BASIC NUMBER THEORY: LECTURE 17

WENHAN DAI

1. Čebotarev density theorem (continued)

We resume on the last theorem in Lecture 16.

Theorem 1. *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 $S_{M/K} \doteq S_{L/K}$.*

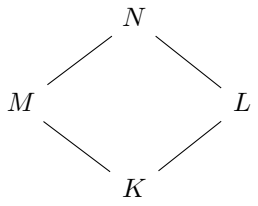
Recall the notation that $\widetilde{S}_{M/K} = \{\mathfrak{p} \text{ unramified in } M \mid f_{\mathfrak{P}|\mathfrak{p}} = 1 \text{ for at least one } \mathfrak{P} \mid \mathfrak{p}\}$ if M is a finite extension of K. The following Proposition 2 implies Theorem 1.

Proposition 2. *Let L, M be finite extensions over K.*

(1) *If M is Galois, then $L \subseteq M$ if and only if $S_{M/K} \dot{\subseteq} S_{L/K}$;*
(2) *If L is Galois, then $L \subseteq M$ if and only if $\widetilde{S}_{M/K} \dot{\subseteq} S_{L/K}$.*

Proof. We first prove (2). Assume $L \subseteq M$. For each $\mathfrak{p} \in \widetilde{S}_{M/K}$, $f_{\mathfrak{P}|\mathfrak{p}} = 1$ for some $\mathfrak{P}$ lying above $\mathfrak{p}$. Let M/K be Galois. Then all inertia degrees of primes in M above $\mathfrak{p}$ are 1. Hence $\mathfrak{p}$ splits completely. Consider prime ideals $\mathfrak{P} \subseteq \mathcal{O}_N$, $\mathfrak{P}' \subseteq \mathcal{O}_M$, and $\mathfrak{p} \subseteq \mathcal{O}_K$.

Conversely we assume $\widetilde{S}_{M/K} \dot{\subseteq} S_{L/K}$. Let N be the Galois closure of LM over K.



Choose $\sigma \in \mathrm{Gal}(N/M)$. By Čebotarev density theorem, there are infinitely many primes $\mathfrak{p}$ such that $\left(\frac{N/K}{\mathfrak{p}}\right) = \langle\sigma\rangle$. So

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}, \quad \forall x \in \mathcal{O}_N.$$

Consequently, for all $x \in \mathcal{O}_M$,

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}', \quad 1 \equiv x^{N(\mathfrak{p})-1} \bmod \mathfrak{P}'.$$

It follows that $f_{\mathfrak{P}'|\mathfrak{p}} = 1$ and $\mathfrak{p} \in \widetilde{S}_{M/K}$. So $\mathfrak{p} \in S_{L/K}$, and $\mathfrak{p}$ splits completely in L. Therefore,

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \sigma|_L = 1, \quad \langle\sigma\rangle = \left(\frac{N/K}{\mathfrak{p}}\right).$$

We infer that for any $\sigma|_L = 1$, and L is invariant under $\mathrm{Gal}(N/M)$. Hence $L \subseteq M$.

Date: December 22, 2020.

For (1), the "only if" part is obvious. We do the "if" part. Let L' be the Galois closure of L. (So $L \subseteq M$ if and only if $L' \subseteq M$.) We have $\mathfrak{p}$ of K splits completely in L if and only if $\mathfrak{p}$ splits completely in L'. This shows the equality $S_{L/K} = S_{L'/K}$. Since M is Galois, we have $\widetilde{S}_{M/K} = S_{M/K}$ by definition. By (2),

$$\widetilde{S}_{M/K} \dot{\subseteq} S_{L'/K} \iff L' \subseteq M \iff L \subseteq M.$$

□

2. Ring class field and $p = x^2 + ny^2$

We are to construct the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$.

Let K be an imaginary quadratic field. Fix $\mathcal{O} \subseteq \mathcal{O}_K$ an order of conductor f. By the existence theorem of global class field theory, there is a unique abelian extension L/K such that the ramified primes dividing f with $\ker(\Phi_{L/K,f}) = P_{K,\mathbb{Z}}(f)$. Then

$$\mathrm{Gal}(L/K) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \simeq C(\mathcal{O}).$$

Theorem 3. *Let n be a positive integer. Then there exists $f_n \in \mathbb{Z}[x]$ monic and irreducible of degree $h(-4n)$ such that if $p \nmid n$ and $p \nmid \mathrm{disc}(f_n)$, 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.*

Moreover, $f_n(x)$ in the main theorem may be taken to be the minimal polynomial of α for which α is a real algebraic integer and $L = K(\alpha)$. By taking

$$\mathcal{O} = [1, \frac{D + \sqrt{D}}{2}], \quad D = -4n,$$

we have $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. One can let $K = \mathbb{Q}(\sqrt{-n})$. Then L is constructed as the ring class field of order $\mathbb{Z}[\sqrt{-n}]$. Conversely, if $f_n(x) \in \mathbb{Z}[x]$ is monic of degree $h(-4n)$, satisfies the condition in Theorem 3, then f_n has to be the minimal polynomial of some positive element of L/K.

$$\begin{array}{c} L \\ {\scriptstyle C(\mathcal{O})}\big(\big| \\ K \\ \big| \\ \mathbb{Q} \end{array}$$

Lemma 4. *Let L be the ring class field of order $\mathcal{O}$. Then $L/\mathbb{Q}$ is a Galois extension and*

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

Here the semi-direct product relation is given by

$$\forall \sigma \in \mathrm{Gal}(L/K), \quad \tau(\sigma) = \sigma^{-1},$$

where τ is the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. We claim that for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with $\mathfrak{P} \mid \mathfrak{p}$ in $\mathcal{O}_L$ above,

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

To prove this, we note that $N(\mathfrak{p}) = N(\tau(\mathfrak{p}))$, and

$$\left(\tau\left(\frac{L/K}{\mathfrak{p}}\right)\tau^{-1}\right)(\tau(x)) \equiv \tau(x)^{N(\mathfrak{p})} \bmod \tau(\mathfrak{P}).$$

Hence

$$\tau\left(\frac{L/K}{\mathfrak{p}}\right)\tau^{-1} = \left(\frac{\tau(L)/K}{\tau(\mathfrak{p})}\right) \in \mathrm{Gal}(L/K) \cap \mathrm{Gal}(\tau(L)/K).$$

Granting the claim now, we see the following diagram commutes:

$$\begin{array}{ccc} L & \xrightarrow{\sim} & \tau(L) \\ \uparrow & & \uparrow \\ I_{K,\mathfrak{m}} & \xrightarrow{\sim} & I_{K,\tau(\mathfrak{m})}. \end{array}$$

In this diagram, we set the modulus $\mathfrak{m} = (f)$; the top horizontal map is simply $x \mapsto \tau(x)$, and the bottom horizontal map is $[\mathfrak{p}] \mapsto [\tau(\mathfrak{p})]$ induced by τ. We infer that

$$P_{K,\mathbb{Z}}(f) = \tau(P_{K,\mathbb{Z}}(f)) = \tau(\ker(\Phi_{L/K,\mathfrak{m}})) = \ker(\Phi_{\tau(L)/K,\mathfrak{m}}).$$

So

$$\ker(\Phi_{L/K,\mathfrak{m}}) = \ker(\Phi_{\tau(L)/K,\mathfrak{m}}).$$

This proves $L = \tau(L)$, namely $L/\mathbb{Q}$ is Galois. Also,

$$\tau\left(\frac{L/K}{\mathfrak{p}}\right)\tau^{-1} = \left(\frac{L/K}{\tau(\mathfrak{p})}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)^{-1}, \quad \tau(\mathfrak{p})\mathfrak{p} = \overline{\mathfrak{p}}\mathfrak{p} = N(\mathfrak{p}).$$

□

Theorem 5. *Set L the ring class field of $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. Let f be the conductor of $\mathcal{O}$. Then for $(p, n) = 1$, $p = x^2 + ny^2$ if and only if p splits completely in L.*

Proof. Recall that $P(\mathcal{O}, f) \cong P_{K,\mathbb{Z}}(f)$. We obtain

$$\begin{aligned} p = x^2 + ny^2 &\iff p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \in P(\mathcal{O}, f) \\ &\iff p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\ &\iff p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \text{ splits completely in } L. \end{aligned}$$

The second last equality is due to the class field theory. □

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