Chapter 17

Classes of quaternion ideals

Having investigated the structure of lattices and ideals in Chapter 16, we now turn to the study of their isomorphism classes.

17.1 ▹ Ideal classes

For motivation, let K be a quadratic number field and $S \subseteq K$ an order. We say that two invertible fractional ideals $\mathfrak{a}, \mathfrak{b} \subset K$ of S are **in the same class**, and write $\mathfrak{a} \sim \mathfrak{b}$, if there exists $c \in K^\times$ such that $c\mathfrak{a} = \mathfrak{b}$; we denote the class of a fractional ideal $\mathfrak{a}$ as $[\mathfrak{a}]$. We have $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are isomorphic as S-modules. The set $\mathrm{Cl}\, S$ of invertible fractional ideals is a group under multiplication, measuring the failure of S to be a PID. The class group $\mathrm{Cl}\, S$ is a finite abelian group, by Minkowski's *geometry of numbers*: every class in $\mathrm{Cl}\, S$ is represented by an integral ideal $\mathfrak{a} \subseteq S$ whose absolute norm is bounded (depending on S, but independent of the class), and there are only finitely many such ideals. For an introduction to orders in quadratic fields and their class numbers, with further connections to quadratic forms, see Cox [Cox89, §7].

The first treatment of isomorphism classes of quaternion ideals was given by Brandt [Bra28]. Let B be a quaternion algebra over $\mathbb{Q}$. In the consideration of classes of lattices $I \subset B$, we make a choice and consider lattices as right modules—considerations on the left are analogous, with the map $I \mapsto \bar{I}$ allowing passage between left and right. We say that lattices $I, J \subseteq B$ are **in the same right class**, and write $I \sim_{\mathsf{R}} J$, if there exists $\alpha \in B^\times$ such that $\alpha I = J$; equivalently, $I \sim_{\mathsf{R}} J$ if and only if I is isomorphic to J as right modules over $O_{\mathsf{R}}(I) = O_{\mathsf{R}}(J)$. The relation $\sim_{\mathsf{R}}$ is evidently an equivalence relation, and the class of a lattice I is denoted $[I]_{\mathsf{R}}$.

Let $O \subset B$ be an order. We define the **right class set** of O as

$$\mathrm{Cls}_{\mathsf{R}}\, O := \{[I]_{\mathsf{R}} : I \subset B \text{ invertible and } O_{\mathsf{R}}(I) = O\};$$

equivalently, $\mathrm{Cls}_{\mathsf{R}}\, O$ is the set of isomorphism classes of invertible right O-modules in B. The standard involution induces a bijection between $\mathrm{Cls}_{\mathsf{R}}\, O$ and the analogously defined left class set $\mathrm{Cls}_{\mathsf{L}}\, O$; working on the right from now on, we will often abbreviate $\mathrm{Cls}\, O := \mathrm{Cls}_{\mathsf{R}}\, O$.

J. Voight, *Quaternion Algebras*, Graduate Texts in Mathematics 288,
https://doi.org/10.1007/978-3-030-56694-4_17

Unfortunately, the class set $\mathrm{Cls}\, O$ does *not* have the structure of a group: only a pointed set, with distinguished element $[O]_{\mathsf{R}}$. One problem is the compatibility of multiplication discussed in the previous chapter. But even if we allowed products between incompatible lattices, the product need not be well-defined: the lattices IJ and $I\alpha J$ for $\alpha \in B^\times$ need not be in the same class, because of the failure of commutativity. (This is the reason we write 'Cls' instead of 'Cl', as a reminder that it is only a class *set*.) In Chapter 19, we will describe the structure that arises naturally instead: a partially defined product on classes of lattices, a *groupoid*.

In any case, using the same method of proof (geometry of numbers) as in the commutative case, we will show that there exists a constant C (depending on O) such that every class in $\mathrm{Cls}\, O$ is represented by an integral ideal $I \subseteq O$ with $\mathsf{N}(I) = \#(O/I) \leq C$. As a consequence, we have the following fundamental theorem.

Theorem 17.1.1. *Let B be a quaternion algebra over $\mathbb{Q}$ and let $O \subset B$ be an order. Then the right class set* $\mathrm{Cls}\, O$ *is finite.*

Accordingly, we call $\#\,\mathrm{Cls}\, O \in \mathbb{Z}_{\geq 1}$ the **(right) class number** of O.

Right class sets pass between orders as follows. Let $O, O' \subset B$ be orders. If $O \simeq O'$ are isomorphic as rings, then of course this isomorphism induces a bijection $\mathrm{Cls}\, O \xrightarrow{\sim} \mathrm{Cls}\, O'$. In fact, $O \simeq O'$ if and only if there exists $\alpha \in B^\times$ such that $O' = \alpha^{-1} O \alpha$ by the Skolem–Noether theorem; for historical reasons, we say that O, O' are **of the same type**.

Note that $I = O\alpha = \alpha O'$ has $O_{\mathsf{L}}(I) = O$ and $O_{\mathsf{R}}(I) = O'$ (recalling 10.2.5). With this in mind, more generally, we say that O' is **connected** to O if there exists an invertible lattice J with $O_{\mathsf{L}}(J) = O$ and $O_{\mathsf{R}}(J) = O'$, called a **connecting ideal**. Because invertible lattices are locally principal, two orders are connected if and only if they are **locally of the same type** (i.e., **locally isomorphic**). If O' is connected to O, then right multiplying by a O, O'-connecting ideal J yields a bijection

$$\begin{aligned} \mathrm{Cls}\, O &\xrightarrow{\sim} \mathrm{Cls}\, O' \\ [I]_{\mathsf{R}} &\mapsto [IJ]_{\mathsf{R}} \end{aligned} \tag{17.1.2}$$

We define the **genus** of an order $O \subset B$ to be the set $\mathrm{Gen}\, O$ of orders in B locally isomorphic to O, and the **type set** $\mathrm{Typ}\, O$ of O to be the set of R-isomorphism classes of orders in the genus of O. The map

$$\begin{aligned} \mathrm{Cls}\, O &\to \mathrm{Typ}\, O \\ [I]_{\mathsf{R}} &\mapsto \text{class of } O_{\mathsf{L}}(I) \end{aligned} \tag{17.1.3}$$

is a surjective map of sets, so the type set is finite: in other words, up to isomorphism, there are only finitely many types of orders in the genus of O. All maximal orders in B are in the same genus, so in particular there are only finitely many conjugacy classes of maximal orders in B. In this way, the right class set of O also organizes the types of orders arising from O.

The most basic question about the class number is of course its size (as a function of O). In the case of quadratic fields, the behavior of the class group depends in a significant way on whether the field is imaginary or real: for negative discriminant

$d < 0$, the Brauer–Siegel theorem provides that $\#\operatorname{Cl} S$ is approximately of size $\sqrt{|d|}$; in contrast, for positive discriminant $d > 0$, one typically sees a small class group and a correspondingly large fundamental unit, but this statement is notoriously difficult to establish unconditionally.

The same dichotomy is at play in the case of quaternion algebras, and to state the cleanest results we suppose that O is a maximal order. Let $D := \operatorname{disc} B = \operatorname{discrd}(O)$ be the discriminant of B. If B is definite, which is to say $\infty \in \operatorname{Ram} B$, then B is like an imaginary quadratic field K: the norm is positive definite. In this case, $\#\operatorname{Cls} O$ is approximately of size D, a consequence of the *Eichler mass formula*, the subject of Chapter 25. On the other hand, if B is indefinite, akin to a real quadratic field, then $\#\operatorname{Cls} O = 1$, this time a consequence of *strong approximation*, the subject of Chapter 28. Just as in the commutative case, estimates on the size of the class number use analytic methods and so must wait until we have developed the required tools.

17.2 Matrix ring

To begin, we first consider classes of ideals for the matrix ring; here, we can use methods from linear algebra before we turn to more general methods in the rest of the chapter.

17.2.1. Let R be a PID with field of fractions F, and let $B = \mathrm{M}_n(F)$. By Corollary 10.5.5, every maximal order of $B = \mathrm{M}_n(F)$ is conjugate to $\mathrm{M}_n(R)$. Moreover, every two-sided ideal of $\mathrm{M}_n(R)$ is principal, generated by an element $a \in F^\times$ (multiplying a candidate ideal by matrix units, as in Exercise 7.5(b)), so the group of fractional two-sided $\mathrm{M}_n(R)$-ideals is canonically identified with the group of fractional R-ideals, itself isomorphic to the free abelian group on the (principal) nonzero prime ideals of R.

Just as in the two-sided case, the right class set for $\mathrm{M}_n(R)$ is trivial.

Proposition 17.2.2. *Let R be a PID with field of fractions F, and let $B = \mathrm{M}_n(F)$. Let $I \subseteq B$ be an R-lattice with either $O_{\mathsf{L}}(I)$ or $O_{\mathsf{R}}(I)$ maximal. Then I is principal, and both $O_{\mathsf{L}}(I)$ and $O_{\mathsf{R}}(I)$ are maximal.*

Proof. We may suppose I is integral by rescaling by $r \in R$. Replacing I by the transpose $I^{\mathrm{t}} = \{\alpha^{\mathrm{t}} : \alpha \in I\}$ interchanging left and right orders (Exercise 10.12) if necessary, we may suppose that $O_{\mathsf{L}}(I)$ is maximal. Then, by Corollary 10.5.5, we have $O_{\mathsf{L}}(I) = \alpha^{-1}\,\mathrm{M}_n(R)\alpha$ with $\alpha \in B^\times$, so replacing I by $\alpha^{-1}I$ we may suppose $O_{\mathsf{L}}(I) = \mathrm{M}_n(R)$.

Now we follow Newman [New72, Theorem II.5]. Let $\alpha_1, \dots, \alpha_m$ be R-module generators for I. Consider the $nm \times n$ matrix $A = (\alpha_1, \dots, \alpha_m)^{\mathrm{t}}$. By row reduction over R (Hermite normal form, proven as part of the structure theorem for finitely generated modules over a PID), there exists $Q \in \mathrm{GL}_{nm}(R)$ such that $QA = (\beta, 0)^{\mathrm{t}}$ and $\beta \in \mathrm{M}_n(R)$. We will show that $I = \mathrm{M}_n(R)\beta$. Let $\nu_{11}, \dots, \nu_{1m} \in \mathrm{M}_n(R)$ be the block matrices in the top n rows of Q. Then $\beta = \nu_{11}\alpha_1 + \cdots + \nu_{1m}\alpha_m$ so $\beta \in I$ and $\mathrm{M}_n(R)\beta \subseteq I$. Conversely, let $\mu_{11}, \dots, \mu_{m1} \in \mathrm{M}_n(R)$ be the block matrices in the left n columns of $Q^{-1} \in \mathrm{GL}_{nm}(R)$. Since $Q^{-1}(\beta, 0)^{\mathrm{t}} = A$, we have $\mu_{i1}\beta = \alpha_i$ so $\alpha_i \in \mathrm{M}_n(R)\beta$ for

$i = 1, \dots, m$, thus $I \subseteq \mathrm{M}_n(R)\beta$. Therefore $I = \mathrm{M}_n(R)\beta$, and so $O_{\mathsf{R}}(I)$ is maximal (16.2.3). □

Returning to the case of quaternion algebras, we have the following corollary of Proposition 17.2.2.

Corollary 17.2.3. *Let R be a Dedekind domain and let B be a quaternion algebra over $F = \operatorname{Frac} R$. Let $I \subseteq B$ be an R-lattice with either $O_{\mathsf{L}}(I)$ or $O_{\mathsf{R}}(I)$ maximal. Then I is locally principal and both $O_{\mathsf{L}}(I)$ and $O_{\mathsf{R}}(I)$ are maximal.*

Proof. For each prime $\mathfrak{p}$ of R, we have that $R_{\mathfrak{p}}$ is a DVR and one of two possibilities: either $B_{\mathfrak{p}} \simeq \mathrm{M}_2(F_{\mathfrak{p}})$, in which case we can apply Lemma 17.2.2 to conclude $I_{\mathfrak{p}}$ is principal, or $B_{\mathfrak{p}}$ is a division algebra, and we instead apply 13.3.10 to conclude that $I_{\mathfrak{p}}$ is principal. □

17.3 Classes of lattices

For the rest of this chapter, let R be a Dedekind domain with field of fractions $F = \operatorname{Frac} R$, and let B be a simple F-algebra.

Definition 17.3.1. Let $I, J \subseteq B$ be R-lattices. We say I, J are **in the same right class**, and we write $I \sim_{\mathsf{R}} J$, if there exists $\alpha \in B^\times$ such that $\alpha I = J$.

17.3.2. Throughout, we work on the right; analogous definitions can be made on the left. When B has a standard involution, the map $I \mapsto \overline{I}$ interchanges left and right.

Lemma 17.3.3. *Let $I, J \subseteq B$ be R-lattices. Then the following are equivalent:*

(i) $I \sim_{\mathsf{R}} J$;
(ii) *I is isomorphic to J as a right module over $O_{\mathsf{R}}(I) = O_{\mathsf{R}}(J)$; and*
(iii) $(J : I)_{\mathsf{L}}$ *is a principal R-lattice.*

Proof. For (i) ⇒ (ii). If $I \sim_{\mathsf{R}} J$ then $J = \alpha I$ with $\alpha \in B^\times$, so $O_{\mathsf{R}}(J) = O_{\mathsf{R}}(I)$ and the map left-multiplication by α gives a right O-module isomorphism $I \xrightarrow{\sim} J$. Conversely, for (i) ⇐ (ii), suppose that $\phi\colon I \xrightarrow{\sim} J$ is an isomorphism of right O-modules. Then $\phi_F : I \otimes_R F = B \xrightarrow{\sim} J \otimes_R F = B$ is an automorphism of B as a right B-module. Then as in Example 7.2.14, such an isomorphism is obtained by left multiplication by $\alpha \in B^\times$, so by restriction ϕ is given by this map as well.

Next, for (i) ⇒ (iii), suppose $\alpha I = J$ with $\alpha \in B^\times$. Then

$$(J : I)_{\mathsf{L}} = \{\beta \in B : \beta I \subseteq J = \alpha I\} = \alpha O_{\mathsf{L}}(I)$$

is principal. The converse follows similarly. □

The relation $\sim_{\mathsf{R}}$ defines an equivalence relation on the set of R-lattices in B, and the equivalence class of an R-lattice I is denoted $[I]_{\mathsf{R}}$. If I is an invertible R-lattice, then every lattice in the class $[I]_{\mathsf{R}}$ is invertible and we call the class **invertible**.

In view of Lemma 17.3.3(b), we organize classes of lattices by their right orders. Let $O \subset B$ be an R-order.

Definition 17.3.4. The **(right) class set** of O is

$$\mathrm{Cls}_{\mathsf{R}}\, O := \{[I]_{\mathsf{R}} : I \text{ an invertible right fractional } O\text{-ideal}\}.$$

In view of 17.3.2, we will soon abbreviate $\mathrm{Cls}\, O := \mathrm{Cls}_{\mathsf{R}}\, O$ and drop the subscript $_{\mathsf{R}}$ from the classes, when no confusion can result.

Remark 17.3.5. The notation $\mathrm{Cl}\, O$ is also used for the class set, but it sometimes means instead the *stably free* class group or some other variant. We use "Cls" to emphasize that we are working with a class *set*.

17.3.6. The set $\mathrm{Cls}_{\mathsf{R}}\, O$ has a distinguished element $[O]_{\mathsf{R}} \in \mathrm{Cls}_{\mathsf{R}}\, O$, so it has the structure of a pointed set (a set equipped with a distinguished element of the set). However, in general it does not have the structure of a group under multiplication: for classes $[I]_{\mathsf{R}}, [J]_{\mathsf{R}}$, we have $[\alpha J]_{\mathsf{R}} = [J]_{\mathsf{R}}$ for $\alpha \in B^\times$ but we need not have $[I\alpha J]_{\mathsf{R}} = [IJ]_{\mathsf{R}}$, because of the lack of commutativity.

17.3.7. An argument similar to the one in Proposition 17.2.2, either arguing locally or with pseudobases (9.3.7), yields the following [CR81, (4.13)].

Let R be a Dedekind domain with $F = \mathrm{Frac}\, R$, and let $I \subseteq B$ be an R-lattice with $O_{\mathsf{L}}(I) = \mathrm{M}_n(R)$. Then there exists $\beta \in \mathrm{GL}_n(F)$ and fractional ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ such that

$$I = \mathrm{M}_n(R)\, \mathrm{diag}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\beta \tag{17.3.8}$$

where $\mathrm{diag}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ is the R-module of diagonal matrices with entries in the given fractional ideal. The representation (17.3.8) is called the **Hermite normal form** of the R-module I, because it generalizes the Hermite normal form over a PID (allowing coefficient ideals).

By 9.3.10, the Steinitz class $[\mathfrak{a}_1 \cdots \mathfrak{a}_n] \in \mathrm{Cl}\, R$ is uniquely defined. Switching to the right, this yields a bijection

$$\begin{aligned} \mathrm{Cl}\, R &\xrightarrow{\sim} \mathrm{Cls}_{\mathsf{R}}(\mathrm{M}_n(R)) \\ [\mathfrak{a}] &\mapsto [\mathrm{diag}(\mathfrak{a}, 1, \ldots, 1)\, \mathrm{M}_n(R)]_{\mathsf{R}} \end{aligned} \tag{17.3.9}$$

17.4 Types of orders

Next, we consider isomorphism classes of orders. Let $O, O' \subseteq B$ be R-orders.

Definition 17.4.1. We say O, O' are **of the same type** if there exists $\alpha \in B^\times$ such that $O' = \alpha^{-1} O \alpha$.

Lemma 17.4.2. *The R-orders O, O' are of the same type if and only if they are isomorphic as R-algebras.*

Proof. If O, O' are of the same type, then they are isomorphic (under conjugation). Conversely, if $\phi\colon O \xrightarrow{\sim} O'$ is an isomorphism of R-algebras, then extending scalars to F we obtain $\phi_F\colon OF = B \xrightarrow{\sim} B = O'F$ an F-algebra automorphism of B. By the theorem of Skolem–Noether (Corollary 7.7.4), such an automorphism is given by conjugation by $\alpha \in B^\times$, so O, O' are of the same type. □

17.4.3. If O, O' are of the same type, then an isomorphism $O \xrightarrow{\sim} O'$ induces a bijection $\mathrm{Cls}\, O \xrightarrow{\sim} \mathrm{Cls}\, O'$ of pointed sets. By Lemma 17.4.2, such an isomorphism is provided by conjugation $O' = \alpha^{-1} O \alpha$ for some $\alpha \in B^\times$. The principal lattice $I = O\alpha = \alpha O'$ has $O_\mathsf{L}(I) = O$ and $O_\mathsf{R}(I) = O'$.

Generalizing 17.4.3, the class sets of two orders are in bijection if they are connected, in the following sense.

Definition 17.4.4. O is **connected** to O' if there exists a locally principal fractional O, O'-ideal $J \subseteq B$, called a **connecting ideal**.

The relation of being connected is an equivalence relation on the set of R-orders. If two R-orders O, O' are of the same type, then they are connected by a principal connecting ideal (17.4.3).

Definition 17.4.5. We say that O, O' are **locally of the same type** or **locally isomorphic** if $O_\mathfrak{p}$ and $O'_\mathfrak{p}$ are of the same type (i.e., $O_\mathfrak{p} \simeq O'_\mathfrak{p}$) for all primes $\mathfrak{p}$ of R.

Lemma 17.4.6. *The R-orders O, O' are connected if and only if O, O' are locally isomorphic.*

Proof. Let J be a connecting ideal, a locally principal fractional O, O'-ideal. Then for all primes $\mathfrak{p}$ of R we have $J_\mathfrak{p} = O_\mathfrak{p}\alpha_\mathfrak{p}$ with $\alpha_\mathfrak{p} \in B_\mathfrak{p}$, and consequently $O'_\mathfrak{p} = O_\mathsf{R}(I_\mathfrak{p}) = \alpha_\mathfrak{p}^{-1} O_\mathfrak{p} \alpha_\mathfrak{p}$. Therefore O is locally isomorphic to O'.

Conversely, if O, O' are locally isomorphic, then for all primes $\mathfrak{p}$ of R we have $O'_\mathfrak{p} = \alpha_\mathfrak{p}^{-1} O_\mathfrak{p} \alpha_\mathfrak{p}$ with $\alpha_\mathfrak{p} \in B_\mathfrak{p}$. Since R is a Dedekind domain, $O'_\mathfrak{p} = O_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$, so we may take $\alpha_\mathfrak{p} \in O_\mathfrak{p} = O'_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$. Therefore, there exists an R-lattice I with $I_\mathfrak{p} = O_\mathfrak{p}\alpha_\mathfrak{p}$ by the local-global principle for lattices, and I is a locally principal fractional O, O'-ideal. □

Lemma 17.4.7. *If $O, O' \subseteq B$ are maximal R-orders, then OO' is a O, O'-connecting ideal.*

The product in Lemma 17.4.7 is not necessarily compatible.

Proof. Since O, O' are R-lattices, their product $I := OO'$ is an R-lattice. We visibly have $O \subseteq O_\mathsf{L}(I)$ and the same on the right; but O, O' are maximal, so equality holds and I is a fractional O, O'-ideal. Finally, I is invertible by Proposition 16.6.15(b), hence locally principal by Main Theorem 16.6.1. □

In analogy with the class set, we make the following definitions.

Definition 17.4.8. Let $O \subset B$ be an R-order. The **genus** $\mathrm{Gen}\, O$ of O is the set of R-orders in B locally isomorphic to O. The **type set** $\mathrm{Typ}\, O$ of O is the set of isomorphism classes of orders in the genus of O.

17.4.9. The orders in a genus have a common reduced discriminant, since the discriminant can be defined locally and is well-defined on (local) isomorphism classes, by Corollary 15.2.9.

17.4.10. Recalling section 15.5, there is a unique genus of maximal R-orders in a quaternion algebra B—that is to say, every two maximal orders are locally isomorphic—and this genus has a well-defined reduced discriminant equal to $\operatorname{disc}_R B$.

The importance of connected orders is attested to by the following result.

Lemma 17.4.11. *Let O, O' be connected R-orders, and let J be a connecting O, O'-ideal. Then the maps*

$$\begin{aligned} \operatorname{Cls}_{\mathsf{R}} O &\xrightarrow{\sim} \operatorname{Cls}_{\mathsf{R}} O' \\ [I]_{\mathsf{R}} &\mapsto [IJ]_{\mathsf{R}} \\ [I'J^{-1}]_{\mathsf{R}} &\leftarrow\!\shortmid [I']_{\mathsf{R}} \end{aligned}$$

are mutually inverse bijections. In particular, if $O' \in \operatorname{Gen} O$ then $\#\operatorname{Cls}_{\mathsf{R}} O = \#\operatorname{Cls}_{\mathsf{R}} O'$.

Proof. By definition, J is invertible with $O_{\mathsf{L}}(J) = O$ and $O_{\mathsf{R}}(J) = O'$. Therefore the map $I \mapsto IJ$ induces a bijection between the set of invertible right O-ideals and the set of invertible right O'-ideals (Lemma 16.5.11), with inverse given by $I' \mapsto I'J^{-1}$, and each of these products is compatible. This map then induces a bijection $\operatorname{Cls} O \xrightarrow{\sim} \operatorname{Cls} O'$, since is compatible with left multiplication in B, i.e., $(\alpha I)J = \alpha(IJ)$ for all $\alpha \in B^{\times}$. □

Remark 17.4.12. The equivalence in Lemma 17.4.11 is a form of *Morita equivalence*: see Remark 7.2.20.

Lemma 17.4.11 says that the cardinality of the right class set is well-defined on the genus $\operatorname{Gen} O$; and of course the cardinality of the type set is also well-defined on the genus (as it is the number of isomorphism classes).

Lemma 17.4.13. *The map*

$$\begin{aligned} \operatorname{Cls}_{\mathsf{R}} O &\to \operatorname{Typ} O \\ [I]_{\mathsf{R}} &\mapsto \text{class of } O_{\mathsf{L}}(I) \end{aligned} \tag{17.4.14}$$

is a surjective map of sets.

Proof. If O' is connected to O, then there is a connecting O', O-ideal I, and $[I]_{\mathsf{R}} \in \operatorname{Cls}_{\mathsf{R}} O$ has $O_{\mathsf{L}}(I) \simeq O'$. □

Remark 17.4.15. The fibers of the map (17.4.14) is given by classes of two-sided ideals: see Proposition 18.5.10.

17.4.16. Let $B = \mathrm{M}_2(F)$ and $O = \mathrm{M}_2(R)$. From the bijection (17.3.9), the classes in $\operatorname{Cl}_{\mathsf{R}}(\mathrm{M}_2(R))$ are represented by $I_{\mathfrak{a}} = \begin{pmatrix} \mathfrak{a} & \mathfrak{a} \\ R & R \end{pmatrix}$ for $[\mathfrak{a}] \in \operatorname{Cl} R$. Consequently

$$O_{\mathsf{L}}(I_{\mathfrak{a}}) = \begin{pmatrix} R & \mathfrak{a} \\ \mathfrak{a}^{-1} & R \end{pmatrix}.$$

We will see later (28.5.11) that there is a bijection

$$\begin{aligned} \operatorname{Cl} R/(\operatorname{Cl} R)^2 &\xrightarrow{\sim} \operatorname{Typ} \mathrm{M}_2(R) \\ \text{class of } [\mathfrak{a}] \text{ up to squares} &\mapsto \text{class of } \begin{pmatrix} R & \mathfrak{a} \\ \mathfrak{a}^{-1} & R \end{pmatrix}. \end{aligned} \tag{17.4.17}$$

17.5 ▹ Finiteness of the class set: over the integers

Over the next two sections, we will show that the set $\operatorname{Cls} O$ of invertible right (fractional) O-ideals is finite using the geometry of numbers. In this section, we carry this out for the simplest case, when B is definite over $\mathbb{Q}$; we consider the general case in the next section. For further reading on the rich theory of the geometry of numbers, see Cassels [Cas97], Gruber–Lekkerkerker [GrLe87], and Siegel [Sie89].

Our strategy is as follows: if J is an invertible right O-ideal, we will show there exists $\alpha \in J^{-1}$ with the property that $\alpha J = I \subseteq O$ has bounded absolute norm $\mathsf{N}(I) = \#(O/I) \leq C$ where $C \in \mathbb{R}_{>0}$ is independent of J. The result will then follow from the fact that there are only finitely many right O-ideals of bounded absolute norm.

We begin with some definitions (generalizing Definition 9.3.1 slightly).

Definition 17.5.1. A **Euclidean lattice** is a $\mathbb{Z}$-submodule $\Lambda \subseteq \mathbb{R}^n$ with $\Lambda \simeq \mathbb{Z}^n$ such that $\mathbb{R}\Lambda = \mathbb{R}^n$. The **covolume** of a Euclidean lattice Λ is $\operatorname{covol}(\Lambda) = \operatorname{vol}(\mathbb{R}^n/\Lambda)$.

17.5.2. Equivalently, a Euclidean lattice $\Lambda \subset \mathbb{R}^n$ is the $\mathbb{Z}$-span of a basis of $\mathbb{R}^n$, and if $\Lambda = \bigoplus_i \mathbb{Z}a_i$, then $\operatorname{covol}(\Lambda) = |\det(a_{ij})_{i,j}|$.

Lemma 17.5.3. *A subgroup $\Lambda \subset \mathbb{R}^n$ is a Euclidean lattice if and only if Λ is discrete and the quotient $\mathbb{R}^n/\Lambda$ is compact.*

Proof. Exercise 17.6. □

Definition 17.5.4. Let $X \subseteq \mathbb{R}^n$ be a subset.

(a) X is **convex** if $tx + (1-t)y \in X$ for all $x, y \in X$ and $t \in [0,1]$.

(b) X is **symmetric** if $-x \in X$ for all $x \in X$.

The main result of Minkowski's geometry of numbers is the following convex body theorem.

Theorem 17.5.5. (Minkowski). *Let $X \subseteq \mathbb{R}^n$ be a closed, convex, symmetric subset of $\mathbb{R}^n$, and let $\Lambda \subset \mathbb{R}^n$ be a Euclidean lattice. If $\operatorname{vol}(X) \geq 2^n \operatorname{covol}(\Lambda)$, then there exists $0 \neq \alpha \in \Lambda \cap X$.*

The following proposition can be seen as a generalization of what was done for the Hurwitz order (11.3.1).

Proposition 17.5.6. *Let B be a definite quaternion algebra over $\mathbb{Q}$ and let $O \subset B$ be an order. Then $O^\times = O^1$ is a finite group, and every right ideal class in* $\operatorname{Cls} O$ *is represented by an integral right O-ideal with*

$$\mathsf{N}(I) \leq \frac{8}{\pi^2} \operatorname{discrd}(O)$$

and the right class set $\operatorname{Cls} O$ *is finite.*

Proof. Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, with $a, b \in \mathbb{Z}_{<0}$. Since B is definite, there is an embedding $B \hookrightarrow B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{H}$. Inside $B_\infty \simeq \mathbb{R}^4$ with Euclidean norm nrd, the order O sits as a Euclidean lattice. The set O^1 is therefore a discrete subset of the compact set $B_\infty^1 \simeq \mathbb{H}^1$, so it is finite.

Explicitly, we identify

$$\begin{aligned} B_\infty &\xrightarrow{\sim} \mathbb{R}^4 \\ t + xi + yj + zij &\mapsto \sqrt{2}\big(t, x\sqrt{|a|}, y\sqrt{|b|}, z\sqrt{|ab|}\big) \end{aligned} \tag{17.5.7}$$

Then $2\operatorname{nrd}(\alpha) = \|\alpha\|^2$ for $\alpha \in B$ in this identification, and we have $\operatorname{covol}(O) = \operatorname{discrd}(O)$ (Exercise 17.7).

Let $J \subset B$ be an invertible right fractional O-ideal. To find I with $[I] = [J]$ and I integral, we look for a small $\alpha \in J^{-1}$ so that $I = \alpha J \subseteq O$ will do. As a measure of (co)volume, counting cosets and applying the definition (16.4.9), we obtain

$$\operatorname{covol}(J^{-1}) = [O : J^{-1}]_{\mathbb{Z}} \operatorname{covol}(O) = \mathsf{N}(J^{-1}) \operatorname{discrd}(O). \tag{17.5.8}$$

Let $c > 0$ satisfy $c^4 = (32/\pi^2)\operatorname{covol}(J^{-1})$, and let

$$X = \{x \in \mathbb{R}^4 : \|x\| \leq c\}.$$

Then X is closed, convex, and symmetric, and $\operatorname{vol}(X) = \pi^2 c^4/2 = 16 \operatorname{covol}(J^{-1})$. Then by Minkowski's theorem (Theorem 17.5.5), there exists $0 \neq \alpha \in J^{-1} \cap X$, and

$$\begin{aligned} \mathsf{N}(\alpha J) = \operatorname{Nm}_{B|\mathbb{Q}}(\alpha)\mathsf{N}(J) = \operatorname{nrd}(\alpha)^2 \mathsf{N}(J) = \frac{1}{4}\|\alpha\|^4 \mathsf{N}(J) \\ \leq \frac{1}{4} c^4 \mathsf{N}(J) = \frac{8}{\pi^2} \operatorname{discrd}(O). \end{aligned} \tag{17.5.9}$$

Since α is nonzero and B is a division algebra, $\alpha \in B^\times$. Since $\alpha \in J^{-1}$, the integral right fractional O-ideal $I = \alpha J \subseteq O$ is as desired.

If $I \subseteq O$ has $\mathsf{N}(I) = \#(O/I) \leq C$ for $C \in \mathbb{Z}_{>0}$, then $CO \subseteq I \subseteq O$ hence there are only finitely many possibilities for I, and the second statement follows. □

17.6 ▹ Example

We pause for an extended example. We steal the following lemma from the future.

Lemma 17.6.1. *Let $e \in \mathbb{Z}_{\geq 0}$. Then every principal right $\mathrm{M}_2(\mathbb{Z}_p)$-ideal I with $\mathrm{nrd}(I) = p^e$ is of the form $I = \alpha\,\mathrm{M}_2(\mathbb{Z}_p)$ where*

$$\alpha \in \left\{ \begin{pmatrix} p^u & 0 \\ c & p^v \end{pmatrix} : u, v \in \mathbb{Z}_{\geq 0}, u + v = e, \text{and} c \in \mathbb{Z}/p^v\mathbb{Z} \right\}. \tag{17.6.2}$$

Proof. The lemma follows from the theory of invariant factors: a more general statement is proven in Lemma 26.4.1. □

Example 17.6.3. Let $B = \left(\frac{-1,-23}{\mathbb{Q}}\right)$, and let

$$O = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}i\frac{1+j}{2}.$$

We have $\mathrm{discrd}(O) = \mathrm{disc}\, B = 23$, so O is a maximal order, and $\beta = (1+j)/2$ satisfies $\beta^2 - \beta + 6 = 0$. For convenience, let $\alpha = i$, so $O = \mathbb{Z}\langle \alpha, \beta \rangle$. Then

$$\alpha\beta + \beta\alpha = \alpha. \tag{17.6.4}$$

By Proposition 17.5.6, it is sufficient to compute the (invertible) right O-ideals $I \subseteq O$ such that

$$\mathrm{nrd}(I)^2 = \mathsf{N}(I) \leq \frac{8}{\pi^2}(23) \leq 18.7$$

so $\mathrm{nrd}(I) \leq 4$. For $\mathrm{nrd}(I) = 1$, we can only have $I = O$, and the class $[I_1] = [O]$. Let $O_1 = O$.

We move to $\mathrm{nrd}(I) = 2$, and refer to Lemma 17.6.1. Since B is split at 2, there is an embedding

$$\begin{aligned} O &\hookrightarrow \mathrm{M}_2(\mathbb{Z}_2) \\ \alpha, \beta &\mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & b_0 \end{pmatrix}. \end{aligned}$$

where $b_0 = 2 + 8 + 16 + 32 + \cdots \in \mathbb{Z}_2$ satisfies $b_0^2 - b_0 + 6 = 0$ and $b_0 \equiv 0 \pmod 2$. We have

$$\beta, \beta + 1, (\alpha + 1)\beta \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \pmod 2$$

so we obtain the three right ideals

$$I_{(1:0)} = 2O + \beta O, \quad I_{(0:1)} = 2O + (\beta - 1)O, \quad I_{(1:1)} = 2O + (\alpha + 1)\beta O \tag{17.6.5}$$

labelled by the corresponding nonzero column. If one of these three ideals is principal, then it is generated by an element of reduced norm 2. We have

$$\begin{aligned} &\mathrm{nrd}(t + x\alpha + y\beta + z\alpha\beta) \\ &\quad = t^2 + ty + x^2 + xz + 6y^2 + 6z^2 \\ &\quad = \left(t + \frac{1}{2}y\right)^2 + \left(x + \frac{1}{2}z\right)^2 + \frac{23}{4}y^2 + \frac{23}{4}z^2. \end{aligned} \tag{17.6.6}$$

So $\mathrm{nrd}(\gamma) = 2$ with $\gamma \in O$ has $t, x, y, z \in \mathbb{Z}$ and therefore $y = z = 0$ and $t = x = 1$, i.e., $I_{(1:1)} = (\alpha + 1)O$ is principal, and the ideals $I_{(1:0)}, I_{(0:1)}$ are not. But $[I_{(1:0)}] = [I_{(0:1)}]$ because $\alpha I_{(1:0)} = I_{(0:1)}$ because $\alpha \in O^\times$ and by (17.6.4)

$$\alpha(2O + (\beta - 1)O) = 2\alpha O + \alpha(\beta - 1)O = 2O - \beta\alpha O = I_{(0:1)}$$

(We have $\alpha I_{(1:0)} \neq I_{(1:0)}$ precisely because $\alpha \notin O_\mathsf{L}(I)$.) In this way, we have found exactly one new right ideal class, $[I_2] = [I_{(1:0)}]$. We compute its left order to be

$$O_2 := O_\mathsf{L}(I_2) = \mathbb{Z} + \beta\mathbb{Z} + \frac{i(1+3j)}{4}\mathbb{Z} + (2ij)\mathbb{Z} \neq O$$

and we also have a new type $[O_2] \neq [O_1] \in \mathrm{Typ}\, O$.

In a similar way, we find 4 right ideals of reduced norm 3, and exactly one new right ideal class, represented by the right ideal $I_3 = 3O + (\alpha + 1)\beta O$. For example, we find that the right ideal $I' = 3O + \beta O$ is not principal using (17.6.6): letting

$$(I' : I_2)_\mathsf{L} = I' I_2^{-1} = \frac{1}{2} I' \overline{I_2}$$

and we find a shortest vector

$$(1 - \beta)/2 \in (I' : I_2)_\mathsf{L},$$

so $[I'] = [I_2]$.

Repeating this with ideals of reduced norm 4 (Exercise 17.8), we conclude that

$$\mathrm{Cls}\, O = \{[I_1], [I_2], [I_3]\}$$

and letting $O_3 := O_\mathsf{L}(I_3)$, checking it is not isomorphic to the previous two orders, we have

$$\mathrm{Typ}\, O = \{[O_1], [O_2], [O_3]\}.$$

17.7 Finiteness of the class set: over number rings

We now turn to the general case.

Main Theorem 17.7.1. *Let F be a number field, let $S \subseteq \mathrm{Pl}\, F$ be eligible and $R = R_{(S)}$ be the ring of S-integers in F. Let B be a quaternion algebra over F, and let $O \subseteq B$ be an R-order in B. Then the class set* $\mathrm{Cls}\, O$ *and the type set* $\mathrm{Typ}\, O$ *is finite.*

We call $\#\mathrm{Cls}\, O$ the **(right) class number** of O. (By 17.3.2, the left class number suitably defined is equal to the right class number.) This result will be drastically improved upon in Part III of this text from analytic considerations; the proof in this section, using the geometry of numbers, has the advantage that is easy to visualize, it works in quite some generality, and it is the launching point for algorithmic aspects.

17.7.2. Before we begin, two quick reductions. The finiteness of the type set follows from finiteness of the right class set by Lemma 17.4.13. And if $R = \mathbb{Z}_F$ is the ring of integers of F, then the general case follows from the fact that the map

$$\begin{aligned} \operatorname{Cls} O &\to \operatorname{Cl}(O \otimes_R R_{(S)}) \\ [I] &\mapsto [I \otimes_R R_{(S)}] \end{aligned} \tag{17.7.3}$$

is surjective for an eligible set S.

Let F be a number field of degree $n = [F : \mathbb{Q}]$, let $R = \mathbb{Z}_F$ be the ring of integers in F, and let B be a quaternion algebra over F.

17.7.4. Suppose that F has r real places and c complex places, so that $n = r + 2c$. Then

$$F \hookrightarrow F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{v|\infty} F_v \simeq \mathbb{R}^r \times \mathbb{C}^c. \tag{17.7.5}$$

Taking the basis $1, i$ for $\mathbb{C}$, we obtain $F_\infty \simeq \mathbb{R}^n$, and then in the embedding (17.7.5), the ring of integers $R \simeq \mathbb{Z}^n$ sits discretely inside $F_\infty \simeq \mathbb{R}^n$ as a Euclidean lattice.

17.7.6. Suppose $B = \left(\frac{a,b}{F}\right)$ and let $1, i, j, k$ be the standard basis for B with $k = ij$, so $B = F \oplus Fi \oplus Fj \oplus Fk \simeq F^4$ as F-vector spaces. Then

$$B \hookrightarrow B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \simeq B \otimes_F F_\infty \simeq F_\infty^4 \tag{17.7.7}$$

in this same basis. Via (17.7.5) in each of the four components, the embedding (17.7.7) then gives an identification $B_\infty \simeq (\mathbb{R}^n)^4 \simeq \mathbb{R}^{4n}$.

The order $R\langle i, j, k\rangle = R + Ri + Rj + Rk$ is discrete in B_∞ exactly because R is discrete in F. But then implies that an R-order O is discrete in B_∞, since $[O : R\langle i, j, k\rangle]_{\mathbb{Z}} < \infty$. Therefore $O \hookrightarrow \mathbb{R}^{4n}$ has the structure of a Euclidean lattice.

In the previous section, the real vector space B_∞ was Euclidean under the reduced norm. In general, that need no longer be the case. Instead, we find a positive definite quadratic form $Q \colon B_\infty \to \mathbb{R}$ that **majorizes** the reduced norm in the following sense: we require that

$$|\operatorname{Nm}_{F/\mathbb{Q}}(\operatorname{nrd}(\alpha))| \leq Q(\alpha)^n \tag{17.7.8}$$

for all $\alpha \in B \subseteq B_\infty$.

Remark 17.7.9. With respect to possible majorants (17.7.8): in general, there are uncountably many such choices, and parametrizing majorants arises in a geometric context as part of *reduction theory*. As it will turn out, the only "interesting" case to consider here is 17.7.10, by strong approximation (see Theorem 17.8.3).

17.7.10. Let B be a totally definite (Definition 14.5.7) quaternion algebra over F, a totally real number field. Then the quadratic form

$$\begin{aligned} Q \colon B &\to \mathbb{Q} \\ \alpha &\mapsto \operatorname{Tr}_{F/\mathbb{Q}}(\operatorname{nrd}(\alpha)) = \sum_{v|\infty} v(\operatorname{nrd}(\alpha)) \end{aligned} \tag{17.7.11}$$

is positive definite: $B_v \simeq \mathbb{H}$ and so $v(\mathrm{nrd}(\alpha)) \geq 0$ with equality if and only if $\alpha = 0$. We call this quadratic form the **absolute reduced norm**. In this case, by the arithmetic-geometric mean,

$$\begin{aligned} \mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{nrd}(\alpha))^{1/n} &= \left(\prod_v v(\mathrm{nrd}(\alpha))\right)^{1/n} \\ &\leq \frac{1}{n}\sum_v v(\mathrm{nrd}(\alpha)) = \frac{1}{n}Q(\alpha) \end{aligned} \tag{17.7.12}$$

(with equality if and only if $v(\mathrm{nrd}\,\alpha)$ agrees for all v).

We pause to note the following important consequence of 17.7.10.

Lemma 17.7.13. *Let B be a totally definite quaternion algebra over a totally real field F and let $O \subseteq B$ be a $\mathbb{Z}_F$-order. Then the group of units of reduced norm* 1

$$O^1 = \{\gamma \in O : \mathrm{nrd}(\gamma) = 1\}$$

is a finite group.

In Lemma 17.7.13, if $F = \mathbb{Q}$ then $O^\times = O^1$, so we have captured the entire unit group.

Proof. As in 17.7.10, we equip $B_\mathbb{R} := B \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{H}^n \simeq \mathbb{R}^{4n}$ with the absolute reduced norm giving $O \hookrightarrow B_\mathbb{R}$ the structure of a Euclidean lattice (17.7.7). We have

$$O^1 = \{\gamma \in O : Q(\gamma) = n\} \tag{17.7.14}$$

by the arithmetic-geometric mean (17.7.12). But the set $\{x \in B_\mathbb{R} : Q(x) = n\}$ is an ellipsoid in $\mathbb{R}^{4n}$ so compact, and O is a lattice so discrete. Therefore the intersection O^1 is finite. □

17.7.15. We now generalize 17.7.10 to the general case. For v an infinite place of F, define

$$\begin{aligned} Q_v \colon B_v &\to \mathbb{R} \\ t + xi + yj + zij &\mapsto |v(t)|^2 + |v(a)||v(x)|^2 + |v(b)||v(y)|^2 + |v(ab)||v(z)|^2; \end{aligned}$$

then Q_v is a positive definite quadratic form on B_v, and

$$\begin{aligned} |v(\mathrm{nrd}(\alpha))| &= |v(t^2 - ax^2 - by^2 + abz^2)| \\ &\leq |v(t)|^2 + |v(a)||v(x)|^2 + |v(b)||v(y)|^2 + |v(ab)||v(z)|^2 \\ &= Q_v(\alpha). \end{aligned} \tag{17.7.16}$$

Let $m_v = 1, 2$ depending on if v is real or complex, and define

$$\begin{aligned} Q \colon B_\infty \simeq \prod_{v|\infty} B_v &\to \mathbb{R} \\ (\alpha_v)_v &\mapsto \sum_{v|\infty} m_v Q_v(\alpha_v). \end{aligned} \tag{17.7.17}$$

Then Q is a positive definite quadratic form on B_∞, again called the **absolute reduced norm** (relative to a, b); it depends on the choice of representation $B = \left(\frac{a,b}{F}\right)$. Nevertheless, (17.7.16) and the arithmetic-geometric mean yield

$$\begin{aligned} |\mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{nrd}(\alpha))|^{1/n} &\leq \frac{1}{n}\sum_{v|\infty} m_v |v(\mathrm{nrd}(\alpha))| \\ &\leq \frac{1}{n}\sum_{v|\infty} m_v Q_v(\alpha) = Q(\alpha). \end{aligned} \tag{17.7.18}$$

We are now ready to prove the main result of this section.

Proposition 17.7.19. *There exists an explicit constant $C \in \mathbb{R}_{>0}$ such that for all R-orders $\mathcal{O}$, every right ideal class in* $\mathrm{Cls}\,\mathcal{O}$ *is represented by an integral right $\mathcal{O}$-ideal I with*

$$\mathsf{N}(I) \leq C\mathsf{N}(\mathrm{discrd}(\mathcal{O})).$$

Proof. If $B \simeq \mathrm{M}_2(F)$, then we appeal to 17.3.7, where such a bound comes from the finiteness of $\mathrm{Cl}\, R$. So we may suppose that B is a division ring.

Let

$$X = \{(x_i)_i \in \mathbb{R}^{4n} : Q(\alpha) \leq 1\}. \tag{17.7.20}$$

Then X is closed, convex, and symmetric.

Let $\mathcal{O}$ be an R-order in B and let J be an invertible right fractional $\mathcal{O}$-ideal. As in (17.5.8), counting cosets gives

$$\mathrm{covol}(J^{-1}) = \mathsf{N}(J)^{-1}\,\mathrm{covol}(\mathcal{O}). \tag{17.7.21}$$

Let

$$c := 2\left(\frac{\mathrm{covol}(J^{-1})}{\mathrm{vol}(X)}\right)^{1/4n}. \tag{17.7.22}$$

Then $\mathrm{vol}(cX) = c^{4n}\,\mathrm{vol}(X) = 2^{4n}\,\mathrm{covol}(J^{-1})$. By Minkowski's theorem, there exists $0 \neq \alpha \in J^{-1} \cap cX$, so $Q(\alpha) \leq c^2$. By (17.7.18),

$$|\mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{nrd}(\alpha))| \leq \frac{1}{n^n}Q(\alpha)^n \leq \frac{c^{2n}}{n^n}.$$

Consequently

$$\begin{aligned} \mathsf{N}(\alpha J) &= |\mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{nrd}(\alpha))|^2\mathsf{N}(J) \leq \frac{c^{4n}}{n^{2n}}\mathsf{N}(J) \\ &= \frac{2^{4n}\mathsf{N}(J)^{-1}\,\mathrm{covol}(\mathcal{O})}{n^{2n}\,\mathrm{vol}(X)}\mathsf{N}(J) = \frac{2^{4n}\,\mathrm{covol}(\mathcal{O})}{n^{2n}\,\mathrm{vol}(X)} \\ &= C\mathsf{N}(\mathrm{discrd}(\mathcal{O})) \end{aligned} \tag{17.7.23}$$

with

$$C := \frac{2^{4n}}{n^{2n}\,\mathrm{vol}(X)}\frac{\mathrm{covol}(\mathcal{O})}{\mathsf{N}(\mathrm{discrd}(\mathcal{O}))}. \tag{17.7.24}$$

The ratio $\mathrm{covol}(O)/\mathsf{N}(\mathrm{discrd}(O))$ is a constant independent of O: if O' is another R-order then

$$\frac{\mathsf{N}(\mathrm{discrd}(O'))}{\mathrm{covol}(O')} = \frac{[O : O']_{\mathbb{Z}}\mathsf{N}(\mathrm{discrd}(O))}{[O : O']_{\mathbb{Z}}\,\mathrm{covol}(O)} = \frac{\mathsf{N}(\mathrm{discrd}(O))}{\mathrm{covol}(O)}.$$

Since α is nonzero and B is a division algebra we conclude that $\alpha \in B^\times$, and since $\alpha \in J^{-1}$, the ideal $I = \alpha J$ is as desired. □

Remark 17.7.25. For an explicit version of the Minkowski bound in the totally definite case, with a careful choice of compact region, see Kirschmer [Kir2005, Theorem 3.3.11].

Lemma 17.7.26. *For all $C > 0$, there are only finitely many integral right O-ideals with $\mathsf{N}(I) \leq C$.*

Proof. We may suppose $C \in \mathbb{Z}$. If $I \subseteq O$ then $\mathsf{N}(I) = [O : I]_{\mathbb{Z}} \leq C$, so $CO \subseteq I \subseteq O$. But the group O/CO is a finite abelian group and there are only finitely many possibilities for I. □

We now have the ingredients for our main theorem.

Proof of Main Theorem 17.7.1. Combine Proposition 17.7.19, the reductions in 17.7.2, and Lemma 17.7.26. □

Remark 17.7.27. The finiteness statement (Main Theorem 17.7.1) can be generalized to the following theorem of Jordan–Zassenhaus. Let R be a Dedekind domain with $F = \mathrm{Frac}(R)$ a global field, let $O \subseteq B$ be an R-order in a finite-dimensional semisimple algebra B, and let V be a left B-module. Then there are only finitely many isomorphism classes $I \subseteq B$ with $O \subseteq O_{\mathsf{L}}(I)$. Specializing to $V = B$ a quaternion algebra, we recover the Main Theorem 17.7.1. For a proof, see Reiner [Rei2003, Theorem 26.4]; see also the discussion by Curtis–Reiner [CR81, §24].

17.8 Eichler's theorem

In this section, we state a special but conceptually important case of Eichler's theorem for number fields: roughly speaking, the class set of an indefinite quaternion order is in bijection with a certain class group of the base ring.

Let F be a number field with ring of integers $R = \mathbb{Z}_F$ and let B be a quaternion algebra over F.

Definition 17.8.1. We say B **satisfies the Eichler condition** if B is indefinite.

Definition 17.8.1 introduces a longer (and rather opaque) phrase for something that we already had a word for, but its use is prevalent in the literature. There are two options: either B is totally definite (F is a totally real field and all archimedean places of F are ramified in B) or B is indefinite and satisfies the Eichler condition.

17.8.2. Recall 14.7.2 that we define $\Omega \subseteq \operatorname{Ram} B$ to be the set of real ramified places of B and $F^\times_{>\Omega 0}$ to be the positive elements for $v \in \Omega$.

We now define the group $\operatorname{Cl}_\Omega R$ as

$$\text{the group of fractional ideals of } F \text{ under multiplication}$$

modulo

$$\text{the subgroup of nonzero principal fractional ideals generated by an element in } F^\times_{>\Omega 0}$$

If Ω is the set of all real places of F, then $\operatorname{Cl}_\Omega R = \operatorname{Cl}^+ R$ is the **narrow** (or **strict**) **class group**. On the other hand, if $\Omega = \emptyset$, then $\operatorname{Cl}_\Omega R = \operatorname{Cl} R$. In general, we have surjective group homomorphisms $\operatorname{Cl}^+ R \to \operatorname{Cl}_\Omega R$ and $\operatorname{Cl}_\Omega R \to \operatorname{Cl} R$. In the language of class field theory, $\operatorname{Cl}_\Omega R$ is the class group corresponding to the cycle given by the product of the places in Ω.

Theorem 17.8.3. (Eichler; strong approximation). *Let F be a number field and let B be a quaternion algebra over F that satisfies the Eichler condition. Let $O \subseteq B$ be a maximal $\mathbb{Z}_F$-order. Then the reduced norm induces a bijection*

$$\begin{aligned} \operatorname{Cls} O &\xrightarrow{\sim} \operatorname{Cl}_\Omega R \\ [I] &\mapsto [\operatorname{nrd}(I)]. \end{aligned} \tag{17.8.4}$$

where $\Omega \subseteq \operatorname{Ram} B$ is the set of real ramified places in B.

Proof. Eichler's theorem is addressed by Reiner [Rei2003, §34], with a global proof of the key result [Rei2003, Theorem 34.9] falling over several pages. We will instead prove a more general version of this theorem as part of strong approximation, when idelic methods allow for a more efficient argument: see Corollary 28.5.17. □

Eichler's theorem says that when B is *not* totally definite, the only obstruction for an ideal to be principal in a maximal order is that its reduced norm fails to be (strictly) principal in the base ring. In particular, we have the following corollary.

Corollary 17.8.5. *If $\#\operatorname{Cl}^+ R = 1$, then $\#\operatorname{Cls} O = 1$: i.e., every right O-ideal of a maximal order in an indefinite quaternion algebra is principal.*

Proof. Immediate from Eichler's theorem and the fact that $\operatorname{Cl}^+ R$ surjects onto $\operatorname{Cl}_\Omega R$, by 17.8.2. □

Corollary 17.8.6. *There is a bijection $\operatorname{Cls} \mathrm{M}_2(\mathbb{Z}_F) \xrightarrow{\sim} \operatorname{Cl} \mathbb{Z}_F$.*

Proof. Immediate from Eichler's theorem; we proved this more generally for a matrix ring (17.3.9) using the Hermite normal form. □

17.8.7. It is sensible for the class group $\operatorname{Cl}_\Omega R$ to appear by norm considerations. Let $v \in \Omega$; then $B_v \simeq \mathbb{H}$, and if $\alpha \in B^\times$ then $v(\operatorname{nrd}(\alpha)) > 0$, as the reduced norm is positive.

The class sets of totally definite orders are not captured by Eichler's theorem, and for good reason: they can be arbitrarily large, a consequence of the Eichler mass formula (Chapter 25).

Exercises

Unless otherwise specified, throughout these exercises let R be a Dedekind domain with field of fractions F, let B be a quaternion algebra over F, and let $O \subseteq B$ be an R-order.

1. Argue for Proposition 17.2.2 directly in a special case as follows. Let $I \subseteq \mathrm{M}_2(F)$ be a lattice with $O_{\mathsf{R}}(I) = \mathrm{M}_2(R)$.

   (a) By considering $I \otimes_R F$ show that

   $$I \subseteq \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix} \mathrm{M}_2(R) \oplus \begin{pmatrix} 0 & 0 \\ F & F \end{pmatrix} \mathrm{M}_2(R).$$

   (b) Suppose that R is a PID. Conclude that I is principal.

2. Let $O, O' \subseteq B$ be R-orders. Show that the map in Lemma 17.4.11 is a bijection of *pointed* sets if and only if O is isomorphic to O'.

▹3. Let $O, O' \subseteq B$ be R-orders with $O \subseteq O'$.

   (a) If I is an invertible right O-ideal, show that IO' is an invertible right O'-ideal. (The product IO' is not necessarily compatible.)

   (b) Show that the map

   $$\begin{aligned} \operatorname{Cls} O &\to \operatorname{Cls} O' \\ [I] &\mapsto [IO'] \end{aligned}$$

   is well-defined, surjective, and has finite fibers. *[Hint: let $r \in R$ be nonzero such that $O' \subseteq r^{-1}O$. If $IO' = I'$, then $I' = IO' \subseteq r^{-1}I \subseteq r^{-1}I'$ so $rI' \subseteq I \subseteq I'$, and conclude there are only finitely many possibilities for I.]*

4 Let $O, O' \subseteq B$ be maximal R-orders. In this exercise, we prove the following statement:

   There is a unique *integral* connecting O, O' ideal I of minimal reduced norm; moreover, we have $\operatorname{nrd}(I) = [O : O \cap O']$.

   (a) Show that this statement is local, i.e., the statement is true over R if and only if it is true over $R_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of R.
   (b) Suppose R is a DVR. Show that the statement is true if B is a division algebra.
   (c) Suppose R is a DVR with maximal ideal $\mathfrak{p}$, and that $B \simeq \mathrm{M}_2(F)$. Show that there is a unique $\alpha \in O \smallsetminus \mathfrak{p}O$ such that $O' = \alpha^{-1}O\alpha$ up to left multiplication by $O^\times$, and conclude that $I = O\alpha$ is the unique integral connecting O, O' ideal of minimal reduced norm. *[Hint: $N_{\mathrm{GL}_2(F)}(\mathrm{M}_2(R)) = F^\times \mathrm{GL}_2(R)$.]*
   (d) Continuing (c), show that $\operatorname{nrd}(\alpha) = [O : O \cap O']$. *[Hint: the statement is equivalent under left or right multiplication of α by $O^\times \simeq \mathrm{GL}_2(R)$, so consider invariant factors.]* [For another perspective, see section 23.5.]

▹5. Let $O \subseteq B$ be an R-order and let I be an invertible fractional right O-ideal. Let $\mathfrak{a} \subseteq R$ be a nonzero ideal. Show that there exists a representative $J \in [I]_R$ (in the same right ideal class as I) such that $J \subseteq O$ and $\mathrm{nrd}(J)$ is coprime to $\mathfrak{a}$. *[Hint: look for $\alpha \in (O : I)_R$ and then look locally.]*

▹6. Prove Lemma 17.5.3: a subgroup $\Lambda \subset \mathbb{R}^n$ is a Euclidean lattice if and only if Λ is discrete (every point of Λ is isolated, i.e., every $x \in \Lambda$ has an open neighborhood $U \ni x$ such that $\Lambda \cap U = \{x\}$) and the quotient $\mathbb{R}^n/\Lambda$ is compact.

▹7. Let B be a definite quaternion algebra over $\mathbb{Q}$ and let $O \subset B$ be an order.

(a) Let $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R}$. Show that nrd is a Euclidean norm on B_∞, and O is discrete in B_∞ with $\mathrm{covol}(O) = 4\,\mathrm{discrd}(O)$. [So it is better to take $\sqrt{2}\,\mathrm{nrd}$ instead, to get $\mathrm{covol}(O) = \mathrm{discrd}(O)$ on the nose.]

(b) Let $K_1, K_2 \subseteq B$ be quadratic fields contained in B with $K_1 \cap K_2 = \mathbb{Q}$. Let $S_i := K_i \cap O$ and $d_i = \mathrm{disc}\, S_i$. Show that

$$(|d_1| - 1)(|d_2| - 1) \geq 4\,\mathrm{discrd}(O).$$

[Hint: write $S_i = \mathbb{Z}[\alpha_i]$ and consider the order $\mathbb{Z}\langle\alpha_1, \alpha_2\rangle$.]

(c) Prove that if $\alpha_1, \alpha_2 \in O$ have

$$\mathrm{nrd}(\alpha_1), \mathrm{nrd}(\alpha_2) < \frac{\sqrt{\mathrm{discrd}(O)}}{2}$$

then $\alpha_1\alpha_2 = \alpha_2\alpha_1$.

8. Complete Example 17.6.3 by showing explicitly that all right O-ideals of reduced norm 4 are in the same right ideal class as one of I_1, I_2, I_3.

9. Let R be a global ring with $\#\,\mathrm{Cl}\, R = 1$, i.e., every fractional R-ideal is principal $\mathfrak{a} = aR$. Suppose further that $\#\,\mathrm{Cls}\, O = 1$. Let $\alpha \in O$ have $\mathrm{nrd}(\alpha) \neq 0$, and factor $\mathrm{nrd}(\alpha) = \pi_1\pi_2\cdots\pi_r \in R$ where $\pi_i \in R$ are pairwise nonassociate nonzero prime elements (equivalently $\pi_i R$ are pairwise distinct nonzero prime ideals).

(a) Show that there exist $\varpi_1, \varpi_2, \ldots, \varpi_r \in O$ such that $\alpha = \varpi_1\varpi_2\cdots\varpi_r$ and $\mathrm{nrd}(\varpi_i)R = \pi_i R$ for all $i = 1, \ldots, r$.

(b) Show that every other such factorization is of the form

$$\alpha = (\varpi_1\gamma_1)(\gamma_1^{-1}\varpi_2\gamma_2)\cdots(\gamma_{r-1}^{-1}\varpi_r)$$

where $\gamma_1, \ldots, \gamma_r \in O^\times$.

(c) Suppose that $\mathrm{nrd}(O^\times) = R^\times$. Refine part (a) and show that the stronger conclusion that there exist ϖ_i such that $\mathrm{nrd}(\varpi_i) = \pi_i$ for all i.

[This generalizes Theorem 11.4.8.]

10. We have seen that maximal orders in (definite) quaternion algebras of discriminant 2 (the Hurwitz order) and discriminant 3 (Exercise 11.11) are Euclidean with respect to the norm, and in particular they have trivial right class set.

(a) Show that maximal orders O in quaternion algebras of discriminants 5, 7, 13 have $\#\operatorname{Cls} O = 1$.
(b) Conclude that the quaternary quadratic forms

$$t^2 + tx + ty + tz + x^2 + xy + xz + 2y^2 - yz + 2z^2,$$
$$t^2 + tz + x^2 + xy + 2y^2 + 2z^2,$$
$$t^2 + ty + tz + 2x^2 + xy + 2xz + 2y^2 + yz + 4z^2$$

are multiplicative and **universal**, i.e., represent all positive integers.
(c) Show that for discriminant 7, 13 the maximal orders are *not* Euclidean with respect to the norm.

[We discuss the maximal orders of class number 1 in Theorem 25.4.1. The maximal order for discriminant 5 is in fact norm Euclidean: see Fitzgerald [Fit2011].]

11. In this exercise, we show that the group of principal two-sided ideals $\operatorname{PIdl}(O)$ need not be normal in the group of invertible fractional O-ideals $\operatorname{Idl}(O)$ of an order.

Let $B = (-1, -1 \mid \mathbb{Q})$, and let $O \subseteq B$ be the Hurwitz order. Let $O' = \mathbb{Z} + 5O = O(5)$ (cf. Exercise 18.6). Show that

$$I' = 10O' + (1 - 2i + j)O'$$

is a two-sided invertible O'-ideal, and that

$$I' j (I')^{-1} = 5O' + (i + 3j + k)O'$$

is not principal.

12. The finiteness of the class group (see Reiner [Rei2003, Lemma 26.3]) can be proven replacing the geometry of numbers with just the pigeonhole principle, as follows. Let B be a division algebra over a number field F with ring of integers R, and let $O \subseteq B$ be an R-order.

(a) To prove the finiteness of $\operatorname{Cls} O$, show that without loss of generality we may take $F = \mathbb{Q}$.
(b) Show that $\operatorname{Nm}_{B|\mathbb{Q}}(x_1\alpha_1 + \cdots + x_n\alpha_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ is a homogeneous polynomial of degree n.
(c) Show that there exists $C \in \mathbb{Z}_{>0}$ such that for all $t > 0$ and all $x \in \mathbb{Z}^n$ with $|x_i| \leq t$, we have $|\operatorname{Nm}_{B|F}(x_1\alpha_1 + \cdots + x_n\alpha_n)| \leq Ct^n$.
(d) Let $I \subseteq O$ be a lattice. Let $s \in \mathbb{Z}$ be such that

$$s^n \leq \mathsf{N}(I) = \#(O/I) \leq (s+1)^n.$$

Using the pigeonhole principle, show that there exists $\alpha = \sum_i x_i\alpha_i \in I$ with $x_i \in \mathbb{Z}$ and $|x_i| \leq 2(s+1)$ for all i.
(e) Show that $\mathsf{N}(\alpha O) \leq 2^n(s+1)^n C$, and conclude that

$$\#(I/\alpha O) \leq 4^n C.$$

(f) Let $M = (4^n C)!$ and show that $MI \subseteq \alpha O$, whence

$$MO \subseteq I' \subseteq O$$

where $I' = (M\alpha^{-1})I$. Conclude that the number of possibilities for I' is finite, hence the number of right classes of lattices $I \subseteq O$ is finite, and hence $\#\operatorname{Cls} O < \infty$.