Math 154. Class groups for imaginary quadratic fields

Homework 6 introduces the notion of *class group* of a Dedekind domain; for a number field K we speak of the "class group" of K when we really mean that of $\mathscr{O}_K$. An important theorem later in the course for rings of integers of number fields is that their class group is *finite*; the size is then called the *class number* of the number field. In general it is a non-trivial problem to determine the class number of a number field, let alone the structure of its class group. However, in the special case of imaginary quadratic fields there is a very explicit algorithm that determines the class group. The main point is that if K is an imaginary quadratic field with discriminant $D < 0$ and we *choose* an orientation of the $\mathbf{Z}$-module $\mathscr{O}_K$ (or more concretely, we choose a square root of D in $\mathscr{O}_K$) then this choice gives rise to a natural bijection between the class group of K and the set S_D of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of positive-definite binary quadratic forms $q(x,y) = ax^2 + bxy + cy^2$ over $\mathbf{Z}$ with discriminant $4ac - b^2$ equal to $-D$.

Gauss developed "reduction theory" for binary (2-variable) and ternary (3-variable) quadratic forms over $\mathbf{Z}$, and via this theory he proved that the set of such forms q with $1 \le a \le c$ and $|b| \le a$ (and $b \ge 0$ if either $a = c$ or $|b| = a$) is a set of representatives for the equivalence classes in S_D. This set of representatives is finite because such inequalities in conjunction with the identity $4ac - b^2 = -D = |D|$ force $1 \le a \le \sqrt{|D|/3}$ (and so $|b|$ is also bounded, whence there are only finitely many such triples (a,b,c) since the identity $b^2 - 4ac = -D$ determines c once a and b are known). This gives rise to a constructive proof of the finiteness of class groups for imaginary quadratic fields.

In fact, one can even directly define a group structure on S_D that recovers the group law on the class group. In a heroic feat of mathematical brilliance, Gauss discovered this law of composition on S_D (see his *Disquisitiones*, or Chapters 12, 13, and 17 of Goldman's "The queen of mathematics: an historically motivated guide to number theory"), but beware that Gauss' conventions for discriminants and determinants are sometimes the negative of what we use today!). After the advent of algebraic number theory many years later, it was seen that the concept of class group provides the right generalization of Gauss' theory to arbitrary number fields. In this handout, we explain the construction of a natural bijection between the class group of an imaginary quadratic field with discriminant $D < 0$ and the set S_D, in case anyone might be interested; we say nothing about the direct construction of the group law on S_D (as it is an unpleasant bit of algebra to make the translation; the only satisfying approach was discovered by Bhargava).

1. Quadratic spaces

Let A be a commutative ring. A *quadratic space* over A is a pair (M,q) where M is a finite free A-module (i.e., free A-module of finite rank) and $q : M \to A$ is a *quadratic form*. That is, q is a map of sets such that

- $q(am) = a^2 q(m)$ for $m \in M$ and $a \in A$,
- the symmetric map $B_q : (m, m') \mapsto q(m+m') - q(m) - q(m')$ is A-bilinear.

We call B_q the *symmetric bilinear form associated to* q. If we choose an ordered A-basis $\{m_1, \dots, m_n\}$ of M then it is easy to check that

$$q(\sum x_i m_i) = \sum_{\{i,j\}} c_{ij} x_i x_j \tag{1}$$

(a sum over *unordered pairs* $\{i,j\}$) with $c_{ii} = q(m_i)$ for all i and $c_{ij} = c_{ji} = B_q(m_i, m_j)$ for $i \ne j$. Likewise, we have

$$B_q(\sum x_i m_i, \sum y_j m_j) = \sum_{(i,j)} c_{ij} x_i y_j \tag{2}$$

(a sum over *ordered pairs* (i,j)). In the special case that A is a $\mathbf{Z}[1/2]$-algebra, it is readily verified that $q \mapsto B_q$ and $B \mapsto (m \mapsto B(m,m)/2)$ are inverse bijections between the set of quadratic forms on M and the set of symmetric A-bilinear forms on M. Of course, $A = \mathbf{Z}$ is not a $\mathbf{Z}[1/2]$-algebra!

An *isomorphism* $(M,q) \simeq (M',q')$ is an A-linear isomorphism $f : M \simeq M'$ such that $q' \circ f = q$. The explicit coordinatization (1) describes an isomorphism of a quadratic space (M,q) onto one whose underlying A-module is $A^{\oplus n}$. The concept of a quadratic space of the form $(A^{\oplus n}, q)$ is just another name for the concept of an n-variable quadratic form $q(X_1, \dots, X_n) = \sum c_{ij} X_i X_j$ having coefficients in A.

For any quadratic space (M, q) over a ring A, the *discriminant* of q is $\mathrm{disc}(q) = \det(c_{ij})$ where (c_{ij}) is the symmetric matrix describing B_q with respect to a choice of A-basis of M as in (2); this notion is well-defined in A up to multiplication by the square of a unit (so the principal ideal $\mathrm{disc}(q)A$ is well-defined). In particular, it is well-defined to say whether or not $\mathrm{disc}(q)$ is a unit. If A is a domain with fraction field F then $\mathrm{disc}(q) \neq 0$ (that is, $\mathrm{disc}(q) \in F^{\times}$) if and only if B_q is a non-degenerate F-bilinear form when expressed in coordinates arising from an A-basis of M (in which case we say that q is *non-degenerate*). If $A = \mathbf{Z}$ then $\mathrm{disc}(q) \in \mathbf{Z}$ is a well-defined element because the only square unit in $\mathbf{Z}$ is 1.

If $A = \mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{R}$ then it makes sense to say whether or not $\mathrm{disc}(q)$ is positive or negative (if it is nonzero). Also, using the dictionary for passing between quadratic forms and bilinear forms we see that if $A = \mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{R}$ then the symmetric bilinear form B_q is positive-definite (resp. negative-definite) if and only if $q(m) > 0$ (resp. $q(m) < 0$) for all nonzero $m \in M$; we say that q is *positive-definite* or *negative-definite* accordingly.

Example 1.1. Let $A = \mathbf{Z}$ and let $M = \mathscr{O}_K$ be the ring of integers of a number field. Let r_1 be the number of embeddings of K into $\mathbf{R}$ and r_2 the number of conjugate pairs of non-real embeddings of K into $\mathbf{C}$. Let $q_K(m) = \mathrm{Tr}_{K/\mathbf{Q}}(m^2)$. It can be shown that the associated bilinear form B_{q_K} has signature $(r_1 + r_2, r_2)$ over $\mathbf{R}$ and so it is positive-definite over $\mathbf{Z}$ if and only if $r_2 = 0$, which is to say that all $\mathbf{C}$-embeddings of K land in $\mathbf{R}$ (one then says K is a totally real field).

Before stating the following lemma, we recall that for any commutative ring A, the "general linear group" $\mathrm{GL}_n(A)$ over A is the group of invertible $n \times n$ matrices with entries in A. (By Cramer's formula and the multiplicativity of determinants, these are the $n \times n$ matrices over A whose determinants lies in $A^{\times}$.) Likewise, the "special linear group" $\mathrm{SL}_n(A)$ is the group of such matrices whose determinant is 1.

Lemma 1.2. *Two quadratic spaces $(A^{\oplus n}, q)$ and $(A^{\oplus n}, q')$ are isomorphic if and only if there exists $[T] \in \mathrm{GL}_n(A)$ such that $q' \circ T = q$, where $T : A^{\oplus n} \simeq A^{\oplus n}$ is the unique A-linear automorphism with matrix $[T]$.*

This elementary lemma (whose proof we leave to the reader) translates the problem of classifying isomorphism classes of rank-n quadratic spaces over A into the problem of classifying n-variable quadratic forms over A up to change of coordinates by a matrix in $\mathrm{GL}_n(A)$ (or, as we shall say, up to $\mathrm{GL}_n(A)$-*equivalence*). In practice for $A = \mathbf{Z}$ it is interesting to consider the restricted class of coordinate changes by matrices in $\mathrm{SL}_n(\mathbf{Z})$, which is called $\mathrm{SL}_n(\mathbf{Z})$-*equivalence*. This restricted notion of equivalence can be interpreted as a coordinatized version of the study of isomorphism classes of *oriented* quadratic spaces (M, q) over $\mathbf{Z}$ (that is, a choice is made among the two equivalence classes of ordered $\mathbf{Z}$-bases of M under the equivalence relation of having change of basis matrix with determinant 1 rather than -1).

Example 1.3. If A is a $\mathbf{Z}[1/2]$-algebra, then by inductively "completing the square" to remove variables, any quadratic space over A can be diagonalized (that is, $q(x_1, \dots, x_n) = \sum c_i x_i^2$) with respect to a suitable basis.

If $M = \mathbf{Z}^{\oplus 2}$ and

$$q(x, y) = ax^2 + bxy + cy^2$$

with respect to the standard basis of M then one checks that $\mathrm{disc}(q) = 4ac - b^2$. In this binary case it is straightforward to check that $q(x, y)$ is positive-definite if and only if $\mathrm{disc}(q) > 0$ and $a, c > 0$.

There is an *enormous* difference between isomorphism of quadratic spaces over a domain A and over the fraction field of A. For example, the quadratic forms $x^2 + 82y^2$ and $2x^2 + 41y^2$ over $\mathbf{Z}$ both have the same discriminant and give rise to isomorphic quadratic spaces (of dimension 2) over $\mathbf{Q}$ but the associated quadratic spaces over $\mathbf{Z}$ are *not isomorphic* (which is not at all obvious).

2. Quadratic spaces attached to imaginary quadratic fields

Let $A = \mathbf{Z}$ and let $M = \mathscr{O}_K$ be the ring of integers of a *quadratic* field K. Another quadratic form on $\mathscr{O}_K$ (in addition to the trace form in Example 1.1 that one has for any number field) is the norm-form

$$\alpha \mapsto \mathrm{N}_{K/\mathbf{Q}}(\alpha) = \alpha\overline{\alpha} \in \mathbf{Z}.$$

The associated bilinear form is

$$(\alpha, \beta) \mapsto \alpha\overline{\beta} + \beta\overline{\alpha} = \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\overline{\beta}) = \mathrm{Tr}_{K/\mathbf{Q}}(\beta\overline{\alpha}).$$

Whereas the trace form is positive-definite for a real quadratic field and is indefinite for an imaginary quadratic field, the situation is "reversed" for the norm form: it is positive-definite in the imaginary quadratic case and is indefinite in the real quadratic case! Indeed, to check this we may work over $\mathbf{Q}$, and the norm-form in suitable coordinates on K is $x^2 - Dy^2$ where D is the discriminant of $K/\mathbf{Q}$. This is positive-definite for $D < 0$ and indefinite for $D > 0$.

A fundamental example is this:

Example 2.1. Let I be a nonzero ideal in the ring of integers $\mathscr{O}_K$ of a quadratic field K. For each nonzero $\alpha \in I$ we have $(\alpha) \subseteq I$ and hence $(\alpha) = IJ$ for some nonzero ideal $J \subseteq \mathscr{O}_K$. Thus, $\mathrm{N}(I) = [\mathscr{O}_K : I]$ divides $\mathrm{N}((\alpha)) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$, and so $\mathrm{N}(I)$ divides $\mathrm{N}_{K/\mathbf{Q}}(\alpha) \in \mathbf{Z}$; of course, the same conclusion holds for $\alpha = 0$. Hence, we get a $\mathbf{Z}$-valued scaled version of the norm form $q_I : I \to \mathbf{Z}$ via $q_I(x) = \mathrm{N}_{K/\mathbf{Q}}(x)/\mathrm{N}(I)$. Note that q_I is positive-definite in the imaginary quadratic case, but it is indefinite in the real quadratic case.

Our interest in this construction is due to:

Theorem 2.2. *If K is* imaginary quadratic *then the isomorphism class of the positive-definite quadratic space (I, q_I) only depends on the ideal class $[I] \in \mathrm{Cl}(\mathscr{O}_K)$.*

Proof. For a nonzero ideal I' in $\mathscr{O}_K$ we have $[I] = [I']$ if and only if $I' = cI$ for some $c \in K^\times$. If K is imaginary quadratic then by positive-definiteness of the norm form and the general equality

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = \mathrm{N}(\alpha\mathscr{O}_K)$$

for nonzero $\alpha \in \mathscr{O}_K$ we may use multiplicativity of both $\mathrm{N}_{K/\mathbf{Q}}$ and the ideal-norm to deduce that the isomorphism of $\mathbf{Z}$-modules $I \simeq I'$ induced by multiplication by c carries q_I on I over to the quadratic form

$$\xi \mapsto \frac{\mathrm{N}_{K/\mathbf{Q}}(\xi/c)}{\mathrm{N}(I)} = \frac{\mathrm{N}_{K/\mathbf{Q}}(\xi)}{\mathrm{N}_{K/\mathbf{Q}}(c)\mathrm{N}(I)} = \frac{\mathrm{N}_{K/\mathbf{Q}}(\xi)}{\mathrm{N}(c\mathscr{O}_K)\mathrm{N}(I)} = q_{cI}(\xi) = q_{I'}(\xi)$$

on I' (as an intermediate step we write $c = \alpha'/\alpha$ for nonzero elements $\alpha, \alpha' \in \mathscr{O}_K$). Hence, $(I, q_I) \simeq (I', q_{I'})$ as quadratic spaces. ∎

To establish an analogue of the preceding theorem for real quadratic fields (using indefinite quadratic spaces), we have to use the *narrow class group*. To define this, let F be a number field and let $\mathscr{I}_F$ be the group of fractional ideals of $\mathscr{O}_F$ and let P_F be the subgroup of principal nonzero fractional ideals. The ordinary class group of F is $\mathrm{Cl}(F) = \mathscr{I}_F/P_F$. The subgroup $P_F^+ \subseteq P_F$ is the group of principal nonzero fractional ideals that admit a generator $\xi \in F^\times$ with the property that ξ has positive image under every embedding of F into $\mathbf{R}$; when F is a totally real field (such as a real quadratic field), such elements are called *totally positive*. By squaring we see that the quotient group P_F/P_F^+ is 2-torsion with size at most 2^{r_1}, where r_1 is the number of embeddings of F into $\mathbf{R}$. The *narrow class group* of F is defined to be $\mathrm{Cl}^+(F) = \mathscr{I}_F/P_F^+$, so there is a surjection $\mathrm{Cl}^+(F) \twoheadrightarrow \mathrm{Cl}(F)$ with finite kernel. If F has no embeddings into $\mathbf{R}$ (such as an imaginary quadratic field) then the narrow class group of F coincides with the ordinary class group of F.

For a real quadratic field K, if an element $c \in K^\times$ is totally positive then obviously $\mathrm{N}_{K/\mathbf{Q}}(c) = c\overline{c} \in \mathbf{Q}^\times$ is positive. Conversely, if $c \in K^\times$ satisfies $\mathrm{N}_{K/\mathbf{Q}}(c) > 0$ then the images of c and $\overline{c}$ have the same sign under each embedding into $\mathbf{R}$. Since there are only two embeddings and conjugation on K interchanges these embeddings it follows that either c is totally positive or $-c$ is totally positive. The equality $c\mathscr{O}_K = (-c)\mathscr{O}_K$ of principal fractional ideals therefore ensures that two nonzero fractional ideals I and I' represent the same class in $\mathrm{Cl}^+(K)$ if and only if $I' = cI$ for $c \in K^\times$ satisfying $\mathrm{N}_{K/\mathbf{Q}}(c) > 0$. Since any $c \in K^\times$ can be expressed as a ratio α/α' with nonzero $\alpha, \alpha' \in \mathscr{O}_K$ and α' totally positive (for example, α' a square), it follows that the method of proof of Theorem 2.2 easily adapts to yield:

Theorem 2.3. *If K is real quadratic then the isomorphism class of the indefinite quadratic space (I, q_I) only depends on the narrow ideal class $[I] \in \mathrm{Cl}^+(K)$.*

Of course, Theorem 2.2 and Theorem 2.3 admit a common formulation via the narrow class group since $\mathrm{Cl}^+(K) = \mathrm{Cl}(K)$ for imaginary quadratic K. Let us carry out one important calculation for the quadratic spaces (I, q_I) associated to nonzero ideals in the ring of integers of a quadratic field (either real or imaginary quadratic).

Lemma 2.4. *Let I be a nonzero ideal in the ring of integers $\mathscr{O}_K$ of a quadratic field K with discriminant D. The discriminant of q_I is D.*

Proof. Since $\mathscr{O}_K$ has $\mathbf{Z}$-basis $\{1, (D+\sqrt{D})/2\}$, it is trivial to calculate a matrix for $B_{q_{\mathscr{O}_K}}$ and to check that its determinant is D. Thus, $\mathrm{disc}(q_I) = D$ if $I = \mathscr{O}_K$. Hence, it remains to show $\mathrm{disc}(q_I) = \mathrm{disc}(q_{\mathscr{O}_K})$ for any nonzero ideal I in $\mathscr{O}_K$. By the definition of q_I, the restriction $q_{\mathscr{O}_K}|_I$ is $\mathrm{N}(I) \cdot q_I$.

In general, if (M, q) is a quadratic space over $\mathbf{Z}$ and $M' \subseteq M$ is a sublattice of index n then the quadratic space $(M', q|_{M'})$ has discriminant $n^2 \mathrm{disc}(q)$, as follows from the structure theorem for modules over a PID and standard calculations for the behavior of the matrix of a bilinear form with respect to a change of basis (working over $\mathbf{Q}$, say, since M' and M generate the same $\mathbf{Q}$-vector space). Thus, $\mathrm{N}(I) \cdot q_I$ has discriminant $[\mathscr{O}_K : I]^2 \mathrm{disc}(q_{\mathscr{O}_K}) = \mathrm{N}(I)^2 \mathrm{disc}(q_{\mathscr{O}_K})$. However, it is also obvious that for any $a \in \mathbf{Z}$ and any quadratic space (M, q) over $\mathbf{Z}$, we have $\mathrm{disc}(aq) = a^2 \mathrm{disc}(q)$. Hence, $\mathrm{N}(I) \cdot q_I$ also has discriminant $\mathrm{N}(I)^2 \mathrm{disc}(q_I)$. We therefore obtain

$$\mathrm{N}(I)^2 \mathrm{disc}(q_{\mathscr{O}_K}) = \mathrm{N}(I)^2 \mathrm{disc}(q_I),$$

so indeed q_I and $q_{\mathscr{O}_K}$ have the same discriminant. ■

3. Orders and rank-2 quadratic spaces over $\mathbf{Z}$

For a quadratic field K with discriminant D and any narrow ideal class $c \in \mathrm{Cl}^+(K)$ we have attached a non-degenerate quadratic space (I, q_I) with discriminant D, with I any nonzero ideal of $\mathscr{O}_K$ representing the narrow ideal class c, and the isomorphism class of this quadratic space only depends on the narrow ideal class c of I. We now wish to show that each such quadratic space "knows" the quadratic ring $\mathscr{O}_K$. More specifically, we claim that for any rank-2 quadratic space (M, q) over $\mathbf{Z}$ such that q is non-vanishing away from the origin we may naturally associate a quadratic ring. Note that the condition on q rules out examples such as $q(x, y) = xy$ but it permits indefinite examples such as $q(x, y) = x^2 + Dy^2$.

Example 3.1. To motivate our construction, consider the special case when M is a nonzero ideal I in the ring of integers of a quadratic field K (so $M_{\mathbf{Q}} = K$) and q is the form $q_I(\alpha) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)/\mathrm{N}(I)$. Let $\alpha \mapsto \alpha^*$ denote the nontrivial automorphism of K, so the corresponding $\mathbf{Q}$-valued bilinear form B on $M_{\mathbf{Q}} = K$ is

$$B(x, y) = q_I(x + y) - q_I(x) - q_I(y) = \frac{(x + y)(x + y)^* - xx^* - yy^*}{\mathrm{N}(I)} = \frac{xy^* + yx^*}{\mathrm{N}(I)} = \frac{\mathrm{Tr}_{K/\mathbf{Q}}(xy^*)}{\mathrm{N}(I)}.$$

In particular, for any $\alpha \in M_{\mathbf{Q}} = K$, the operator $m_\alpha : x \mapsto \alpha x$ has B_q-adjoint $m_\alpha^\dagger$ equal to the multiplication operator m_{α^*} since $B_q(\alpha x, y) = B_q(x, \alpha^* y)$. Hence,

$$m_\alpha + m_\alpha^\dagger = m_{\alpha + \alpha^*} = m_{\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)} = \mathrm{Tr}(m_\alpha) \cdot 1_M.$$

We conclude that $m_\alpha^\dagger \in \mathrm{End}_{\mathbf{Z}}(M)$ and $m_\alpha + m_\alpha^\dagger = \mathrm{Tr}(m_\alpha) \cdot 1_M$. This property of m_α will point the way toward reconstructing the ring of integers of K from the quadratic space.

Let (M, q) be a quadratic space over $\mathbf{Z}$ with M of rank 2 and assume $q(m) \neq 0$ for all $m \neq 0$. (The examples we have in mind are (I, q_I) for a nonzero ideal I in the ring of integers of a quadratic field K.) Let $D = \mathrm{disc}(q)$, so $D \neq 0$. Let $(M_{\mathbf{Q}}, q_{\mathbf{Q}})$ denote the associated quadratic space over $\mathbf{Q}$. Since the associated quadratic space over $\mathbf{Q}$ is non-degenerate, for any $f \in \mathrm{End}_{\mathbf{Q}}(M_{\mathbf{Q}})$ we get an adjoint $f^\dagger \in \mathrm{End}_{\mathbf{Q}}(M_{\mathbf{Q}})$ with respect to the $\mathbf{Z}$-bilinear form $B_q(m, m') = q(m + m') - q(m) - q(m')$ on M that is perfect on $M_{\mathbf{Q}}$. Example 3.1 leads us to consider the associative ring

$$A = A(M, q) = \{f \in \mathrm{End}_{\mathbf{Z}}(M) \,|\, f^\dagger = \mathrm{Tr}(f) \cdot 1_M - f \in \mathrm{End}_{\mathbf{Z}}(M)\} \subseteq \mathrm{End}_{\mathbf{Z}}(M) \simeq \mathrm{Mat}_{2\times 2}(\mathbf{Z})$$

intrinsically attached to the quadratic space (M, q). (An equivalent condition on f is that $f^\dagger \in \mathrm{End}_{\mathbf{Z}}(M)$ and $f + f^\dagger = \mathrm{Tr}(f) \cdot 1_M$.) To see that $A(M, q)$ is a subring of $\mathrm{End}_{\mathbf{Z}}(M)$, note that it is clearly a $\mathbf{Z}$-submodule that contains $\mathbf{Z}$ and so it is enough to check the stability under composition after extending scalars to an algebraic closure $\overline{\mathbf{Q}}$. Over $\overline{\mathbf{Q}}$ we may put the perfect bilinear form B_q into the standard diagonal form $x_1y_1+x_2y_2$ with respect to which $f \rightsquigarrow f^\dagger$ is just matrix transpose, so the problem becomes a trivial calculation. Observe also that if $f \in A(M,q)$ then $q \circ f = \det(f) \cdot q$ because $B_q \circ (f \times f) = \det(f) \cdot B_q$, as we see via the calculation:

$$\begin{aligned} B_q(f(m), f(m')) = B_q((f^\dagger \circ f)(m), m') &= B_q(((\mathrm{Tr}(f) \cdot 1_M - f) \circ f)(m), m') \\ &= B_q((\mathrm{Tr}(f) \cdot f - f^2)(m), m') \\ &= B_q((\det f) \cdot m, m') \\ &= (\det f) \cdot B_q(m, m') \end{aligned}$$

because $f^2 - \mathrm{Tr}(f)f + \det f = 0$ by Cayley–Hamilton. We shall call $A(M,q)$ the *twisted endomorphism algebra* of the quadratic space (M,q).

Theorem 3.2. *The ring $A(M,q)$ is a commutative domain with rank 2 over $\mathbf{Z}$, so it is an order in a quadratic field. The field is imaginary quadratic if $D > 0$ and real quadratic if $D < 0$.*

Proof. If $f'f = 0$ then $\det(f'f) \cdot q = 0$. Since $q \neq 0$, we must have $\det(f') = 0$ or $\det(f) = 0$. Hence, to show that $A = A(M,q)$ is a (perhaps non-commutative) domain it suffices to show that if $f \in A$ satisfies $\det(f) = 0$ then $f = 0$. We have $q \circ f = 0$, yet $q(m) \neq 0$ for all $m \neq 0$. Hence, $f = 0$. We conclude that the $\mathbf{Q}$-algebra $A_{\mathbf{Q}}$ arising from A is a finite-dimensional associative $\mathbf{Q}$-algebra in which products of nonzero elements are nonzero.

Let R be an associative ring equipped with a ring homomorphism $k \to R$ from a field k such that k lands in the center of R and $\dim_k R$ is finite. For any $r \in R$ such that left multiplication $\ell_r : x \mapsto rx$ is injective, linear algebra forces this map to be an isomorphism and so there is a unique $r' \in R$ satisfying $rr' = 1$. The k-linear map ℓ_r is therefore a left-inverse to the k-linear map $\ell_{r'}$, so by linear algebra it is also a right-inverse. That is, $r'r = 1$. Hence, elements of R that are not zero-divisors with respect to left multiplication must have a two-sided inverse, and likewise for elements that are not zero-divisors with respect to right multiplication. In particular, if all nonzero elements of R are not zero divisors then R is a division algebra (i.e., an associative ring in which all nonzero elements admit a 2-sided multiplicative inverse).

Returning to our original setup, we conclude that $A_{\mathbf{Q}}$ is a division algebra over $\mathbf{Q}$ and it is contained in a 2×2 matrix algebra $\mathrm{End}_{\mathbf{Q}}(M_{\mathbf{Q}})$ over $\mathbf{Q}$. Since the matrix algebra is not a division algebra, we conclude that $A_{\mathbf{Q}}$ has dimension at most 3 over $\mathbf{Q}$. We now rule out the case of dimension 3. (It is a general fact that a division algebra with finite dimension over its center has square dimension over its center, which would rule out the possibility $\dim_{\mathbf{Q}} A_{\mathbf{Q}} = 3$, but we shall avoid that deeper general fact and give a direct argument to rule out dimension 3.)

It has to be shown that inside $\mathrm{End}_{\mathbf{Q}}(M_{\mathbf{Q}}) \simeq \mathrm{Mat}_{2\times 2}(\mathbf{Q})$ there is no 3-dimensional $\mathbf{Q}$-subalgebra D that is a division algebra. (There are 3-dimensional subalgebras; e.g., the subset of upper triangular matrices is such a subalgebra though it has zero-divisors.) Pick $d \in D - \mathbf{Q}$. Every 2×2 matrix satisfies a degree-2 polynomial over $\mathbf{Q}$ (by inspection or by the Cayley-Hamilton theorem), so $K := \mathbf{Q}[d] \subset D$ is a 2-dimensional $\mathbf{Q}$-subalgebra that is certainly commutative. But K has no zero-divisors since it lies inside D, so the commutative ring K of finite dimension over $\mathbf{Q}$ is a domain and thus it is a *field*. Viewing D as a K-vector space via left multiplication, $r : -\dim_K D > 1$ since $D \neq K$ (as $[K : \mathbf{Q}] = 2$ but $\dim_{\mathbf{Q}} D = 3 > 2$), yet upon choosing a K-basis of D to write $D \simeq K^r$ as K-vector spaces we see (via a $\mathbf{Q}$-basis of K) that $3 = \dim_{\mathbf{Q}} D = r[K : \mathbf{Q}] = 2r$, an absurdity. Thus, no such D exists.

We conclude that the division algebra $A_{\mathbf{Q}}$ has $\mathbf{Q}$-dimension at most 2, so it is *commutative* (since if it is larger than $\mathbf{Q}$ then it is generated by a single element outside $\mathbf{Q}$ for dimension reasons); i.e., it is a field K with degree at most 2 over $\mathbf{Q}$. Hence, either $A = \mathbf{Z}$ (that is, $K = \mathbf{Q}$) or else A is an order in a quadratic field.

In order to prove that the option $A = \mathbf{Z}$ is impossible and to determine the nature of the quadratic field K, it suffices to analyze the situation after extending scalars to $\mathbf{R}$ (as the formation of the twisted endomorphism algebra is compatible with extension of scalars from $\mathbf{Z}$ to $\mathbf{Q}$ and from $\mathbf{Q}$ to $\mathbf{R}$). The sign of D is detectable over $\mathbf{R}$, so the case $D < 0$ gives rise to the indefinite quadratic form $x^2 - y^2$ and the case $D > 0$ gives rise to one of the definite quadratic forms $x^2 + y^2$ or $-x^2 - y^2$. In the definite cases over

$\mathbf{R}$ we have $q_{\mathbf{R}}(m) \neq 0$ for all nonzero $m \in M_{\mathbf{R}}$, so we may use the exact same argument as above over $\mathbf{Z}$ to see that the twisted endomorphism algebra $A_{\mathbf{R}} = K_{\mathbf{R}} \simeq \mathbf{R}[t]/(t^2 - D)$ is *still* a domain, and hence if $D > 0$ then K must be an imaginary quadratic field. In the indefinite case the involution $(x, y) \mapsto (y, x)$ is easily checked to lie in the commutative twisted endomorphism algebra over $\mathbf{R}$, so together with the central involution $(x, y) \mapsto (-x, -y)$ we obtain more than one non-trivial solution to the equation $T^2 = 1$ in the twisted endomorphism algebra over $\mathbf{R}$. Hence, in this case the twisted endomorphism algebra over $\mathbf{R}$ cannot be a domain (since if it were a domain then it would be a field and then the equation $T^2 = 1$ could not have more than one nontrivial solution). Thus, in the case $D < 0$ the field K cannot equal $\mathbf{Q}$ and cannot be imaginary quadratic, so K must be a real quadratic field. ■

Let us now revisit Example 3.1. Let K be a quadratic field with discriminant D, and let $(M, q) = (I, q_I)$ be the quadratic space associated to a nonzero ideal I of $\mathscr{O}_K$. Let A be the corresponding twisted endomorphism algebra, so A is an order in a quadratic field F. In fact, the multiplication action on I by elements of $\mathscr{O}_K$ gives rise to the adjoint operation defined by the non-trivial involution σ of K over $\mathbf{Q}$ (as the bilinear form associated to the quadratic norm form on $K = I_{\mathbf{Q}}$ over $\mathbf{Q}$ is $\mathrm{Tr}_{K/\mathbf{Q}}(x\sigma(y))$), so by the formula for $\mathrm{Tr}_{K/\mathbf{Q}}$ in terms of Galois theory we see that $\mathscr{O}_K$ is thereby embedded into the twisted endomorphism ring A of (I, q_I). This inclusion $\mathscr{O}_K \hookrightarrow A$ must be an equality since $\mathscr{O}_K$ is a maximal order in K and A is an order in a quadratic field!

By considering (I, q_I) merely as an "abstract" quadratic space (ignoring the natural inclusion of I into $\mathscr{O}_K$), it is equally natural to allow $\mathscr{O}_K$ to act on I by letting $\alpha \in \mathscr{O}_K$ act by $x \mapsto \overline{\alpha}x$. This provides an isomorphism $A \simeq \mathscr{O}_K$ that is the conjugate of the first one. Thus, for the "abstract" quadratic space (I, q_I) associated to an ideal $I \subseteq \mathscr{O}_K$ we may use the inclusion of I into $\mathscr{O}_K$ to select a *preferred* isomorphism of abstract rings $A \simeq \mathscr{O}_K$, namely the one given through the canonical action of $\mathscr{O}_K$ on I via multiplication.

In general, we can partially reverse this process in the imaginary quadratic case:

Theorem 3.3. *Let (M, q) be a rank-2 non-degenerate quadratic space over $\mathbf{Z}$ with discriminant $D \neq 0$ such that $-D \equiv 0, 1 \bmod 4$. If D is odd then assume that D is squarefree, and if D is even then assume $D = 4D_0$ for a squarefree integer D_0. Assume that q is positive-definite, so $D > 0$. The twisted endomorphism ring A associated to (M, q) is the ring of integers in an imaginary quadratic field with discriminant $-D$.*

It is important to observe that if K is an *a priori* choice of imaginary quadratic field with discriminant D then there is *not* a canonical isomorphism of A with $\mathscr{O}_K$ in Theorem 3.3. Theorem 3.2 shows that A is a commutative domain with rank 2 over $\mathbf{Z}$ and that $F = \mathrm{Frac}(A)$ is an imaginary quadratic field, but there are *two* isomorphisms of F with K, and likewise there are *two* isomorphisms of A with $\mathscr{O}_K$. There is no preferred isomorphism!

Proof. Choose a $\mathbf{Z}$-basis for M, so we identify (M, q) with a quadratic space $(\mathbf{Z}^{\oplus 2}, q_0)$ where q_0 is a binary quadratic form $q(x, y) = ax^2 + bxy + cy^2$ satisfying $b^2 - 4ac = -D$. Let $K/\mathbf{Q}$ be a splitting field for $X^2 + D$, and choose a root $\sqrt{-D} \in K$ for this quadratic polynomial. The hypotheses on D ensure that $\mathscr{O}_K$ has discriminant $-D$, and in fact $\mathscr{O}_K = \mathbf{Z}[(-D + \sqrt{-D})/2]$. Note that b and D have the same parity (since $b^2 \equiv D \bmod 4$), so

$$\frac{b - \sqrt{-D}}{2} = \frac{b - D}{2} - \frac{-D + \sqrt{-D}}{2} \in \mathscr{O}_K.$$

Also, a and c are nonzero because $b^2 - 4ac = -D < 0$.

Let $I \subseteq \mathscr{O}_K$ be the ideal generated by a and $(b - \sqrt{-D})/2$. We shall construct an isomorphism $(\mathbf{Z}^{\oplus 2}, q_0) \simeq (I, q_I)$, so A is identified with the twisted endomorphism algebra of (I, q_I), which we have seen is isomorphic to $\mathscr{O}_K$. The definition of I uses a choice of square root of $-D$ in $\mathscr{O}_K$ (or, more intrinsically, it uses an *orientation* of the $\mathbf{Z}$-module $\mathscr{O}_K$), and so this is how we are managing to pick one identification $A \simeq \mathscr{O}_K$ over another in this proof.

As a preliminary step, we claim that I has a $\mathbf{Z}$-basis given by a and $(b - \sqrt{-D})/2$. These two elements are linearly independent over $\mathbf{Z}$ (because $a \neq 0$) and they lie in I. Since these two elements generate I over

$\mathscr{O}_K$, and $\mathscr{O}_K$ is spanned over $\mathbf{Z}$ by 1 and $(-D+\sqrt{-D})/2$, it suffices to check that the elements

$$a \cdot \frac{-D+\sqrt{-D}}{2}, \quad \frac{b-\sqrt{-D}}{2} \cdot \frac{-D+\sqrt{-D}}{2} \in I$$

are in the $\mathbf{Z}$-span of a and $(b-\sqrt{-D})/2$. This is a direct calculation:

$$\frac{-D+b}{2} \cdot a + -a \cdot \frac{b-\sqrt{-D}}{2} = a \cdot \frac{-D+\sqrt{-D}}{2}, \quad c \cdot a + \frac{-D-b}{2} \cdot \frac{b-\sqrt{-D}}{2} = \frac{b-\sqrt{-D}}{2} \cdot \frac{-D+\sqrt{-D}}{2}.$$

A direct calculation with the ordered $\mathbf{Z}$-basis $\{a, (b-\sqrt{-D})/2\}$ for I also shows that the restriction of $\mathrm{N}_{K/\mathbf{Q}}$ to I is $a(ax^2+bxy+cy^2) = aq(x,y)$, and we have

$$\mathrm{N}(I) = [\mathscr{O}_K : I] = |a|$$

because $\mathscr{O}_K$ has a $\mathbf{Z}$-basis given by 1 and $(b-\sqrt{-D})/2$ and I has a $\mathbf{Z}$-basis given by a and $(b-\sqrt{-D})/2$. Since q is positive definite and $q(x,0) = ax^2$, it follows that $|a| = a$. Hence, we get an isomorphism

$$(M,q) \simeq (\mathbf{Z}^{\oplus 2}, ax^2+bxy+cy^2) \simeq (I, a^{-1}\mathrm{N}_{K/\mathbf{Q}}) = (I, q_I).$$

■

4. Bijection between class group and classes of quadratic forms

Let K be an imaginary quadratic field with discriminant $-D$ for $D > 0$. Let S_D denote the set of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of positive-definite binary quadratic forms over $\mathbf{Z}$ with discriminant D. For any nonzero ideal I in $\mathscr{O}_K$ we have constructed a positive-definite rank-2 quadratic space (I, q_I), with *extra* structure: there is a "preferred" isomorphism of $\mathscr{O}_K$ with the twisted endomorphism algebra A of the quadratic space (I, q_I).

Now consider triples (M, q, ι) with (M, q) a rank-2 positive-definite quadratic space over $\mathbf{Z}$ having discriminant D and $\iota : A \simeq \mathscr{O}_K$ an isomorphism, where A is the twisted endomorphism ring of (M, q). Such triples will be called *K-normalized* quadratic spaces over $\mathbf{Z}$ (with discriminant D). An *isomorphism* between K-normalized quadratic spaces (M, q, ι) and (M', q', ι') is an isomorphism of quadratic spaces $f : (M, q) \simeq (M', q')$ such that the induced isomorphism $A \simeq A'$ of twisted endomorphism rings is compatible with the isomorphisms $\iota : A \simeq \mathscr{O}_K$ and $\iota' : A' \simeq \mathscr{O}_K$.

Theorem 4.1. *Let Q_D be the set of isomorphism classes of rank-2 positive-definite quadratic spaces over $\mathbf{Z}$ with discriminant D, and let Q_K denote the set of isomorphism classes of K-normalized positive-definite quadratic spaces over $\mathbf{Z}$ with discriminant D. Let $Q_K \to Q_D$ be the map induced by $(M, q, \iota) \mapsto (M, q)$, "forgetting" the K-normalization structure ι.*

Let G_D denote the set of $\mathrm{GL}_2(\mathbf{Z})$-equivalence classes of positive-definite binary quadratic forms over $\mathbf{Z}$ with discriminant D, and let S_D denote the set of $\mathrm{SL}_2(\mathbf{Z})$ equivalence classes of positive-definite binary quadratic forms over $\mathbf{Z}$ with discriminant D. Let $S_D \to G_D$ be the forgetful map that expresses $\mathrm{GL}_2(\mathbf{Z})$-equivalence as a coarsening of $\mathrm{SL}_2(\mathbf{Z})$-equivalence.

1. *The natural maps of sets $Q_K \to Q_D$ and $S_D \to G_D$ are surjections with fibers of size at most 2.*
2. *Upon choosing an orientation of $\mathscr{O}_K$ as a $\mathbf{Z}$-module, there is a canonical bijection $S_D \simeq Q_K$ that is compatible with the canonical bijection $G_D \simeq Q_D$ in the sense that the diagram*

$$\begin{tikzcd} S_D \arrow[r, "\simeq"] \arrow[d] & Q_K \arrow[d] \\ G_D \arrow[r, "\simeq"'] & Q_D \end{tikzcd}$$

commutes, where the bottom map is the canonical bijection as in Lemma 1.2.

Proof. By Theorem 3.3, any rank-2 positive-definite quadratic space (M, q) over $\mathbf{Z}$ with discriminant D admits a K-normalized structure. Thus, the map $Q_K \to Q_D$ is surjective. This map has fibers with size at most 2 because there are exactly two isomorphisms from $A(M, q)$ to $\mathscr{O}_K$. (A fiber may have size 1 in case there is an automorphism of the quadratic space (M, q) that induces conjugation on $A(M, q)$; this will correspond to $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes that happen to also be $\mathrm{GL}_2(\mathbf{Z})$-equivalence classes.) It is obvious that $S_D \to G_D$ is surjective, and its fibers have size at most 2 because $\mathrm{GL}_2(\mathbf{Z})/\mathrm{SL}_2(\mathbf{Z}) = \mathbf{Z}^\times/(\mathbf{Z}^\times)^2 = \mathbf{Z}^\times$ has order 2.

Fix an orientation of $\mathscr{O}_K$ as a $\mathbf{Z}$-module, so this selects a preferred choice of $\sqrt{-D} \in \mathscr{O}_K$ (namely, the ordered $\mathbf{Q}$-basis $\{1, \sqrt{-D}\}$ of K rather than $\{1, -\sqrt{-D}\}$ is in the preferred equivalence classes of ordered bases, as specified by the orientation). We now define the map of sets $S_D \to Q_K$ by using this square root of $-D$ in $\mathscr{O}_K$. Pick an element $s \in S_D$, and choose a representative positive-definite binary quadratic form $q(x, y) = ax^2 + bxy + cy^2$ with discriminant $4ac - b^2$ equal to D. Since $b^2 - 4ac = -D < 0$, we have $a, c \neq 0$. Let I be the ideal in $\mathscr{O}_K$ generated by a and $(b - \sqrt{-D})/2$. We have seen in the proof of Theorem 3.3 that (I, q_I) as a quadratic space is isomorphic to $(\mathbf{Z}^{\oplus 2}, q)$, and there is a *canonical* isomorphism ι_I from twisted endomorphism ring of (I, q_I) to $\mathscr{O}_K$.

We consider the K-normalized triple (I, q_I, ι_I) as giving rise to an element in Q_K, and we claim that this isomorphism class only depends on q up to $\mathrm{SL}_2(\mathbf{Z})$-equivalence (and hence the isomorphism class of (I, q_I, ι_I) in Q_K only depends on the initial choice of element $s \in S_D$ and not on the representative quadratic form q). It is unpleasant to work by hand with an arbitrary change of coordinates on q by an element of $\mathrm{SL}_2(\mathbf{Z})$, so to check that invariance under $\mathrm{SL}_2(\mathbf{Z})$-equivalence on q we recall the standard fact that $\mathrm{SL}_2(\mathbf{Z})$ is generated by the two elements corresponding to the substitutions

$$(x, y) \mapsto (y, -x), \ \ (x, y) \mapsto (x, x + y).$$

Applying the preceding general construction "$q \mapsto (I, q_I, \iota_I)$" to the two quadratic forms

$$q'(x, y) = q(y, -x) = cx^2 - bxy + ay^2, \ \ q''(x, y) = q(x, x + y) = (a + b + c)x^2 + (b + 2c)xy + cy^2$$

in the $\mathrm{SL}_2(\mathbf{Z})$-equivalence class of q gives K-normalized triples $(I', q_{I'}, \iota_{I'})$ and $(I'', q_{I''}, \iota_{I''})$, and it suffices to prove that the ideal classes $[I'], [I''] \in \mathrm{Cl}(K)$ coincide with $[I]$. Indeed, once we have such an equality of ideal classes then we can argue as in the proof of of Theorem 3.3 to see that the associated quadratic spaces $(I', q_{I'})$ and $(I'', q_{I''})$ are then isomorphic to (I, q_I) via multiplication by a suitable element of $K^\times$, and such a multiplication isomorphism respects the $\mathscr{O}_K$-actions on all three ideals and hence respects the ι's as well!

It is unpleasant to prove by hand that $[I] = [I']$ and $[I''] = [I]$ by finding elements of $K^\times$ that scale one ideal to the other. We shall instead use a slightly indirect criterion that is available *only* for quadratic fields: if J and J' are two nonzero ideals in $\mathscr{O}_K$ then $[J] = [J']$ if and only if $J'\overline{J}$ is principal. Let us briefly digress to verify this criterion; it says that $[\overline{J}]$ and $[J]$ are inverse ideal classes, and to prove this general claim it suffices to check that $J\overline{J}$ is principal. This principality assertion is visibly "multiplicative" in J, so by unique factorization it suffices to treat the case when $J = \mathfrak{p}$ is a *prime* ideal. Let p be the prime of $\mathbf{Z}$ beneath $\mathfrak{p}$. If p is inert in K then $\mathfrak{p} = p\mathscr{O}_K$ is already principal, so $\mathfrak{p}\overline{\mathfrak{p}} = p^2\mathscr{O}_K$. If p is split in K then $\mathfrak{p}\overline{\mathfrak{p}} = p\mathscr{O}_K$ is again principal. Finally, if p is ramified in K then $\mathfrak{p}$ is the unique prime of $\mathscr{O}_K$ over p and hence $\overline{\mathfrak{p}} = \mathfrak{p}$. Hence, in the ramified case $\mathfrak{p}\overline{\mathfrak{p}} = \mathfrak{p}^2 = p\mathscr{O}_K$ is again principal.

Returning to our initial situation, it suffices to check that the ideals $I\overline{I'}$ and $I\overline{I''}$ are principal. Since I is generated by a and $(b - \sqrt{-D})/2$ while $\overline{I'}$ is generated by c and $(-b + \sqrt{-D})/2 = -(b - \sqrt{-D})/2$, it follows that $I\overline{I'}$ is the principal ideal generated by $(b - \sqrt{-D})/2$ because

$$ac = \frac{b^2 + D}{4} = \frac{b + \sqrt{-D}}{2} \cdot \frac{b - \sqrt{-D}}{2}.$$

Slightly more tricky is the study of $I\overline{I''}$, but one can check that $a(a + b + c) \in I\overline{I''}$ is the norm of $a + (b - \sqrt{-D})/2 \in \mathscr{O}_K$. Some simple algebra shows that this latter element in fact is a principal generator of $I\overline{I''}$. Hence, the procedure $q \mapsto (I, q_I, \iota_I)$ as given above does in fact provide a well-defined map $S_D \to Q_K$ that lies over the bijection $G_D \to Q_D$. This gives the commutative diagram in (2), except that we need to check that the top side is a bijection.

For any representative $q(x, y) = ax^2 + bxy + cy^2$ as above, the form $q'(x, y) = q(x, -y) = ax^2 - bxy + cy^2$ is in the $\mathrm{GL}_2(\mathbf{Z})$-equivalence class of q and the class in Q_K associated to q' is clearly $(\overline{I}, q_{\overline{I}}, \iota_{\overline{I}})$. Thus, by (1) we conclude that the map $S_D \to Q_K$ is surjective. For injectivity, we need to recover the $\mathrm{SL}_2(\mathbf{Z})$-equivalence class of a positive-definite q from the isomorphism class of the associated K-normalized triple (I, q_I, ι_I).

Since $S_D \to Q_K$ is surjective, every K-normalized triple is isomorphic to one of the form (I, q_I, ι_I) for a nonzero ideal I in $\mathscr{O}_K$, and isomorphisms among triples of this latter type are given by $K^\times$-scalings. The orientation on $\mathscr{O}_K$ determines an orientation on each such I (since I and $\mathscr{O}_K$ generate the same $\mathbf{Q}$-vector space, namely K), and so among the two $\mathrm{SL}_2(\mathbf{Z})$-orbits in the principal $\mathrm{GL}_2(\mathbf{Z})$-homogenous space of choices of ordered basis of I we may distinguish the *positive* ordered bases $\{e_1, e_2\}$ (for which $e_1 \wedge e_2$ is positive with respect to the orientation) from the *negative* ordered bases.

For any $\xi \in K^\times$, multiplication by ξ on K has determinant $\mathrm{N}_{K/\mathbf{Q}}(\xi) > 0$ (by the *definition* of $\mathrm{N}_{K/\mathbf{Q}}$) and such positivity implies that this action of $K^\times$ preserves the orientation. Hence, for each K-normalized triple (M, q, ι) we may use *any* isomorphism $\phi : (M, q, \iota) \simeq (I, q_I, \iota_I)$ to define an orientation on the $\mathbf{Z}$-module M and this orientation is independent of ϕ and is preserved under the action of $A(M, q)$ on M. In the special case of the ideal $I = (a, (b - \sqrt{-D})/2)$ associated to a positive-definite quadratic form $q = ax^2 + bxy + cy^2$ with discriminant $D > 0$ we see that via the inclusion $I \hookrightarrow \mathscr{O}_K \hookrightarrow K$ the ordered basis $\{a, \frac{b-\sqrt{-D}}{2}\}$ is $-a/2$ times the ordered basis $\{1, \sqrt{-D}\}$. Since $a > 0$, it follows that the ordered basis $\{a, (b - \sqrt{-D})/2\}$ of I (with respect to which q_I is equal to q) is a *negative* $\mathbf{Z}$-basis of I. Hence, for each K-normalized triple (M, q, ι) we are led to consider the computation of q with respect to a *negative* $\mathbf{Z}$-basis of M. This is an $\mathrm{SL}_2(\mathbf{Z})$-equivalence class in S_D that only depends on the isomorphism class of (M, q, ι), and so provides a well-defined map $Q_K \to S_D$. A direct check shows that the composite map $S_D \to Q_K \to S_D$ is the identity, and hence the surjection $S_D \to Q_K$ is also injective. ■

Now we can prove the main result. Let K be an imaginary quadratic field with discriminant $D < 0$. Pick an orientation of $\mathscr{O}_K$ as a $\mathbf{Z}$-module. Of course, it is equivalent to pick an orientation of K as a $\mathbf{Q}$-module, or an orientation of the field $K_{\mathbf{R}} \simeq \mathbf{C}$ over $\mathbf{R}$. There is no preferred isomorphism $K_{\mathbf{R}} \simeq \mathbf{C}$, but nonetheless we can identify the choice of orientation with a choice of half-line in the (-1)-eigenline for the action of the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$ on $K_{\mathbf{R}}$. With this orientation chosen, we have:

Theorem 4.2. *Upon fixing a $\mathbf{Z}$-orientation of $\mathscr{O}_K$ as above, there is a canonical bijection $\mathrm{Cl}(K) \simeq S_D$ from the class group of K onto the set of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of positive-definite binary quadratic forms over $\mathbf{Z}$ with discriminant D.*

Proof. Since we have chosen an orientation, Theorem 4.1 provides a canonical bijection between S_D and the set Q_K of isomorphism classes of K-normalized triples (M, q, ι). We shall now construct a bijection between $\mathrm{Cl}(K)$ and Q_K that is *truly* canonical in the sense that it does not even require a choice of orientation on $\mathscr{O}_K$. Consider the map that carries the ideal class $[I]$ of a nonzero ideal $I \subseteq \mathscr{O}_K$ to the isomorphism class of the K-normalized triple (I, q_I, ι_I). Using the argument in the proof of Theorem 2.2, this latter isomorphism class only depends on the ideal class $[I]$, and so since every element of the class group is represented by a nonzero ideal we have defined a map of sets $\mathrm{Cl}(K) \to Q_K$. In the proof of Theorem 4.1 we saw that this map is a surjection (that is, every K-normalized triple is isomorphic to one of the form (I, q_I, ι_I) for a suitable nonzero ideal I of $\mathscr{O}_K$). Injectivity of $\mathrm{Cl}(K) \to Q_K$ is obvious because if (I, q_I, ι_I) and $(I', q_{I'}, \iota_{I'})$ are isomorphic as K-normalized spaces then the isomorphism of such triples gives an isomorphism of $\mathscr{O}_K$-modules $I \simeq I'$ and hence forces $[I] = [I']$ in the class group $\mathrm{Cl}(K)$. ■