BASIC NUMBER THEORY: LECTURE 13

WENHAN DAI

1. Orders in imaginary quadratic field

We first introduce the definition of orders. We always assume K is an imaginary quadratic field.

Definition 1. An ideal $\mathcal{O} \subseteq K$ is called an *order* if

(1) $\mathcal{O}$ is a subring of K,
(2) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module, and
(3) there exists an isomorphism $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq K$ of $\mathbb{Q}$-vector spaces.

Note that (1)(2) in the definition above guarantee that $\mathcal{O}$ is a subring of $\mathcal{O}_K$. As it is clear that $\mathcal{O}_K$ is an order, it turns out that $\mathcal{O}_K$ is the maximal order of K.

Remark 2. Note that when K is an imaginary quadratic field, $\mathcal{O}$ is an order if and only if $\mathcal{O}$ is a subring of $\mathcal{O}_K$ with $\operatorname{rank}_{\mathbb{Z}} \mathcal{O} = 2$ as a $\mathbb{Z}$-module, which implies that $\mathcal{O} \neq \mathbb{Z}$.

Recall that

$$\mathcal{O}_K = [1, w_K] := \mathbb{Z}[w_K], \quad w_K = \frac{\sqrt{d_K} + d_K}{2}.$$

In the upcoming context we use $[-]$ to denote the $\mathbb{Z}$-linear combination for short.

Lemma 3. *Suppose $\mathcal{O}$ is an order of K. Then:*

(1) *$\mathcal{O}$ has finite index in $\mathcal{O}_K$;*
(2) *Let $f = [\mathcal{O}_K : \mathcal{O}]$ by regarding $\mathcal{O}$ as a subgroup of $\mathcal{O}_K$. Then*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, fw_K].$$

Proof. (1) Since $\mathcal{O} \subseteq \mathcal{O}_K$ and both of them share the same $\mathbb{Z}$-rank 2, we have

$$[\mathcal{O}_K : \mathcal{O}] = |\mathcal{O}_K/\mathcal{O}| < \infty.$$

(2) Note that $f\mathcal{O}_K \subseteq \mathcal{O}$ and then

$$\mathbb{Z} + f\mathcal{O}_K = \mathbb{Z} + [f, fw_K] = [1, fw_K] \subseteq \mathcal{O}.$$

Since $[1, fw_K]$ has index f in $\mathcal{O}_K$, we see $\mathcal{O} \subseteq [1, fw_K]$. $\square$

Definition 4. Suppose $\mathcal{O}$ is an order of K. We call $f = [\mathcal{O}_K : \mathcal{O}]$ the *conductor* of $\mathcal{O}$.

Be careful that there might be various versions of "conductor" in algebraic number theory, e.g. there is an irrelevant definition with the same name in Kronecker-Weber theorem.

Date: November 24, 2020.

Corollary 5. *Let f be the conductor of the order $\mathcal{O}$. Then*

(1) *The discriminant of $\mathcal{O}$ over $\mathbb{Z}$ is*

$$\Delta_{\mathcal{O}/\mathbb{Z}} = f^2 \Delta_{\mathcal{O}_K/\mathbb{Z}} = f^2 d_K.$$

(2) *$\mathcal{O}$ is uniquely determined by $\Delta_{\mathcal{O}/\mathbb{Z}}$.*

Proof. (1) is already known by definition of the discriminant. For (2), take

$$\Delta = \Delta_{\mathcal{O}/\mathbb{Z}}, \quad K = \mathbb{Q}(\sqrt{\Delta}), \quad f = \sqrt{\frac{\Delta}{d_K}}.$$

We have

$$\mathcal{O} = [1, f w_K] = [1, (\Delta + \sqrt{\Delta})/2].$$

This determines $\mathcal{O}$ by Δ. $\square$

The following Lemma 6 and Remark 7 dictate that $\mathcal{O}$ partially satisfies the property of a Dedekind domain.

Lemma 6. *Let $\mathcal{O}$ be an order.*

(1) *$\mathcal{O}$ is noetherian as a ring.*
(2) *For any $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ ideal, we have $|\mathcal{O}/\mathfrak{a}| < \infty$.*
(3) *If $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ is a prime ideal then $\mathfrak{a}$ is maximal in $\mathcal{O}$.*

Proof. (1) is clear as $\mathcal{O}_K$ is noetherian as a Dedekind domain. For (2), choose $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ and hence

$$\mathfrak{a}\mathcal{O} \subseteq \mathfrak{a} \subseteq \mathcal{O}.$$

So $\mathfrak{a}$ is of rank 2 over $\mathbb{Z}$, as $\operatorname{rank}_{\mathbb{Z}} \mathcal{O} = \operatorname{rank}_{\mathbb{Z}} \mathfrak{a}\mathcal{O} = 2$. This shows $|\mathcal{O}/\mathfrak{a}| < \infty$.

(3) follows from noticing that $\mathcal{O}/\mathfrak{a}$ is a finite integral domain. $\square$

Remark 7. (1) For any order $\mathcal{O}$, the maximal order $\mathcal{O}_K$ is the integral closure of $\mathcal{O}$ in K. However, $\mathcal{O}$ is not a Dedekind domain unless $\mathcal{O} = \mathcal{O}_K$ because it fails to be integrally closed.

(2) In general, $\mathcal{O}$ does not have unique factorization of ideals.

Definition 8. An $\mathcal{O}$-ideal $\mathfrak{a}$ is called *proper* if

$$\{\beta \in K \mid \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}.$$

Note that in Definition 8, $\mathcal{O}_K$ always encompasses the set $\{\beta \in K \mid \beta\mathfrak{a} \subseteq \mathfrak{a}\}$. In fact, the equality can be replaced with "$\subseteq$" above.

Example 9. For $K = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$, take the order

$$\mathcal{O} = \mathbb{Z}[\sqrt{-3}] \subsetneq \mathcal{O}_K = [1, \frac{1+\sqrt{-3}}{2}].$$

Consider the $\mathcal{O}$-ideal $\mathfrak{a} = [2, 1+\sqrt{-3}] = 2\mathcal{O}_K \subseteq \mathcal{O}$. As an extension of $\mathbb{Z} \cdot 2\mathbb{Z} \subseteq 2\mathbb{Z}$, we see

$$\{\beta \in K \mid \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}_K.$$

So in this case $\mathfrak{a}$ is not proper in $\mathcal{O}$.

Definition 10. A *fractional $\mathcal{O}$-ideal* $\mathfrak{a}$ is a finitely generated $\mathcal{O}$-submodule of K. It is called *proper* if $\{\beta \in K \mid \beta\mathfrak{a} \subseteq \mathfrak{a}\} \subseteq \mathcal{O}$. It is called *invertible* if there is fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Proposition 11. *Let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then*

$$\mathfrak{a} \text{ is proper} \iff \mathfrak{a} \text{ is invertible.}$$

Proof. The necessity is easy. Suppose $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ for some $\mathfrak{b}$. Then the candidate condition $\beta\mathfrak{a} \subseteq \mathfrak{a}$ implies $\beta\mathcal{O} \subseteq \mathfrak{a}\mathfrak{b} = \mathcal{O}$, and hence $\beta \in \mathcal{O}$. Conversely, the following Lemma 12 is required. Granting the lemma, as $\mathfrak{a}$ is of rank 2 over $\mathbb{Z}$, let

$$\mathfrak{a} = [\alpha, \beta] = \alpha[1, \tau]$$

for some τ with minimal polynomial $ax^2 + bx + c$, where $(a, b, c) = 1$. The strategy is trying to construct $\mathfrak{a}\overline{\mathfrak{a}}$ as a principal ideal. Then

$$\mathfrak{a}\overline{\mathfrak{a}} = \alpha\overline{\alpha}[1, \tau][1, \overline{\tau}] = \alpha\overline{\alpha}[1, \tau, \overline{\tau}, \tau\overline{\tau}].$$

Then, as $\mathcal{O} = [1, a\tau]$,

$$\begin{aligned} a\mathfrak{a}\overline{\mathfrak{a}} &= N(\alpha)[a, a\tau, a\overline{\tau}, a\tau\overline{\tau}] \\ &= N(\alpha)[a, a\tau, -b, c] \\ &= N(\alpha)[1, a\tau] \qquad (\text{as } (a, b, c) = 1) \\ &= N(\alpha)\mathcal{O}. \end{aligned}$$

Therefore,

$$\mathfrak{a} \cdot \frac{a}{N(\alpha)}\overline{\mathfrak{a}} = \mathcal{O}.$$

So $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal. □

Lemma 12. *Let $K = \mathbb{Q}(\tau)$ be an imaginary quadratic field with $ax^2 + bx + c$ being the minimal polynomial of τ, where $(a, b, c) = 1$. Then $[1, \tau]$ is a proper fractional ideal of the order $[1, a\tau]$.*

Proof. Note that $a\tau$ is an algebraic integer such that $a\tau \in \mathcal{O}_K$. Then $\mathcal{O} = [1, a\tau]$ is an order of K. It remains to show that

$$\{\beta \in K : \beta[1, \tau] \subseteq [1, \tau]\} = \mathcal{O}.$$

Suppose $\beta[1, \tau] \subseteq [1, \tau]$, then we have

- $\beta = m + n\tau$ for some $m, n \in \mathbb{Z}$,
- $\beta\tau = m\tau + n\tau^2 = (m - \frac{b}{a})\tau - \frac{cn}{a} \in [1, \tau]$,[1] and
- $\frac{bn}{a}, \frac{cn}{a} \in \mathbb{Z}$ if and only if $\frac{n}{a} \in \mathbb{Z}$.

Or equivalently, $\beta \in [1, a\tau]$. □

Definition 13. Given an order $\mathcal{O}$, we define

(1) $I(\mathcal{O}) :=$ the group of proper fractional $\mathcal{O}$-ideals,
(2) $P(\mathcal{O}) :=$ the group of principal fractional $\mathcal{O}$-ideals, and
(3) $C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$, the ideal class group of the order $\mathcal{O}$, with $h(\mathcal{O}) := |C(\mathcal{O})|$ the class number of $\mathcal{O}$.

[1]By using the condition $\tau^2 + \frac{b}{a}\tau + \frac{c}{a} = 0$ one cancels the items of degree $\geqslant 2$.

2. Orders and quadratic forms

Theorem 14. *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, $h(\mathcal{O}) = h(D)$.

Proof. (1) We have
$$[a, \frac{-b+\sqrt{D}}{2}] = a[1, \frac{-b+\sqrt{D}}{2a}] = a[1,\tau], \quad \tau = \frac{-b+\sqrt{D}}{2}.$$
And τ is a root of $f(x,1)$. Since $D<0$, we see τ lies in the upper half plane. Call τ the root of $f(x,y)$. As $[1,\tau]$ is a proper fractional ideal of $[1,a\tau]$, $a[1,\tau] = [a,a\tau]$ is a proper fractional ideal of $[1,a\tau]$. Also, for $f = [\mathcal{O}_K : \mathcal{O}]$,
$$\begin{aligned}[1,a\tau] &= [1, \frac{-b+\sqrt{D}}{2}] = [1, \frac{(-b-fd_K)+fd_K+\sqrt{D}}{2}] \\ &= [1, \frac{fd_K+\sqrt{D}}{2}] = [1, fw_K] = \mathcal{O}.\end{aligned}$$
Here the second-last equality is due to $D = f^2 d_K$, and the third equality is because of $b \equiv D = b^2 - 4ac = f^2 d_K \equiv f d_K \bmod 2$.

(2) Let $f(x,y), g(x,y)$ be ppdfs of discriminant D with roots τ, τ', respectively.

Claim 1. $f \sim g$ via proper equivalence if and only if
$$\tau' = \frac{p\tau+q}{r\tau+s}, \quad \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$
(Recall that the upper half plane is stable under the action of $\mathrm{SL}_2(\mathbb{Z})$.)

For this, if $f \sim g$ then $f(x,y) = g(px+qy, rx+sy)$, and in particular,
$$f(x,1) = (rx+s)^2 g(\frac{px+q}{rx+s}, 1),$$
and hence
$$f(\tau,1) = g(\frac{p\tau+q}{r\tau+s}, 1) = g(\tau',1) = 0.$$
This shows that τ and τ' are differed by an element of $\mathrm{SL}_2(\mathbb{Z})$. Conversely, we take
$$f'(x,y) = g(px+qy, rx+sy).$$
Then $f(x,y)$ and $f'(x,y)$ has the same root τ. This shows $f = f'$ and proves Claim 1.

Claim 2. $[1,\tau]$ and $[1,\tau']$ are in the same ideal class if and only if
$$\tau' = \frac{p\tau+q}{r\tau+s}, \quad \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

For Claim 2, we note that $[1,\tau] \sim [1,\tau']$ if and only if there is some λ such that $\lambda[1,\tau'] = [1,\tau]$. This implies

$$\lambda = r\tau + s, \quad \lambda\tau' = p\tau + q, \quad r, s, p, q \in \mathbb{Z}.$$

Hence

$$\tau' = \frac{\lambda\tau'}{\lambda} = \frac{p\tau + q}{r\tau + s}, \quad \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Conversely, supposing the condition above, we get $\lambda = r\tau + s$ and $\lambda[1,\tau'] = [1,\tau]$. Then Claim 2 follows.

Combining two claims together, we see the map

$$\begin{aligned} C(D) &\longrightarrow C(\mathcal{O}) \\ f(x,y) &\longmapsto [a, \frac{-b+\sqrt{D}}{2}] \end{aligned}$$

is a group homomorphism and injective. It remains to prove the surjectivity. Let $[1,\tau]$ be any proper fractional ideal of $\mathcal{O}$, and $ax^2 + bx + c$ with $(a,b,c) = 1$ and $a > 0$ the minimal polynomial of τ. Consider the ppdf $f(x,y) = ax^2 + bxy + cy^2$. Then $[1,\tau]$ is a proper fractional ideal of an order $\mathcal{O}'$ which has discriminant $\mathrm{disc}(f(x,y))$. Hence

$$\mathcal{O} = \mathcal{O}', \quad D = \mathrm{disc}(f(x,y)).$$

This finishes the proof. $\square$

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