If $\operatorname{disc}(a,b,c) < 0$ then $4ac - b^2 = -\operatorname{disc}(a,b,c) > 0$, so the nonzero values taken on by $ax^2 + bxy + cy^2$ are only positive or only negative, depending on the sign of a. On the other hand, if $\operatorname{disc}(a,b,c) > 0$, then $(2ax+by)^2 + (4ac-b^2)y^2$ takes both positive and negative values, so (a,b,c) does also.

9.2.5 Rings of Integers in Quadratic Fields

We have seen quadratic number fields several times before. We now make the theory more precise, in order to see how the arithmetic of quadratic number fields is closely linked to the theory of quadratic forms.

Let $D \neq 0, 1$ be a square-free integer. The quadratic field obtained by adjoining $\sqrt{D}$ to $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Definition 9.2.12 (Integral). An element $x \in K$ is *integral over* $\mathbb{Z}$ if it is the root of a quadratic polynomial of the form $x^2 + ax + b$ with $a, b \in \mathbb{Z}$.

The integral elements of K form an important subring of K.

Definition 9.2.13 (Ring of Integers). The *ring of integers* in K is

$$\mathcal{O}_K = \{x \in K \mid x \text{ is integral over } \mathbb{Z}\}.$$

It's not at all clear from the definition just what $\mathcal{O}_K$ is, or even that it's a ring. Proposition 9.2.16 below will give a more explicit description of $\mathcal{O}_K$.

Lemma 9.2.14. *The map $K \to K$ given by*

$$a + b\sqrt{D} \mapsto \overline{a + b\sqrt{D}} = a - b\sqrt{D}$$

is an isomorphism of fields.

Proof. We have

$$\begin{aligned}
\overline{(a + b\sqrt{D})(c + d\sqrt{D})} &= \overline{(ac + bd) + (ad + bc)\sqrt{D}} \\
&= (ac + bd) - (ad + bc)\sqrt{D} \\
&= (a - b\sqrt{D})(c - d\sqrt{D}) \\
&= \overline{a + b\sqrt{D}c + d\sqrt{D}}.
\end{aligned}$$

□

Lemma 9.2.15. *Let $\alpha \in K$. The determinant of left multiplication by α on the 2-dimensional $\mathbb{Q}$-vector space K is $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$. The trace of left multiplication is $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$. The characteristic polynomial of left multiplication by α is $x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha)$.*

Proof. A basis for K as a $\mathbb{Q}$-vector space is $1, \sqrt{D}$. The matrix of left multiplication by $\alpha = a + b\sqrt{D}$ on this basis is $\begin{pmatrix} a & Db \\ b & a \end{pmatrix}$. Since $T(\alpha) = 2a$ and $\mathrm{N}(\alpha) = a^2 - Db^2$, the lemma follows. □

Proposition 9.2.16. *If $D \equiv 1 \pmod 4$ let $\alpha = (1+\sqrt{D})/2$, and otherwise let $\alpha = \sqrt{D}$. Then*

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}.$$

Proof. First we prove that if $x = a + b\alpha \in \mathbb{Z}[\alpha]$, then $x \in \mathcal{O}_K$. By Lemma 9.2.15 it suffices to show that $\mathrm{Tr}(x)$ and $\mathrm{N}(x)$ lie in $\mathbb{Z}$. First we verify this for $x = \alpha$ by noting that $\mathrm{Tr}(\alpha) = 1$ and

$$\mathrm{N}(\alpha) = \begin{cases} (1-D)/4 & \text{if } D \equiv 1 \pmod 4 \\ D & \text{otherwise.} \end{cases}$$

More generally, if $x = a + b\alpha$ with $a, b \in \mathbb{Z}$, then

$$\mathrm{Tr}(x) = \mathrm{Tr}(a + b\alpha) = 2a + b\,\mathrm{Tr}(\alpha) = 2a + b \in \mathbb{Z},$$

and

$$\begin{aligned} \mathrm{N}(x) &= (a + b\alpha)(a + b\overline{\alpha}) \\ &= a^2 + ab(\alpha + \overline{\alpha}) + b^2\alpha\overline{\alpha} \\ &= a^2 + ab\,\mathrm{Tr}(\alpha) + b^2\,\mathrm{N}(\alpha) \in \mathbb{Z}. \end{aligned}$$

For the other inclusion, suppose $x = a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ is integral over $\mathbb{Z}$. Then $\mathrm{Tr}(x) = 2a \in \mathbb{Z}$ and $\mathrm{N}(x) = a^2 - b^2D \in \mathbb{Z}$. Thus $a = a'/2$ for some $a' \in \mathbb{Z}$ and $(a')^2/4 - b^2D \in \mathbb{Z}$. Thus $(2b)^2D \in \mathbb{Z}$, so since D is square free the denominator of b is either 1 or 2. The denominator of b is 2 if and only if the denominator of a is 2 since $a^2 - b^2D \in \mathbb{Z}$. If the denominator of b is 1, then $a, b \in \mathbb{Z}$ and we are done, and if the denominator of b is 2, then $2b \in \mathbb{Z}$ and $(a')^2 \equiv (2b)^2D \pmod 4$, so D is a perfect square modulo 4 and hence $D \equiv 1 \pmod 4$ (since D is square free) and $x \in \mathbb{Z}[\alpha]$. □

Definition 9.2.17 (Field Discriminant). Let γ_1, γ_2 be any basis for $\mathcal{O}_K$, e.g., $\gamma_1 = 1$, $\gamma_2 = \alpha$ where α is as in Proposition 9.2.16. The *discriminant* of $\mathcal{O}_K$ is

$$d = \mathrm{disc}(\mathcal{O}_K) = \det\left(\begin{pmatrix} \gamma_1 & \gamma_1' \\ \gamma_2 & \gamma_2' \end{pmatrix}\right)^2.$$

Making a different choice of basis γ_1, γ_2 amounts to changing the determinant in the definition by ± 1, so the discriminant is well defined.

Proposition 9.2.18. *Let $K = \mathbb{Q}[\sqrt{D}]$ with D squarefree. Then the discriminant of K is D if $D \equiv 1 \pmod 4$ and $4D$ otherwise.*

Proof. First suppose $D \equiv 1 \pmod 4$. Then 1 and $\alpha = (1+\sqrt{D})/2$ are a basis for $\mathcal{O}_K$, so

$$\begin{aligned} d &= \det\left(\begin{pmatrix} 1 & \alpha \\ 1 & \alpha' \end{pmatrix}\right)^2 \\ &= (-\alpha' - \alpha)^2 \\ &= (-\sqrt{D})^2 = D. \end{aligned}$$

On the other hand, if $D \not\equiv 1 \pmod 4$, then $\alpha = \sqrt{D}$ and $d = (-\sqrt{D} - \sqrt{D})^2 = 4D$. □

Let d be the discriminant of $\mathbb{Q}[\sqrt{D}]$. In Section 9.5 we will see that there is an bijection between certain equivalence classes of ideals in $\mathcal{O}_K$ and equivalence classes of binary quadratic forms of discriminant d. The set of equivalence classes of ideals in $\mathcal{O}_K$ will have the structure of finite abelian group induced by multiplication of ideals. Understanding whether or not numbers are represented by certain quadratic forms, is related to deciding whether or not certain ideals are principal in $\mathcal{O}_K$; this leads to class field theory, one of the major accomplishments of 20th century number theory.

9.3 Reduction Theory

Recall that a binary quadratic form is a polynomial of the form $f(x,y) = ax^2+bxy+cy^2$. Our motivating problem is to decide which numbers are represented by f; i.e., for which integers n do there exist integers x, y such that $ax^2+bxy+cy^2 = n$? If $g \in \mathrm{SL}_2(\mathbb{Z})$ then $f(x,y)$ and $f|_g(x,y) = f\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$ represent exactly the same set of integers. Also, $\mathrm{disc}(f) = \mathrm{disc}(f|_g)$, where $\mathrm{disc}(f) = b^2 - 4ac$, and f is called *positive definite* if $\mathrm{disc}(f) < 0$ and $a > 0$.

This section is about reduction theory, which allows us to decide whether or not two positive definite binary quadratic forms are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$.

9.3.1 Reduced Forms

Definition 9.3.1 (Reduced). A positive definite quadratic form (a,b,c) is *reduced* if $|b| \le a \le c$ and if, in addition, when one of the two inequalities is an equality (i.e., either $|b| = a$ or $a = c$), then $b \ge 0$.

There is a geometric interpretation of the notion of being reduced. Let $D = \mathrm{disc}(a,b,c) = b^2 - 4ac$ and set $\tau = \frac{-b+\sqrt{D}}{2a}$, so τ is the root of $ax^2 + bx + c$ with positive imaginary part. The right action of $\mathrm{SL}_2(\mathbb{Z})$ on positive definite binary quadratic forms corresponds to the left action to have that $[I][I] = [I][I'] = 1$, so the group of ideals would be a finite 2-torsion group, hence have order a power of 2, which is generally not the case. We must be much more careful in how we associate a binary quadratic form to an ideal.

Definition 9.5.2 (Correctly Ordered). A basis $[\alpha, \beta]$ for an ideal I is *correctly ordered* if

$$\frac{\alpha\beta' - \beta\alpha'}{\sqrt{d}} > 0.$$

Example 9.5.3. Let $d = -4$ and let I be the ideal generated by $(5, i-2)$. Note that $\mathcal{O}_K = \mathbb{Z}[i]$, so $\mathcal{O}_K/I \cong \mathbb{Z}/5$. We have $I = [5, i-2]$, since $[5, i-2] \subset I$ and $\det\left(\begin{smallmatrix} 5 & -2 \\ 0 & 1 \end{smallmatrix}\right) = 5$ (so that $\#(\mathcal{O}_K/[5, i-2]) = 5$). Notice that $[5, i-2]$ is not correctly ordered because

$$\frac{5(-i-2) - (i-2)5}{\sqrt{-4}} = -5 < 0.$$

The basis $[i-2, 5]$ is correctly ordered.

Proposition 9.5.4. *Any two correctly ordered bases of an ideal I are equivalent by an element in $\mathrm{SL}_2(\mathbb{Z})$, and conversely.*

Proof. Suppose $[\alpha, \beta] = [\gamma, \delta]$ are two correctly ordered basis for an ideal I. Because these are two different basis for the same free $\mathbb{Z}$-module, there are $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = A \begin{pmatrix} \gamma \\ \delta \end{pmatrix},$$

and $\det(A) = \pm 1$ (this is just like a change of basis matrix in linear algebra; its determinant is a unit in the base ring). Since $a, b, c, d \in \mathbb{Z}$ and the conjugation automorphism fixes $\mathbb{Z}$, we have

$$\begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix}.$$

Taking determinants, we have

$$\alpha\beta' - \beta\alpha' = \det(A)(\gamma\delta' - \delta\gamma'). \tag{9.1}$$

Since $[\alpha, \beta]$ and $[\gamma, \delta]$ are correctly oriented, we must have $\det(A) = +1$, so $A \in \mathrm{SL}_2(\mathbb{Z})$.

Conversely, if $A \in \mathrm{SL}_2(\mathbb{Z})$ and $[\gamma, \delta]$ is a correctly oriented basis then,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix} = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$$

and by (9.1) $[\alpha, \beta]$ is also correctly oriented. $\square$

9.5.2 Norms of Ideals

Definition 9.5.5 (Norm). The *norm* of a nonzero ideal I of $\mathcal{O}_K$ is the positive integer
$$\mathrm{N}(I) = \#(\mathcal{O}_K/I).$$

Proposition 9.5.6. $II' = (N(I))$

Proof. A complete proof is given on page 128-129 of Cohn "Advanced Number Theory". This fact follows from "Hurwitz's Lemma", i.e., it is nontrivial. [5] □ 5

Lemma 9.5.7. *Let (a, b) and (c, d) be elements of $\mathbb{Z} \oplus \mathbb{Z}$ such that $D = |\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)| \neq 0$. Then the quotient abelian group*

$$M = (\mathbb{Z} \oplus \mathbb{Z})/(\mathbb{Z}(a, b) + \mathbb{Z}(c, d))$$

is finite of order D.

Proof. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. By repeatedly swapping rows, swapping columns, adding a multiple of one row to another row, or adding a multiple of one column to another column, we can transform A into a diagonal matrix $\left(\begin{smallmatrix} e & 0 \\ 0 & f \end{smallmatrix}\right)$. Each swapping and adding operations changes at most change the sign of the determinant, so $|\det(A)| = |ef|$. We may thus assume that A is diagonal, in which case the lemma is clear. □

Lemma 9.5.8. *Suppose I is an ideal of $\mathcal{O}_K$ with basis $[\alpha, \beta]$, and let d be the discriminant of K. Then*

$$\det \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}^2 = d \cdot \mathrm{N}(I)^2.$$

Proof. Let γ_1, γ_2 be a basis for $\mathcal{O}_K$. Since α and β can be written as a $\mathbb{Z}$-linear combination of γ_1 and γ_2 there is a 2×2 integer matrix A such that
$$A \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

We have

$$\begin{aligned} \det \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}^2 &= \det \left(A \cdot \begin{pmatrix} \gamma_1 & \gamma_1' \\ \gamma_2 & \gamma_2' \end{pmatrix} \right)^2 \\ &= \det(A)^2 d \\ &= \mathrm{N}(I)^2 d, \end{aligned}$$

where we use Lemma 9.5.7 to see that $\det(A) = \mathrm{N}(I)$. □

[5] Write a proof for the notes based on Cohn's proof.

9.5.3 The Ideal Class Group

For the rest of this section, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with discriminant d.

Definition 9.5.9. Two ideals $I, J \subset \mathcal{O}_K$ are *equivalent*, written $I \sim J$, if there are $\alpha, \beta \in \mathcal{O}_K$ such that

$$\alpha I = \beta J \qquad \text{and} \qquad \mathrm{N}(\alpha\beta) > 0.$$

We will denote the set of equivalence classes of **nonzero** ideals in $\mathcal{O}_K$ by $\mathrm{Cl}^+(\mathcal{O}_K)$.

Proposition 9.5.10. *Multiplication of ideals gives* $\mathrm{Cl}^+(\mathcal{O}_K)$ *an abelian group structure in which the ideal class of* $\mathcal{O}_K = (1)$ *is the identity element.*

Proof. If I and J are ideals of $\mathcal{O}_K$ then their product $IJ = \{xy : x \in I, y \in J\}$ is again an ideal in $\mathcal{O}_K$. Multiplication of ideals is easily seen to be associative and commutative, since the usual multiplication of elements in $\mathcal{O}_K$ is associative and commutative. Next we check that multiplication of ideals induces a well-defined multiplication of ideal classes. If $I_0 \sim J_0$ and $I_1 \sim J_1$, then there exists $\alpha_0, \beta_0, \alpha_1, \beta_1 \in \mathcal{O}_K$ such that $\alpha_i I_i = \beta_i J_i$ for $i = 0, 1$. Multiplying these two equalities, we see that $\alpha_0 I_0 \alpha_1 I_1 = \beta_0 J_0 \beta_1 J_1$, so $\alpha_0\alpha_1 I_0 I_1 = \beta_0\beta_1 J_0 J_1$, hence $I_0 I_1 \sim J_0 J_1$. This proves that multiplication of ideals induces a well-defined associative commutative multiplication of ideal classes.

To finish the proof, we verify that every element of $\mathrm{Cl}^+(\mathcal{O}_K)$ has an inverse. Let $I = [\alpha, \beta]$ be an ideal in $\mathcal{O}_K$. Then the ideal I' generated by the conjugates of elements of I is $[\alpha', \beta']$. By Proposition 9.5.6, the product II' is the principal ideal generated by the positive integer $\#(\mathcal{O}_K/I)$. Thus $II' \sim (1)$, so I has an inverse. $\square$

Example 9.5.11. Let $K = \mathbb{Q}[\sqrt{-20}]$. Then $\mathrm{Cl}^+(\mathcal{O}_K)$ is cyclic of order 2. A nonidentity element of $\mathrm{Cl}^+(\mathcal{O}_K)$ is $I = [1 + \sqrt{-5}, 2]$.

9.5.4 Correspondence Between Ideals and Forms

Recall that a binary quadratic form $Q = ax^2 + bxy + cy^2$ is primitive if $\gcd(a, b, c) = 1$ and has discriminant $b^2 - 4ac$. The following proposition associates a primitive binary quadratic form to an ideal of $\mathcal{O}_K$.

Proposition 9.5.12. *Let* I *be an ideal in* $\mathcal{O}_K$ *and let* $[\alpha, \beta]$ *be a correctly ordered basis for* I. *Then the quadratic form*

$$Q = \frac{\mathrm{N}(\alpha x + \beta y)}{\mathrm{N}(I)} = ax^2 + bxy + cy^2$$

has integral coefficients and is a primitive form of discriminant d.

Note that the numerator $\mathrm{N}(\alpha x+\beta y)$ in the definition of Q depends on the order of α and β.

Proof. We have

$$\begin{aligned}\mathrm{N}(\alpha x+\beta y) &= (\alpha x+\beta y)(\alpha' x+\beta' y)\\ &= \alpha\alpha' x^2+(\alpha\beta'+\alpha'\beta)xy+\beta\beta' y^2\\ &= Ax^2+Bxy+Cy^2.\end{aligned}$$

The coefficients A, B, and C are elements of $\mathbb{Z}$ because they are norms and traces. They are also elements of $(\mathrm{N}(I))$, since they are visibly elements of II' and by Proposition 9.5.6, $II'=(\mathrm{N}(I))$. Thus there exists $a,b,c\in\mathcal{O}_K$ such that

$$\begin{array}{rclcl} A &=& \alpha\alpha' &=& a\,\mathrm{N}(I),\\ B &=& \alpha\beta'+\alpha'\beta &=& b\,\mathrm{N}(I),\\ C &=& \beta\beta' &=& c\,\mathrm{N}(I).\end{array}$$

Since A and $\mathrm{N}(I)$ are both in $\mathbb{Z}$ and $a\in\mathcal{O}_K$, we see that $a\in\mathbb{Z}$; likewise, $b,c\in\mathbb{Z}$. Thus $Q=ax^2+bxy+cy^2$ has coefficients in $\mathbb{Z}$.

By Lemma 9.5.8,

$$\begin{aligned}b^2-4ac &= (B^2-4AC)/\,\mathrm{N}(I)^2\\ &= (\alpha\beta'-\beta\alpha')^2/\,\mathrm{N}(I)^2=d,\end{aligned}$$

where d is the discriminant of K.

All that remains is to show that $\gcd(a,b,c)=1$. If f is a positive divisor of $\gcd(a,b,c)$, then $f^2\mid b^2-4ac=d$. If $d\equiv 1 \pmod 4$ then d is square free so $f=1$. If $d\equiv 0\pmod 4$ then $d'=d/4$ is square free and $d'\not\equiv 1 \pmod 4$, so $f=1$ or $f=2$. If $f=2$ write $a=2a'$, $b=2b'$, and $c=2c'$ for integers a',b',c' with b' odd. Then

$$b^2-4ac=4b'^2-16a'c'=4d'.$$

Reducing this equation modulo 16 implies that $4b'^2\equiv 4d' \pmod{16}$. Dividing this congruence through by 4 implies that $b'^2\equiv d'\pmod 4$. Since b' is odd, $b'^2\equiv 1\pmod 4$, which contradicts the fact that $d'\not\equiv 1\pmod 4$. Thus $f=1$ in all cases, so $ax^2+bxy+cy^2$ is primitive. $\square$

Example 9.5.13. Let $K=\mathbb{Q}[\sqrt{-20}]$ and $I=[1+\sqrt{-5},2]$, as in Example 9.5.11. Then

$$\begin{aligned}\mathrm{N}(\alpha x+\beta y) &= ((1+\sqrt{-5})x+2y)((1-\sqrt{-5})x+2y)\\ &= 6x^2+4xy+4y^2.\end{aligned}$$

The norm of I is $|\det((\begin{smallmatrix}1&2\\1&0\end{smallmatrix}))|=2$. Thus $Q=3x^2+2xy+2y^2$. Notice, as a check, that $\mathrm{disc}(Q)=b^2-4ac=2^2-4\cdot 3\cdot 2=-20$.

Example 9.5.14. Let $K = \mathbb{Q}[\sqrt{23}]$, which has discriminant $d = 92$. The ideal $I = (\sqrt{23})$ is principal, but it is not equivalent to $(1) \in \mathrm{Cl}^+(\mathcal{O}_K)$. The quadratic form associated to $I = [\sqrt{23}, 23]$ is

$$Q = \frac{-23x^2 + 23^2y^2}{23} = -x^2 + 23y^2.$$

The quadratic form associated to $(1) = [\sqrt{23}, 1]$ is $R = -23x^2 + y^2$. These two forms can not be equivalent since Q represents -1 but R doesn't (since modulo 4 we have $R \equiv x^2 + y^2$, which never takes on the value $3 \mod 4$).

MAGMA **incorrectly asserts that Q and R are equivalent. I sent in a bug report this morning.**

Proposition 9.5.15. *Let $Q = ax^2 + bxy + cy^2$ be a primitive binary quadratic form of discriminant d (if $d < 0$ assume that $a > 0$). Then*

$$I = [\alpha, \beta] = \begin{cases} [a, \frac{b-\sqrt{d}}{2}] & \text{if } a > 0, \\ [a\sqrt{d}, (\frac{b-\sqrt{d}}{2})\sqrt{d}] & \text{if } a < 0. \end{cases}$$

is an ideal of $\mathcal{O}_K$ and $[\alpha, \beta]$ is a correctly ordered basis for I.

Example 9.5.16. Let $d = -20$ and $Q = 3x^2 + 2xy + 2y^2$. Then $I = [3, 1 - \sqrt{-5}]$. Notice that $I \neq [1 + \sqrt{-5}, 2]$, so the operations of the two propositions are not inverses before passing to equivalence classes.

Proof. All we have to do is check that $\gamma = (b - \sqrt{d})/2$ is in $\mathcal{O}_K$ and that I is correctly ordered. If $d \equiv 1 \pmod 4$ then b is odd, so $\gamma \in \mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{d})/2]$, and if $d \equiv 0 \pmod 4$ then b is even, so

$$\gamma = \frac{2b' - 2\sqrt{d'/4}}{2} \in \mathcal{O}_K = \mathbb{Z}[\sqrt{d'}].$$

It is straightforward but tedious to check that the given basis is ordered. [6] $\square$ 6

Theorem 9.5.17. *Let K be a quadratic field with discriminant d. Let $\mathcal{Q}(d)$ be the set of equivalence classes of primitive binary quadratic forms of discriminant d (if $d < 0$ include only positive definite forms in $\mathcal{Q}$). Then Propositions 9.5.12 and 9.5.15 induce a bijection between $\mathcal{Q}(d)$ and $\mathrm{Cl}^+(\mathcal{O}_K)$. In particular, $\mathcal{Q}(d)$ has the structure of finite abelian group.*

The proof is on pages 204–206 of Cohn's book. It doesn't look difficult, but it is long and tedious, so we will omit it. [7] 7

[6] Add details.

[7] But maybe add it to the book.