left(\frac{\mathbb{Q}(\mu_p)/\mathbb{Q}}{q}\right)(\zeta_p) = \zeta_p^q.$$

This gives rise to the desired quadratic character

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}, \quad [q] \longmapsto \left(\frac{p^*}{q}\right)_2.$$

Hence we have proved quadratic reciprocity. $\square$

2.2. **Hilbert class field.** If $\mathfrak{m} = 1$ then $P_{K,1}(\mathfrak{m}) = P_K$ and $I_K(\mathfrak{m}) = I_K$. By the existence theorem, there is an abelian extension L/K corresponding to the congruence subgroup $P_K \subseteq I_K$.

Theorem 7. *The abelian extension L/K corresponding to the congruence subgroup $P_K \subseteq I_K$ is the Hilbert class field of K.*

Proof. Since we have taken $\mathfrak{m} = 1$, L/K must be everywhere unramified. Conversely, let L'/K be abelian and unramified. Then we can choose $\mathfrak{m} = 1$, and by Artin reciprocity (i.e. the uniqueness theorem),

$$\Phi_{L'/K,1} : I_K \longrightarrow \mathrm{Gal}(L'/K)$$

is surjective. So P_K is contained in $\ker \Phi_{L'/K,1}$. Hence $L' \subseteq L$, i.e. L is the maximal extension. $\square$

3. Čebotarev density theorem

In this section we will see a phenomenon of local-global compatibility. Let K be a number field. Let P_K be the set of all finite primes of K. Given $S \subseteq P_K$ finite or infinite, define the *Dirichlet density*

$$\delta(S) := \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{-\log(s-1)}.$$

It enjoys some basic properties as one may expected, such as

(1) $\delta(P_K) = 1$, and
(2) if S is finite then $\delta(S) = 0$.

For example, one may assume $K = \mathbb{Q}$ to check (1), by noting that $\zeta(s)$ absolutely converges on $\Re(s) > 1$ and has a single pole at $s = 1$.

Theorem 8 (Čebotarev density theorem)**.** *Let L/K be a Galois extension.*[2] *Let $\sigma \in \mathrm{Gal}(L/K)$ as well as its conjugacy class $\langle \sigma \rangle$. Define*

$$S_\sigma = \left\{ \mathfrak{p} \in P_K \mid \mathfrak{p} \textit{ is unramified in } L \textit{ and } \left(\frac{L/K}{\mathfrak{p}} \right) = \langle \sigma \rangle \right\}.$$

Then

$$\delta(S_\sigma) = \frac{|\langle \sigma \rangle|}{|\mathrm{Gal}(L/K)|} = \frac{|\langle \sigma \rangle|}{[L:K]}.$$

Corollary 9. *Let L/K be an abelian extension with $\sigma \in \mathrm{Gal}(L/K)$. Then*

$$\left\{ \mathfrak{p} \in P_K \mid \left(\frac{L/K}{\mathfrak{p}} \right) = \sigma \right\}$$

has density $1/[L:K]$. In particular, the sets of this form are infinite sets.

Example 10. Let $\sigma \in Gal(L/K)$ be a unit. Then

$$\left(\frac{L/K}{\mathfrak{p}} \right) = \sigma \iff \mathfrak{p} \text{ splits completelt.}$$

Notation 11. (1) We set-theoretically denote $S \dot{\subseteq} T$ if $S \subseteq T \cup \Sigma$ for some finite set Σ. Denote $S \doteq T$ if $S \dot{\subseteq} T$ and $S \dot{\supseteq} T$.

[2] A priori this should be finite. However the theorem hopefully holds for infinite extensions.

(2) Let L/K be a finite extension. Denote

$$S_{L/K} = \{\text{primes splits completely in } L\}$$

and

$$\widetilde{S}_{L/K} = \{\mathfrak{p} \text{ unramified in } L \mid f_{\mathfrak{P}|\mathfrak{p}} = 1 \text{ for at least one } \mathfrak{P} \mid \mathfrak{p}\}.$$

Note that $S_{L/K} \subseteq \widetilde{S}_{L/K}$, and they are equal if L/K is Galois.

Theorem 12. *Let L, M be Galois extensions over K. Then*

(1) $L \subseteq M$ *if and only if* $S_{M/K} \dot{\subseteq} S_{L/K}$.
(2) $L = M$ *if and only if* $S_{M/K} \doteq S_{L/K}$.

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