BASIC NUMBER THEORY: LECTURE 14

WENHAN DAI

1. Orders in imaginary quadratic field (continued)

Let K be an imaginary quadratic field. We resume on Theorem 14 of Lecture 13 last time.

Theorem 1. *Fix an order $\mathcal{O}$ of discriminant $D = \Delta_{\mathcal{O}/\mathbb{Z}} < 0$. Then*

(1) *If $f(x,y) = ax^2 + bxy + cy^2$ is a ppdf of discriminant D, then*
$$[a, \frac{-b+\sqrt{D}}{2}] \subseteq \mathcal{O}$$
is a proper ideal of $\mathcal{O}$.

(2) *Resuming on (1), the map*
$$f(x,y) \longmapsto [a, \frac{-b+\sqrt{D}}{2}]$$
induces an isomorphism $C(D) \simeq C(\mathcal{O})$. In particular, $h(\mathcal{O}) = h(D)$.

(3) *A positive integer m is represented by a ppdf $f(x,y)$ of discriminant D if and only if $m = N(\alpha)$ for some proper $\mathcal{O}$-ideal $\mathfrak{a}$ corresponding to $f(x,y)$ via the isomorphism $C(D) \simeq C(\mathcal{O})$ in (2).*

We have finished the proof of (1)(2) last time.

Remark 2. There was a small gap in our proof of Theorem 1(2) last time, and we left it to the reader to fill. That is, it remains to show that $f(x,y) \longmapsto [a, \frac{-b+\sqrt{D}}{2}]$ is a homomorphism.

Given two ppdfs $f(x,y) = ax^2+bxy+cy^2$ and $g(x,y) = a'x^2+b'xy+c'y^2$ of discriminant D with $(a', a, (b+b')/2) = 1$, there is an integer B such that
$$B \equiv b \bmod 2a, \quad B \equiv b' \bmod 2a', \quad B^2 \equiv D \bmod 4aa'.$$

Recall that the *direct composition* (or Dirichlet composition) of f and g is defined as
$$F(x,y) = aa'x^2 + Bxy + \frac{B^2-D}{4aa'}y^2.$$

Consider the images under the bijection $C(D) \to C(\mathcal{O})$:
$$F \mapsto [aa', \frac{-B-\sqrt{D}}{2}], \quad f \mapsto [a, \frac{-b-\sqrt{D}}{2}], \quad g \mapsto [a', \frac{-b'-\sqrt{D}}{2}].$$

Denote $\Delta = \frac{-B-\sqrt{D}}{2}$. Then
$$[a, \frac{-b-\sqrt{D}}{2}] = [a, \Delta], \quad [a', \frac{-b'-\sqrt{D}}{2}] = [a', \Delta],$$

Date: December 4, 2020.

and

$$[a,\Delta]\cdot[a',\Delta]=[aa',a\Delta,a'\Delta,\Delta^2].$$

As $B^2\equiv D \bmod 4aa'$,

$$\Delta^2=\frac{B^2+D-2B\sqrt{D}}{4}=\frac{2B^2-2B\sqrt{D}}{4}=-B\Delta.$$

Hence

$$[a,\Delta]\cdot[a',\Delta]=[aa',a\Delta,a'\Delta,-B\Delta]=[aa',\Delta],$$

where the last equality is due to $(B,a,a')=1$.

To summarize, the class of F is well-defined, i.e. independent of the choice of f and g. Clearly, $C(D)\to C(\mathcal{O})$ is a group homomorphism. Moreover, $C(D)$ is an abelian group under direct composition such that $C(D)\cong C(\mathcal{O})$.

To prove Theorem 1(3), the following lemma would be useful.

Lemma 3. *Fix an order $\mathcal{O}$ of K with the ideal norm map $N(\cdot)$ on K.*

(1) *For each $0\neq\alpha\in\mathcal{O}$, $N(\alpha\mathcal{O})=N(\alpha)$, where the right hand side is the norm of elements in K.*
(2) *$N(\mathfrak{a}\mathfrak{b})=N(\mathfrak{a})N(\mathfrak{b})$ for any proper $\mathcal{O}$-ideals $\mathfrak{a},\mathfrak{b}$.*
(3) *$\mathfrak{a}\overline{\mathfrak{a}}=N(\mathfrak{a})\cdot\mathcal{O}$, where $\mathfrak{a}$ is any proper $\mathcal{O}$-ideal.*

Proof. (1) is clear for the following reason. Consider the $\mathbb{Z}$-linear map

$$T_\alpha:\mathcal{O}\longrightarrow\mathcal{O},\quad x\longmapsto\alpha x.$$

Then $N(\alpha)=\det(T_\alpha)=|\mathcal{O}/T_\alpha(\mathcal{O})|=|\mathcal{O}/\alpha\mathcal{O}|=N(\alpha\mathcal{O})$.

Now we prove (2)(3). For $\alpha\in\mathcal{O}$, $N(\alpha\mathfrak{a})=N(\alpha)N(\mathfrak{a})$ because

$$0\to\alpha\mathcal{O}/\alpha\mathfrak{a}\to\mathcal{O}/\alpha\mathfrak{a}\to\mathcal{O}/\alpha\mathcal{O}\to 0$$

is an exact sequence, where by multiplicating by α we have an isomorphism $\mathcal{O}/\mathfrak{a}\simeq\alpha\mathcal{O}/\alpha\mathfrak{a}$. Suppose $\mathfrak{a}=\alpha[1,\tau]$ so that $\mathcal{O}=[1,\alpha\tau]$. Then $a\mathfrak{a}=\alpha[a,a\tau]$; here a comes from the ppdf $f(x,y)=ax^2+bx+c$ of discriminant D for $(a,b,c)=1$, $f(\tau)=0$, and $a>0$. Thus, $N(a)=a^2$ and

$$N(a\mathfrak{a})=N(a)N(\mathfrak{a})=N(\alpha)N([a,a\tau])=aN(\alpha)\implies N(\mathfrak{a})=\frac{N(\alpha)}{a}.$$

We also have $\overline{\mathfrak{a}}=\overline{\alpha}[1,\overline{\tau}]$. Therefore,

$$\begin{aligned}\mathfrak{a}\overline{\mathfrak{a}}&=\alpha\overline{\alpha}[1,\tau][1,\overline{\tau}]\\&=N(\alpha)[1,\tau,\overline{\tau},\tau\overline{\tau}]\\&=\frac{N(\alpha)}{a}[a,\frac{-b+\sqrt{D}}{2},c]\\&=\frac{N(\alpha)}{a}[a,b,c,\frac{-b+\sqrt{D}}{2}]\\&=\frac{N(\alpha)}{a}\mathcal{O}=N(\mathfrak{a})\mathcal{O}.\end{aligned}$$

Now we have proved (3). As for (2), we have

$$N(\mathfrak{a}\mathfrak{b})\mathcal{O}=\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{b}\overline{\mathfrak{b}}=N(\mathfrak{a})N(\mathfrak{b})\mathcal{O}.$$

This completes the proof. $\square$

Now we are ready to resume on the proof of our main theorem.

Proof of Theorem 1(3). Suppose m is represented by f. Then $m^2 = d^2 a$ for some a, where a is properly represented by $f(x,y) = ax^2 + bxy + cy^2$. Let τ be a root of $f(x,1)$ in the upper half plane. Then $\mathfrak{a} = [a, a\tau]$ is a proper $\mathcal{O}$-ideal. It follows that for $\mathcal{O} = [1, a\tau]$, we have an isomorphism $f \mapsto \mathfrak{a}$ from Theorem 1(2) that we have proved last time, with $N(\mathfrak{a}) = a$. Conversely, let

$$m = N(\mathfrak{a}) = \frac{N(\alpha)}{a}, \quad \mathfrak{a} = \alpha[1,\tau], \quad \mathcal{O} = [1, a\tau],$$

where $\alpha, \alpha\tau \in \mathcal{O}$. Then for some $p, q, r, s \in \mathbb{Z}$,

$$\alpha = p + qa\tau, \quad \alpha\tau = r + sa\tau.$$

So we compute that

$$\begin{aligned} m = N(\mathfrak{a}) = \frac{N(\alpha)}{a} &= \frac{1}{a}(p + qa\tau)(p + qa\overline{\tau}) \\ &= \frac{1}{a}(p^2 - bpq + acq^2) \\ &= \frac{1}{a}((sa)^2 + sa(bq) + acq^2), \qquad (p = qb + sa, \ -qc = r) \\ &= as^2 + bsq + cq^2 \\ &= f(p,q). \end{aligned}$$

$\square$

Corollary 4. *Let $0 \neq m \in \mathbb{Z}$ Then for any ideal class in $C(\mathcal{O})$, there exists a proper $\mathcal{O}$-ideal whose norm is coprime to m.*

Caveat. We remark that the isomorphism $C(D) \simeq C(\mathcal{O})$ is not valid for *real* quadratic fields. For a counterexample, let $K = \mathbb{Q}(\sqrt{3})$ and then $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ is a UFD. We have seen before that $d_K = 12$ and $h(12) \neq 1$, because $x^2 - 3y^2$ is not proper equivalent to $x^2 + 3y^2$ under any $\mathrm{SL}_2(\mathbb{Z})$-action. Hence the group homomorphism $C(D) \to C(\mathcal{O})$ fails to be injective in this case.

2. Ideal prime to the conductor

Recall that for any order $\mathcal{O}$ of K, its conductor f is defined as $[\mathcal{O}_K : \mathcal{O}]$. The ultimate goal of this section is to construct the following isomorphism:

$$\begin{aligned} C(\mathcal{O}) &\simeq \text{class group of } \mathcal{O}\text{-ideals prime to } f \\ &\simeq \text{class group of } \mathcal{O}_K\text{-ideals prime to } f \end{aligned}$$

Definition 5.
(1) Say an $\mathcal{O}$-ideal $\mathfrak{a}$ is *prime to f* if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.
(2) Let m be a positive integer. Say an $\mathcal{O}_K$-ideal $\mathfrak{a}$ is *prime to m* if $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$.

Lemma 6.
(1) *An ideal $\mathfrak{a} \subseteq \mathcal{O}$ is prime to f if and only if $(N(\mathfrak{a}), f) = 1$.*
(2) *Every $\mathcal{O}$-ideal prime to f is proper.*

Proof. (1) Take the multiplicating map

$$m_f : \mathcal{O}/\mathfrak{a} \xrightarrow{\cdot f} \mathcal{O}/\mathfrak{a}.$$

Then we obtain

$$\begin{aligned}\mathfrak{a} \text{ is prime to } f &\iff m_f \text{ is surjective}\\ &\iff m_f \text{ is an isomorphism}\\ &\iff (f, |\mathcal{O}/\mathfrak{a}|) = (f, N(\mathfrak{a})) = 1.\end{aligned}$$

(2) Suppose $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f. Take $\beta \in K$ such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$ (and hence $\beta \in \mathcal{O}_K$). We have

$$\begin{aligned}&\beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathcal{O}\\ &\beta(\mathfrak{a} + f\mathcal{O}) \subseteq \mathfrak{a} + \beta f\mathcal{O} \subseteq \mathfrak{a} + f\mathcal{O}_K \subseteq \mathfrak{a} + \mathcal{O} = \mathcal{O}.\end{aligned}$$

Hence $\beta\mathcal{O} \subseteq \mathcal{O}$ and $\beta \in \mathcal{O}$ follows, i.e. $\{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}$. So $\mathfrak{a}$ is proper.

□

Notation 7. Denote $I(\mathcal{O}, f)$ the subgroup of $I(\mathcal{O})$ generated by $\mathcal{O}$-ideals prime to f. And denote $P(\mathcal{O}, f)$ the subgroup of $I(\mathcal{O}, f)$ generated by $\{\alpha\mathcal{O} \mid \alpha \in \mathcal{O}, (N(\alpha), f) = 1\}$.

Proposition 8. *There is a natural isomorphism*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \xrightarrow{\sim} I(\mathcal{O})/P(\mathcal{O}).$$

Proof. By Corollary 4 this is surjective. Note that the injectivity is equivalent to

$$P(\mathcal{O}, f) = P(\mathcal{O}) \cap I(\mathcal{O}, f).$$

The "$\subseteq$" direction is apparent. Conversely, for $\alpha \in K$ we have $\alpha\mathcal{O} \in P(\mathcal{O}) \cap I(\mathcal{O}, f)$. Then $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ with some $\mathfrak{b}, \mathfrak{b}$ being $\mathcal{O}$-ideals that are prime to f. Hence $N(\mathfrak{b})\alpha\mathcal{O} = \mathfrak{a}\overline{\mathfrak{b}}$ by multiplicating by $\overline{\mathfrak{b}}$. Let $\alpha' = N(\mathfrak{b})\alpha$ and then $\alpha'\mathcal{O} = \mathfrak{a}\overline{\mathfrak{b}}$, and

$$(N(\mathfrak{b}), f) = 1, \quad (N(\mathfrak{b}\overline{\mathfrak{b}}), f) = 1, \quad (N(\alpha'), f) = 1.$$

Thus, $\alpha\mathcal{O} = (\alpha'\mathcal{O})(N(\mathfrak{b})\mathcal{O})^{-1}$ with $\alpha'\mathcal{O}, N(\mathfrak{b})\mathcal{O} \in P(\mathcal{O}, f)$. This proves $\alpha\mathcal{O} \in P(\mathcal{O}, f)$, and hence the injectivity. □

Proposition 9. (1) *If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal prime to f with the same norm.*

(2) *If $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal prime to f with the same norm.*

(3) *We obtain an isomorphism*

$$\begin{aligned}I_K(f) &\xrightarrow{\sim} I(\mathcal{O}, f)\\ \mathfrak{a} &\longmapsto \mathfrak{a} \cap \mathcal{O}\\ \mathfrak{a}\mathcal{O}_K &\longleftarrow\!\shortmid\ \mathfrak{a}\end{aligned}$$

Proof. (1) Consider the natural injection

$$\iota : \mathcal{O}/\mathfrak{a} \cap \mathcal{O} \hookrightarrow \mathcal{O}_K/\mathfrak{a}.$$

Since $\mathfrak{a} + f\mathcal{O}_K = \mathcal{O}_K$, we see $m_f : \mathcal{O}_K/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}$ is an isomorphism. In particular, $(N(\mathfrak{a}), f) = 1$. Then $(N(\mathfrak{a} \cap \mathcal{O}), f) = 1$ follows. Hence $\mathfrak{a} \cap \mathcal{O}$ is prime to f. Note that

$\operatorname{coker}(\iota)$ is annihilated by f, so that $\operatorname{coker}(\iota) = 0$. This proves that ι is an isomorphism, and the assertion (1) follows. $\square$

In the next lecture we will resume on the proof for (2)(3).

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