# 8430 HANDOUT 4: IDENTIFICATION OF $\mathcal{C}(D)$ AND $\mathrm{Pic}(\mathcal{O}(D))$

PETE L. CLARK

## 1. Statement of the Fundamental Bijection

Let $D$ be a negative quadratic discriminant. If $f = ax^2 + bxy + c^2$ is primitive positive definite of discriminant $D$, then it is easy to check that $I(f) := \mathbb{Z}a + \mathbb{Z}(\frac{-b+\sqrt{D}}{2})$ is an integral ideal of $\mathcal{O}(D)$. (The formula consolidates the cases $D \equiv 0 \pmod 4$ and $D \equiv 1 \pmod 4$; in the former case, $\mathcal{O}(D) = \mathbb{Z}[\frac{\sqrt{D}}{2}]$ and in the latter case $\mathcal{O}(D) = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

For an ideal $I$ of $\mathcal{O}(D)$, we will denote its image in the ideal class monoid by $[I]$. In particular, composing the map $f \mapsto I(f)$ with the map which sends an ideal to its class, we get a map which sends a primitive, positive definite quadratic form $f$ of discriminant $D$ to the ideal class $[I(f)]$.[1] This has remarkable properties. Indeed, we have the following important and beautiful result (unlike some of the other results presented in this course, this exploits particular properties of imaginary quadratic fields):

**Theorem 1.** *(Fundamental Bijection) Consider the function which maps a primitive, positive definite quadratic form $f = ax^2 + bxy + cy^2$ to the $\mathcal{O}(D)$-ideal $I(f) = \mathbb{Z}a + \mathbb{Z}(\frac{-b+\sqrt{D}}{2})$.*
*a) The ideal $I(f)$ is invertible.*
*b) If $f$ and $f'$ are properly equivalent, $I(f)$ and $I(f')$ have equal images in $\mathrm{Pic}(\mathcal{O}(D))$, thus $I$ descends to a map $[I] : \mathcal{C}(D) \to \mathrm{Pic}(\mathcal{O}(D))$. The map $[I]$ is a **bijection**.*
*c) We have $[I(\iota(f))] = [I(ax^2 - bxy + cy^2)] = \overline{[I(f)]} = [I(f)]^{-1}$.*
*d) $f$ represents $m \in \mathbb{Z}$ iff there exists some ideal $J \in [I(f)]$ such that $N(J) = m$.*

Let us stop and record some immediate consequences.

Part c) tells us that the subset of ambiguous classes corresponds precisely to the 2-torsion subgroup $\mathrm{Pic}(\mathcal{O}(D))[2]$, hence explains why the number of ambiguous classes is always a power of 2.

Part d) gives further perspective on our problem: we saw first that if $m$ is an integer prime to $D$ such that $D$ is a square modulo $m$, then there exists an ideal $J$ of $\mathcal{O}(D)$ of norm $m$, and that the principal form $q_D$ represents $m$ iff $J$ is principal. Now we see the other part of this: if the ideal is nonprincipal, then $m$ is represented instead by some non-properly equivalent form $f'$.

[1] In the first draft of the notes I wrote the ideal class as $\overline{I(f)}$, and got all the way into the second lecture before realizing that, since in part c) of the Theorem below we want to take complex conjugates of ideals, this is unacceptably poor notation. I have tried to change all the overbars to [ ]'s except for the ones that really are complex conjugation. Please let me know if I missed any!

Moreover, if we further assume that $m = p$ is prime, we know that there exists exactly two ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ of norm $p$. Since for any inverible ideal $J$ in $\mathcal{O}(D)$ we have $J\overline{J} = (N(J))$, this means that in the Picard group $[J][\overline{J}] = 1$, i.e., the complex conjugate of $J$ represents the inverse ideal class. We conclude:

**Corollary 2.** *Let $p$ be any prime such that $(\frac{D}{p}) = 1$. Then the set of classes of quadratic forms in $\mathcal{C}(D)$ representing $p$ forms a single* ***wide*** *equivalence class: i.e., there exists $f = (a, b, c)$ representing $p$; also $\iota(f) = (a, -b, c)$ represents $p$ (widely equivalent forms represent the same integers!), and any form $f'$ representing $p$ is widely equivalent to $f$, i.e., properly equivalent to either $f$ or $\iota(f)$.*

At this point the largest missing piece of the puzzle is the **equidistribution** result claimed earlier. Namely, if we believe that for any two elements $c, c' \in \operatorname{Pic}(\mathcal{O}(D))$, the set of invertible prime ideals in $\mathcal{O}(D)$ whose class is $c$ is the same as the density of the set whose class is $c'$, then we can conclude that each of these densities is equal to $\frac{1}{h(D)}$. Combining this with the fundamental congruence further cuts down the density by a factor of 2 – this involves comparing rational primes with the pairs of primes in $\mathcal{O}(D)$ lying over them and will be considered later in full detail, of course – and then we will have that the density of the set of rational primes $p$ is precisely $\frac{1}{2h(D)}$. So we are getting close to the answer to our main question!

## 2. Preliminaries on proper ideals

In this section $K$ is a number field of degree $[K : \mathbb{Q}] = d$, with ring of integers $\mathcal{O}_K$.

### 2.1. **Order associated to a lattice.**

Let $\Lambda \subset K$ be a (full)[2] lattice: i.e.,

$$\Lambda = [x_1, \ldots, x_d] = \mathbb{Z}x_1 + \ldots + \mathbb{Z}x_d,$$

where $x_1, \ldots, x_d$ are a $\mathbb{Q}$-basis for $K$. Let

$$\mathcal{O}(\Lambda) = \{x \in K \mid x\Lambda \subset \Lambda\}.$$

It is essentially obvious that $\mathcal{O}(\Lambda)$ is a subring of $K$. More precisely, the punishment for not seeing this right away is the following:

Exercise 4.2.1: Let $R$ be a commutative ring and $\Lambda \subset (R, +)$ be a subgroup of the additive group of $R$. Show that $\mathcal{O}(\Lambda) := \{x \in R \mid x\Lambda \subset \Lambda\}$ is a subring of $R$.

What is not quite so immediate (but still not very hard) is that when $\Lambda$ is a lattice in the number field $K$, $\mathcal{O}(\Lambda)$ is finitely generated as a $\mathbb{Z}$-module, i.e., is by definition an **order** of $K$.

**Proposition 3.** *Let $\Lambda$ be a full lattice in the number field $K$.*
*a) $\mathcal{O}(\Lambda)$ is an order of $K$, and $\Lambda$ is a fractional $\mathcal{O}(\Lambda)$-ideal.*
*b) For any $\alpha \in K^\times$, we have $\mathcal{O}(\alpha\Lambda) = \mathcal{O}(\Lambda)$.*

[2]We shall not be considering any other kind, so the official name is just "lattice."

Exercise 4.2.2: Prove Proposition 5. Here are some suggestions:
(i) Observe that $\mathcal{O}(\Lambda)$ is a subring of $K$.
(ii) Using matrices as above, show that every element of $\mathcal{O}(\Lambda)$ is an integer in $K$, i.e., $\mathcal{O}(\Lambda) \subset \mathcal{O}_K$, and in particular $\mathcal{O}(\Lambda)$ is a finitely generated $\mathbb{Z}$-module.
(iii) Prove part b) by a direct calculation.
(iv) Given part b), we may rescale and assume that $\Lambda \subset \mathcal{O}_K$. Then $\Lambda$ has finite index $N$; show that $N\mathcal{O}_K \subset \mathcal{O}(\Lambda)$, so $\mathcal{O}(\Lambda)$ has full rank.

Note that part b) of Proposition 5 can be expressed in (rather erudite) words as follows: the associated order is a **homothety invariant** of the lattice. (Two lattices $\Lambda_1$, $\Lambda_2$ are homothetic if there exists $\alpha \in K^\times$ such that $\Lambda_2 = \alpha\Lambda_1$. The relation of lattice homothety is important in, "e.g.", elliptic curve theory.)

Exercise 4.2.3: Is every order $\mathcal{O}$ the order associated to some lattice $\Lambda$? [3]

## 2.2. **Proper fractional ideals.**

Now let $\mathcal{O}$ be an order in $K$, and let $I$ be a fractional ideal of $\mathcal{O}$. $I$ is in particular a lattice of $K$, so that from the previous construction we have an associated order $\mathcal{O}(I)$. But now we have an embarrassment of riches: [4] two different orders!

Exercise 4.2.4: Show that

$$\mathcal{O} \subset \mathcal{O}(I). \tag{1}$$

The best state of affairs would be to have equality in (1): $\mathcal{O} = \mathcal{O}(I)$. When this occurs we say that $I$ is a **proper** fractional ideal for $\mathcal{O}$. (Note that this has nothing to do with proper containment.)

Exercise 4.2.5: a) Show that any lattice $\Lambda$ is a proper $\mathcal{O}(\Lambda)$ ideal.
b) If $\mathcal{O} = \mathcal{O}_K$ is the maximal order, show that every fractional $\mathcal{O}$-ideal is proper.

Example: Take $K = \mathbb{Q}[\sqrt{-3}]$, $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ and $\mathfrak{p}_2 = \langle 1+\sqrt{-3}, 1-\sqrt{-3}\rangle$ the unique ideal of norm 2. Then

$$(\frac{1+\sqrt{-3}}{2}) \cdot (1+\sqrt{-3}) = \frac{1}{2}(1+2\sqrt{-3}-3) = -(1+\sqrt{-3}) \in \mathfrak{p}_2,$$

$$(\frac{1+\sqrt{-3}}{2}) \cdot (1-\sqrt{-3}) = \frac{1}{2}(1^2-(\sqrt{-3})^2) = 2 = (1+\sqrt{-3}) + (1-\sqrt{-3}) \in \mathfrak{p}_2,$$

so that $\mathcal{O}_K\mathfrak{p}_2 = \mathfrak{p}_2$ and $\mathcal{O}(\mathfrak{p}_2) = \mathcal{O}_K$ and $\mathfrak{p}_2$ is not proper.

Now let us assume that $K$ is a quadratic field and compute the order associated to an arbitrary lattice $\Lambda = [\alpha, \beta]$. Using Proposition 5b), we may as well rescale and look at the lattice

$$[1, \frac{\beta}{\alpha}] = [1, \tau];$$

---

[3] Yes, most of the exercises in this handout are trivial. I didn't have much inspiration here.

[4] I picked up this phrase $\sim$ 12 years ago from Kaplansky's *Set Theory and Metric Spaces*.

with $\tau = \frac{\beta}{\alpha}$; here the condition that $\alpha, \beta$ form a $\mathbb{Q}$-basis is equivalent to $\tau \in K \setminus \mathbb{Q}$.

**Lemma 4.** *Suppose that $K = \mathbb{Q}(\tau)$ is a quadratic field. Let $P(t) = at^2+bt+c \in \mathbb{Z}[t]$ be the unique polynomial such that $P(\tau) = 0$, $\gcd(a,b,c) = 1$, $a > 0$. Then the order associated to the lattice $[1,\tau]$ is $[1, a\tau] = \mathbb{Z}[a\tau]$. Its discriminant is*

Proof: First note that $(a\tau)^2 + ab(a\tau) + a^2c = a^2(\tau^2 + b\tau + c) = 0$, so that $a\tau$ is an algebraic integer and $\mathbb{Z}[a\tau]$ is indeed an order in $K$. Now let $\alpha \in K$ be such that $\alpha[1,\tau] \subset [1,\tau]$. This holds iff there exist integers $m, n, p, q$ such that

$$\alpha = m + n\tau, \tag{2}$$

$$\alpha\tau = p + q\tau. \tag{3}$$

Substituting (2) into (3), we get

$$p + q\tau = (m + n\tau)(\tau) = m\tau + \frac{n}{a}(-b\tau + c) = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau.$$

Thus $a \mid bn$ and $a \mid cn$, so $a | \gcd(bn, cn) = n \gcd(b,c)$; since $\gcd(a, \gcd(b,c)) = 1$, $a \mid n$ and therefore $\alpha \in \mathbb{Z}[a\tau]$.

**Theorem 5.** *For a fractional ideal $I$ in an order $\mathcal{O}$ in a* ***quadratic*** *number field $K = \mathbb{Q}(\tau)$, TFAE:*
*(i) $I$ is invertible.*
*(ii) $I$ is proper.*

Proof: (i) $\implies$ (ii): Suppose that $I$ is invertible, i.e., there exists an integral ideal $J$ such that $IJ = \mathcal{O}$. If $\alpha \in K$ is such that $\alpha I \subset I$, then

$$\alpha = \alpha \cdot 1 \in \alpha\mathcal{O} = \alpha IJ = (\alpha I)J \subset IJ = \mathcal{O},$$

so $I$ is proper.

Now let $\mathcal{O}$ be an order in the quadratic field $K$, and let $I = [\alpha, \beta] = \mathbb{Z}\alpha + \mathbb{Z}\beta$ be a proper $\mathcal{O}$-ideal. Then putting $\tau = \frac{\beta}{\alpha}$, we have $I = \alpha[1,\tau]$. Let $ax^2 + bx + c$ be the minimal polynomial of $\tau$, so Lemma 4 implies $\mathcal{O}(I) = [1, a\tau]$; since by assumption $I$ is proper, we have $\mathcal{O} = [1, a\tau]$. Let us denote the unique nontrivial automorphism of $K$ by $\alpha \mapsto \overline{\alpha}$: in the imaginary quadratic case this is usual complex conjugation; in the real case, it is not. Then we have $\overline{I} = \overline{\alpha}[1, \overline{\tau}]$; since $\overline{\tau}$ has the same minimal polynomial as $\tau$, according to Lemma 4 we have $\mathcal{O}(\overline{I}) = [1, a\overline{\tau}] = \mathbb{Z}[a\overline{\tau}] = \mathbb{Z}[a\tau] = \mathcal{O}$. Note $\tau + \overline{\tau} = \frac{-b}{a}$ and $\tau\overline{\tau} = \frac{c}{a}$, so

$$aI\overline{I} = a\alpha\overline{\alpha}[1,\tau][1,\overline{\tau}] = N(\alpha)[a, a\tau, a\overline{\tau}, a\tau\overline{\tau}]$$

$$= N(\alpha)[a, a\tau, a\tau + a\overline{\tau}, a\tau\overline{\tau}] = N(\alpha)[a, a\tau, -b, c] = N(\alpha)[1, a\tau] = N(\alpha)\mathcal{O}.$$

Therefore

$$I\overline{I} = \frac{|N(\alpha)|}{a}\mathcal{O}, \tag{4}$$

so $I$ is invertible.

Exercise 4.2.5: a) Observe (i) $\implies$ (ii) in any number field $K$.
b)$*$ Prove/disprove: for any order $\mathcal{O}$ in any number field $K$, a proper fractional $\mathcal{O}$-ideal is invertible. (Comment: I suspect this is true, but didn't have much luck

finding either a reference or a proof. Since it has the – true, but nontrivial – consequence that all fractional $\mathcal{O}_K$-ideals are invertible, it presumably it is itself not especially easy to prove.)

Next we give some – perhaps overdue – facts about the norms of proper ideals. Recall that for an ideal $I$ in an order $\mathcal{O}$ of a (possibly real) quadratic field $K$, we defined $N(I) = \#\mathcal{O}/I$ and showed that the norm of a nonzero principal ideal $(\alpha)$ is $|N(\alpha)| = |\alpha\overline{\alpha}|$, where again we are, slightly abusively in the real case, denoting the Galois conjugation on $K$ by $\alpha \mapsto \overline{\alpha}$.

**Proposition 6.** *Let $\mathcal{O}$ be an order in a quadratic field and let $I$ and $J$ be nonzero proper $\mathcal{O}$-ideals.*
*a) $N(IJ) = N(I)N(J)$.*
*b) $I\overline{I} = N(I)\mathcal{O}$.*

Proof: Step 1: If $I$ is proper and $0 \neq \alpha \in \mathcal{O}$, we show

$$N(\alpha I) = |N(\alpha)|N(I).$$

The inclusions $\alpha I \subset \alpha\mathcal{O} \subset \mathcal{O}$ give rise to an exact sequence of finite abelian groups

$$0 \to \frac{\alpha\mathcal{O}}{\alpha I} \to \frac{\mathcal{O}}{\alpha\mathcal{I}} \to \frac{\mathcal{O}}{\alpha\mathcal{O}} \to 0,$$

so that $\#\frac{\mathcal{O}}{\alpha I} = \#\frac{\mathcal{O}}{\alpha\mathcal{O}}\#\frac{\alpha\mathcal{O}}{\alpha I}$. Multiplication by $\alpha$ induces an isomorphism

$$\frac{\mathcal{O}}{I} \xrightarrow{\sim} \frac{\alpha\mathcal{O}}{\alpha I},$$

so

$$N(\alpha I) = \#\frac{\mathcal{O}}{\alpha I} = \#\frac{\mathcal{O}}{\alpha\mathcal{O}}\#\frac{\alpha\mathcal{O}}{\alpha I} = |N(\alpha)|N(I).$$

Step 2: Write $I = \alpha[1, \tau]$, so that by Lemma 4 (and using its notation), we have $\mathcal{O} = [1, a\tau]$. Evidently the lattice $[a : a\tau]$ has index $a$ in $[1 : a\tau] = \mathcal{O}$, so

$$a^2 N(I) = N(a)N(I) = N(aI) = N(\alpha a[1, \tau]) = |N(\alpha)|N(a[1, \tau]) = |N(\alpha)| \cdot a,$$

and hence

$$N(I) = \frac{|N(\alpha)|}{a}.$$

Therefore using (4) we have

$$I\overline{I} = \frac{|N(\alpha)|}{a}\mathcal{O} = N(I)\mathcal{O},$$

establishing b).

Step 3: Using b) we have

$$N(IJ)\mathcal{O} = IJ\overline{IJ} = (I\overline{I})(J\overline{J}) = (N(I)\mathcal{O})(N(J)\mathcal{O}) = N(I)N(J)\mathcal{O},$$

so that there exists a unit $u \in \mathcal{O}^\times$ such that $N(IJ) = N(I)N(J)u$. But then also $u \in \mathbb{Q}^{>0}$ and $\mathcal{O}^\times \cap \mathbb{Q}^{>0} = \{1\}$. So $N(IJ) = N(I)N(J)$.

## 3. Proof of Theorem 1

Let $f = ax^2 + bxy + cy^2$ be primitive, positive definite of discriminant $D < 0$. The roots of $f(x, 1) = ax^2 + bx + c$ are

$$\tau = \frac{-b + \sqrt{D}}{2a}, \ \overline{\tau} = \frac{-b - \sqrt{D}}{2a};$$

since $a > 0$, the imaginary part of $\tau$ is positive, i.e., $\tau$ lies in the upper halfplane. We then have

$$[a, \frac{-b + \sqrt{D}}{2}] = [a, a\tau] = a[1, \tau].$$

By Lemma 4, $a[1, \tau]$ is a proper ideal for the order $[1, a\tau]$. Let's check that this order is actually $\mathcal{O}(D)$: introduce the conductor $f$ so that $D = f^2 D_0$ – here $D_0 = \operatorname{disc}(K)$. We compute

$$a\tau = \frac{-b + \sqrt{D}}{2} = \frac{-b + f\sqrt{D_0}}{2} = -\frac{b + fD_0}{2} + f\left(\frac{D_0 + \sqrt{D_0}}{2}\right) = -\frac{b + fD_0}{2} + f\tau_K,$$

where $\tau_K = \frac{D_0 + \sqrt{D_0}}{2}$ is such that $\mathcal{O}_K = \mathbb{Z}[\tau_K]$. Since $D = f^2 D_0 = b^2 - 4ac$, $fD_0 \equiv f^2 D_0 \equiv b^2 \equiv b \pmod 2$, and thus $\frac{b + fD_0}{2} \in \mathbb{Z}$. This shows

$$[1, a\tau] = [1, f\tau_K] = \mathcal{O}(D),$$

and therefore $a[1, \tau]$ is a proper $\mathcal{O}(D)$-ideal. This proves part a) of Theorem 1.

Now let $f$ be a primitive positive definite quadratic form of discriminant $D$, with associated root $\tau$. For any matrix $A = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{Z})$, a quick calculation shows that the root $\tau'$ of the properly equivalent form $f' = A \cdot f$ is $\tau' = \frac{p\tau + q}{r\tau + s}$. Note that by a standard calculation, since $\det(A) = 1 > 0$, $\tau'$ is also in the upper half plane. Therefore

$$[1, \tau'] = [1, \frac{p\tau + q}{r\tau + s}] = \frac{1}{r\tau + s}[r\tau + s, p\tau + q] = \frac{1}{r\tau + s}[1, \tau] = \lambda[1, \tau]$$

for $\lambda = \frac{1}{r\tau + s} \in K^\times$. Therefore

$$I(f) = [a, a\tau] = a[1, \tau] = a\lambda[1, \tau'] = \frac{a\lambda}{a'}[a', a'\tau'] = \gamma I(f')$$

for $\gamma = \frac{a\lambda}{a'} \in K^\times$. In other words, if $f'$ is properly equivalent to $f$, we get an equality of classes of invertible ideals $[I(f)] = [I(f')]$.

The argument can be reversed, giving a map from invertible ideal classes to primitive quadratic forms. Suppose that $[I] \in \operatorname{Pic}(\mathcal{O}(D)$, write $I = [\alpha, \beta]$.

Exercise 4.3.1: Convince yourself this is true, i.e., given a proper fractional $\mathcal{O}(D)$-ideal $J = [\alpha, \beta]$ with $\Im(\frac{\beta}{\alpha}) > 0$, assign the quadratic form $ax^2 + bxy + cy^2$, where $at^2 + bt + c$ is the unique quadratic polynomial satisfied by $\frac{\beta}{\alpha}$ with $a > 0$ and $\gcd(a, b, c) = 1$. Precisely, you are asked to show:
a) That the proper equivalence class of $ax^2 + bxy + cy^2$ is independent of the choice of basis for $J$ and also independent under rescaling $J \mapsto \alpha J$.
b) That applying the two maps in either direction yields the identity.[5]

[5]In general, unlike Cox I prefer not to leave parts of the proof of an important result as exercises, but in this case it is truly a good exercise to get a feel for the correspondence.

As for part c), since $I(f) = a[1, \frac{-b+\sqrt{D}}{2}]$, clearly $I(\iota f) = a[1, \frac{b+\sqrt{D}}{2}]$, whereas $\overline{I(f)} = a[1, \frac{-b-\sqrt{D}}{2}] = a[1, \frac{b+\sqrt{D}}{2}]$, so $[\overline{I(f)}] = [I(\iota f)]$.

Finally, we prove part d). If $f$ represents the positive integer $m$, then (as usual) we may write $m = d^2 a$ with $a$ properly represented by $f$. By Exercise 3.4.1, $f$ is properly equivalent to $ax^2 + bxy + cy^2$. Then $f$ maps to $I(f) = a[1, \tau]$, so $N(I(f)) = a$, and then $N(dI(f)) = d^2 N(I(f)) = d^2 a = m$, so that $m$ is the norm of an ideal in the class of $I(f)$.

Conversely, suppose that there exists an ideal $J$ with $[J] = [I(f)]$ and $N(J) = m$. We may write $J = \alpha[1, \tau]$ for $\Im(\tau) > 0$, $a\tau^2 + b\tau + c = 0$, $\gcd(a, b, c) = 0$, $a > 0$. We want to show that $f$ represents $m$. We know that

$$m = N(J) = \frac{N(\alpha)}{a}.$$

But also $\alpha[1, \tau] = J \subset \mathcal{O} = [1, a\tau]$, so that

$$\alpha = p + qa\tau, \;\; \alpha\tau = r + sa\tau$$

for suitable $p, q, r, s \in \mathbb{Z}$. Then $(p + qa\tau)\tau = r + sa\tau$, and using $a\tau^2 = -b\tau - c$ we get $p = as + bq$. Therefore

$$m = \frac{N(\alpha)}{a} = \frac{1}{a}\left(p^2 - bpq + acq^2\right)$$

$$= \frac{1}{a}\left((as + bq)^2 - b(as + bq)q + acq^2\right) = \frac{1}{a}\left(a^2 s^2 + absq + acq^2\right)$$

$$= as^2 + bsq + cq^2 = f(s, q).$$

This completes the proof of Theorem 1.

### 3.1. **References.**

All of this material is taken from Part II of Cox's book, except for the idea that one can assign an order to an arbitrary lattice.[6] This seems to motivate Lemma 4, which is arguably the most important single step of the argument.

## 4. But in fact...

... this is not really the strongest possible statement of the fundamental bijection. On the ideal class side we defined the structure of an abelian group and on the quadratic forms side we defined only an inversion. Via the canonical bijection we can therefore **endow** $\mathcal{C}(D)$ with the structure of a finite abelian group – this is what N. Bourbaki liked to call **transport of structure** – but in order to compute the group law on the quadratic forms side we would have to map to ideal classes, take the product, and then map back.

There is nothing particularly wrong with this, but the fact remains that it is unnecessary: Gauss defined a group structure on $\mathcal{C}(D)$ directly, without recourse to ideal classes (and of course no one in Gauss' time thought in terms of ideal classes). Later on we will describe this "composition law" on quadratic forms, in a version due to Dirichlet.

[6] This idea is certainly not due to me. Rather, after mulling over Cox's book I remembered a similar construction from the theory of quaternion orders. So far as I am aware, the only novelties that may be present in these notes are novelties of exposition.