Chapter 4

Integral structures in algebras

In this chapter, we will introduce the notions of integrality and ideal theory in algebras in a reasonable amount of generality. Specifically, we will consider algebras[1] A over p-adic or number fields F with ring of integers $R = \mathcal{O}_F$. Then we will study orders in A which are rings with an integral structure over R (they are R-modules). Since we will be using capital $\mathcal{O}$'s for our orders in A, to make notation more suggestive, I will now generally use $\mathfrak{o}_F$ for the ring of integers for our "base field" F instead of $\mathcal{O}_F$. (Morally, $\mathcal{O}$ will be an order in our big ring A which is "an extension" of an order $\mathfrak{o}$ in our small ring F.)

In order to treat both p-adic fields and global fields at once, it's convenient to work in the following more general setting, as we did in Section 3.2.

Recall that an **integral domain** is a nonzero commutative ring without zero divisors, and a **Dedekind domain** to be an integral domain such that every nontrivial ideal factors into a product of prime ideals. In Dedekind domains, factorization of ideals into prime ideals is necessarily unique. We can start with any Dedekind domain R and let F be its field of fractions. This includes the cases where F is a p-adic field or a number field, and R its ring of integers. Indeed, this is our primary concern, and if you like you can just think about these cases (and we may sometimes quote results for Dedekind domains which you might have only seen in the case of p-adic or number fields). Dedekind domains also include the case of nonarchimedean local fields in characteristic p, global function fields (also finite characteristic), and localizations $\mathfrak{o}_{F,(\mathfrak{p})}$ of rings of integers of number fields ([Neu99, Prop I.11.4]).

Using our definition, technically a field itself is also Dedekind domain, so one can always take $R = F$ to get, say, the archimedean fields $F = \mathbb{R}$ and $F = \mathbb{C}$. However our real interest here (unlike in Section 3.2) is when R is really is some ring of integers, so cases where $R = F$ are not so useful and there is no need to keep them in mind in this chapter.

On the other hand if R is an arbitrary order in a number field F, then R is not necessarily a Dedekind domain, as we saw in Example 1.4.5 (no prime factorization of ideals). However, one can still study general orders $\mathcal{O}$ in a number field K in this framework by viewing K as a $F = \mathbb{Q}$-algebra and $\mathcal{O}$ as an order over $R = \mathbb{Z}$. That said, eventually we will restrict to central simple algebras, which will exclude non-maximal commutative orders $\mathcal{O} \subset K$ since K is not central over $\mathbb{Q}$.

[1] Our assumptions on algebras from Chapter 2 are still in place: associative, unital, finite dimensional. However, we don't need to assume F does not have characteristic 2 as we did for most of Chapter 3.

My primary reference for this chapter is Reiner's book [Rei03]. Much of this (as well as a lot of other) material can be found in Reiner's survey [Rei70], which has additional references. Subsequently, we will focus more specifically on the arithmetic structure of quaternion algebras, as in [Vig80] or [MR03].

4.1 Integrality

Let R be a Dedekind domain with (characteristic zero) fraction field F, and let A be an F-algebra. The main examples to keep in mind are $R = \mathbb{Z}$ so $F = \mathbb{Q}$ and $R = \mathbb{Z}_p$ so $F = \mathbb{Q}_p$.

An element $\alpha \in A$ is **integral over** R (or R**-integral**) if $f(\alpha) = 0$ for some *monic* polynomial f with coefficients in R. When R is understood, we often just say α is integral.

Proposition 4.1.1. *The following are equivalent:*
(i) α is integral over R;
(ii) $R[\alpha]$ is a finitely-generated R-module; and
(iii) the minimal polynomial of α over F has coefficients in R.

Proof. Suppose α is integral. Let $f \in R[x]$ be a monic polynomial which annihilates α If f has degree n, then any $\alpha^j \in R[\alpha]$ can be expressed to an R-linear combination of $1, \alpha, \dots, \alpha^{n-1}$. Thus (i) $\implies$ (ii).

Now let $m_\alpha \in F[x]$ be the minimal polynomial of α. Then m_α divides any polynomial which kills α, in particular $m_\alpha | f$. Thus $f = m_\alpha g$ for some monic polynomial $g \in F[x]$. Gauss's lemma says that since f has coefficients in R, the coefficients of m_α and g must also lie in R. Hence (i) also implies (iii).

Note (iii) implies (i) is trivial, as we can take $f = m_\alpha$. The implication (ii) $\implies$ (i) is the exercise below. □

Exercise 4.1.1. Finish the proof of the above proposition by showing (ii) implies (i) (see [Rei03, Thm 1.10] if you wish).

Note that α being integral over $\mathbb{R}$ does not tell you anything about the coefficients of a matrix representation of α (even if you choose a nice basis).

Example 4.1.1. Let $R = \mathbb{Z}$ so $F = \mathbb{Q}$ and $A = M_2(\mathbb{Q})$. Consider $\alpha = \begin{pmatrix} 1 & a \\ & 1 \end{pmatrix}$. Then α is killed by the monic polynomial $(x-1)^2$, and thus is integral over $\mathbb{Z}$ for any $a \in \mathbb{Q}$. While this may seem strange at first, it makes sense that such α are integral because, for $a \neq 0$,

$$\alpha = \begin{pmatrix} a & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & \\ & 1 \end{pmatrix}$$

so if we want $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ to be integral, then its conjugates should also be for a purely abstract (basis free) definition of integral.

Exercise 4.1.2. Let A be a CSA over F. For $\alpha \in A$, show α is R-integral if and only if its (reduced) characteristic polynomial has coefficients in R. (*Hint:* the minimal and characteristic polynomials have the same irreducible factors.)

Corollary 4.1.2. *Let A be a CSA over F. If $\alpha \in A$ is integral, then the (reduced) norm $N(\alpha)$ and (reduced) trace $\mathrm{tr}(\alpha)$ are also integral (i.e., they lie in R). If A/F is a quaternion algebra, the converse is also true.*

Proof. This follows from the exercise as $N(\alpha)$ and $\mathrm{tr}(\alpha)$, up to signs, are coefficients in the (reduced) characteristic polynomial $p_\alpha(x)$. If A is quaternion, i.e., degree 2, then $p_\alpha(x) = x^2 - \mathrm{tr}(\alpha)x + N(\alpha)$, so the trace and norm being integral means all coefficients are. □

For the next result, we do not need to assume A is a CSA.

Lemma 4.1.3. *If $\alpha, \beta \in A$ commute and are integral over R, then $\alpha \pm \beta$ and $\alpha\beta$ are also integral over R.*

Proof. Suppose α, β commute and are integral. Then $R[\alpha]$ and $R[\beta]$ are subrings of A which are finitely generated as R-modules. Say they have bases $x_1, \ldots, x_m$ and $y_1, \ldots, y_n$. Then it is easy to see that the elements $x_i y_j$, $1 \le i \le m$, $1 \le j \le n$, contain a basis of $R[\alpha, \beta]$, and thus it is a finitely-generated R-module. Thus for any $\gamma \in R[\alpha, \beta]$, $R[\gamma]$ is a finitely generated R-module, whence γ is also integral by Proposition 4.1.1. □

This is not true if α, β do not commute, as the next example shows.

Example 4.1.2. Take $R = \mathbb{Z}$ so $F = \mathbb{Q}$ and put $A = M_2(\mathbb{Q})$. Then

$$\alpha = \begin{pmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{pmatrix}$$

are both killed by $f(x) = x^2$ whence both integral, but $\alpha + \beta$ is not integral because it has minimal polynomial $m(x) = x^2 - \frac{1}{4}$.

The **integral closure** of R in A is the set of all elements of A which are integral over R. The above lemma tells us the following.

Corollary 4.1.4. *If A is commutative, then the integral closure of R is a subring of A.*

Example 4.1.3. Let $R = \mathbb{Z}$, so $F = \mathbb{Q}$ and let $A = K$ be a finite extension of $\mathbb{Q}$. Then the integral closure of $\mathbb{Z}$ in K is the ring of integers $\mathcal{O}_K$ of K. (Often this is the definition of $\mathcal{O}_K$, and it is compatible upon "changing the base field F": if K/F is any extension of number fields then the integral closure of $R = \mathcal{O}_F$ in K is $\mathcal{O}_K$.) A similar statement is true for finite extensions of $\mathbb{Q}_p$.

Note Example 4.1.2 shows the integral closure of a non-commutative algebra A is not in general a ring, so the term "the ring of integers" will not make sense. But let's think about what one can hope for.

Suppose we have a quaternion algebra $B = \left(\frac{a,b}{F}\right)$, then $\alpha = x + yi + zj + wk \in B$ is integral if and only if

$$\mathrm{tr}\alpha = 2x \in R \quad \text{and} \quad N(\alpha) = x^2 - ay^2 - bz^2 + abw^2 \in R. \tag{4.1.1}$$

Let

$$\mathcal{O} = \{x + yi + zj + wk : x, y, z, w \in R\} \subset B. \tag{4.1.2}$$

Then any $\alpha \in \mathcal{O}$ is integral over R by (4.1.1). Further, it is clear that $\mathcal{O}$ is a subring of R, and thus sort of analogous to the ring of integers in a number or p-adic field (actually, it is more analogous to an order in a number or p-adic field as it may not be maximal among rings contained in the integral closure of R in A, as the exercise below shows). The ring $\mathcal{O}$ will be an example of such an order in B, once we define orders in algebras.

Exercise 4.1.3. Let $B = \mathbb{H}_{\mathbb{Q}} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Consider the ring $\mathcal{O} = \mathbb{Z}[i, j, \frac{1+i+j+k}{2}]$ in B. Show $\mathcal{O}$ is contained in the integral closure of $\mathbb{Z}$ in $\mathbb{H}_{\mathbb{Q}}$. We call $\mathcal{O}$ the **Hurwitz integers**.

Here is a general fact about integrality and direct sums.

Exercise 4.1.4. Let A and B be F-algebras. Then, for $\alpha \in A$ and $\beta \in B$, show (α, β) is integral in $A \oplus B$ if and only if α and β are both R-integral. Deduce that the integral closure of the semisimple commutative algebra $A = \bigoplus_{i=1}^n F$ is $\bigoplus_{i=1}^n R$.

4.2 Orders

We define orders in algebras analogously to our definition for number fields from Section 1.4. Recall that in that section we defined a an order in a number field K to be complete $\mathbb{Z}$-lattice in K (i.e., a finitely-generated $\mathbb{Z}$-module which generates K over $\mathbb{Q}$) which is also a subring of K. First we generalize our definition of $\mathbb{Z}$-lattices to R-lattices.

Let V be a finite dimensional vector space over F, the fraction field of our Dedekind domain R. An **R-lattice** in V is a subset $\Lambda \subset V$ such that Λ is a finitely-generated module over R. (Since R is commutative, there is no difference between defining left and right actions, so we can consider right modules as left modules and vice versa. For definiteness, we will work with left R-modules.) Here the R-action on Λ is just taken to be the restriction to R of scalar multiplication on V. When $R = \mathbb{Z}$ this definition agrees with the one in Section 1.4.

Example 4.2.1. Let $V = F$. Since any Dedekind domain is Noetherian (i.e., satisfies the ACC), any ideal $\mathcal{I} \subset R$ is finitely generated and thus an R-lattice in F.

Over a general Dedekind domain R, an R-lattice Λ need not be a free module. If R is a PID, e.g. if $R = \mathbb{Z}$ or R is the ring of integers of a p-adic field, then Λ must be free by Corollary 1.1.2. But otherwise, e.g. if $R = \mathfrak{o}_F$ is the ring of integers of a number field with class number > 1, about the most one can say say is that Λ is a *projective module.* For instance, there can be ideals $\mathcal{I}$ of $\mathfrak{o}_F$, which are necessarily finitely generated and torsion-free, that are not free $\mathfrak{o}_F$-modules.

We say an R-lattice $\Lambda \subset V$ is **complete** (or **full**) if $V = F \cdot \Lambda$, i.e., if Λ contains a basis of V. Thus if $e_1, \dots, e_n$ is any basis for V,

$$\Lambda = R\langle e_1, \dots, e_n \rangle := \{r_1 e_1 + \cdots r_n e_n : r_i \in R\}$$

is a complete lattice in V.

Sometimes one defines lattices just as finitely-generated torsion-free R-modules, rather than as specifying them as subsets of a particular vector space. Recall torsion-free means that $rx = 0$ for $r \in R$, $x \in \Lambda$ implies $r = 0$ or $x = 0$. (In fact [Rei03] makes one definition in one section, and the other in another section.) However, these definitions are equivalent. Namely, given a set of independent generators $e_1, \dots, e_n$ for a torsion free R-module, so any $x \in \Lambda$ can be written uniquely in the form $r_1 e_1 + \cdots r_n e_n$ with $r_i \in R$, we can extend Λ to an F-vector space $V = \{\sum a_i e_i : a_i \in F\}$. Conversely, given a lattice Λ in some F-linear space V, the action of V (and therefore of R) must be torsion free.

In the last paragraph, we started with a torsion-free R-module Λ and used it to generate an F-vector space V. But if we start with Λ a lattice in V, we can still take the vector space W generated by Λ, which will be a vector subspace of V. Then we see Λ being complete in V just means the vector space Λ generates is all of V.

> **Example 4.2.2.** Let $V = A$ be an F-algebra. Then R itself is a lattice in V, but it is only complete if $\dim_F A = 1$.

Lattices are an analogue of vector spaces over a ring. Of course, general modules are also, but we've eliminated a lot of "bad" things that can happen with modules in the definition of lattices (bad meaning our intuition from vector spaces fails): the ring R must be commutative and have no zero divisors (and have prime factorization of ideals), the R-action cannot have torsion, and we have a finite set of generators.

Definition 4.2.1. *Let A be an F-algebra. An* **order** *(or* **arithmetic***) in A over R is a complete R-lattice $\mathcal{O}$ in A which is a subring of A.*

The terminology order is standard now, and most people probably won't know what you mean by an arithmetic, which is old terminology I believe introduced by Dickson. However, I like the term arithmetic, and may occasionally use it, but will typically use the modern term order. (I think of the term "order" as in "Order of the Phoenix," or maybe when I'm hungry "an Order of Fries," but definitely not in the sense of "an ordered set" or "order your math books by color.")

When we want to specify R we may say R-order, but often R will be understood and we will just say "an order" or "an order in A."

Just like an algebra is a vector space over a field which is also a ring, i.e., you can multiply your vectors, an order is a module (lattice) over a ring which is itself a ring. Technically A itself an F-order in A, though as mentioned above, we are really interested in the case of R-orders where R is a ring of integers, so we can think of order as being an integral version of the notion of algebra. As a nonzero F-algebra A contains F, an R-order $\mathcal{O}$ in a nonzero algebra A contains R, since $\mathcal{O}$ being a ring means $\mathcal{O}$ contains 1 and $\mathcal{O}$ is also a (say left) R-module.

It takes little imagination to define suborders: we say that $\mathcal{O}'$ is a **suborder** of $\mathcal{O}$ in A if $\mathcal{O}'$ and $\mathcal{O}$ are both R-orders in A such that $\mathcal{O}' \subset \mathcal{O}$. Note that since $\mathcal{O}'$ and $\mathcal{O}$ are subrings of A, $\mathcal{O}' \subset \mathcal{O}$ means in fact $\mathcal{O}'$ is a subring of $\mathcal{O}$ (identities and operations agree).

Example 4.2.3. Let $B = \left(\frac{a,b}{F}\right)$ and $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rk$ as in (4.1.2). Then $\mathcal{O}$ is an order.

Alternatively, if a is a nonsquare, using the matrix representation

$$B = \left\{ \begin{pmatrix} \alpha & b\beta \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\},$$

from (3.1.7) where $K = F(\sqrt{a})$, we can write

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & b\beta \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathfrak{o} \right\},$$

where $\mathfrak{o} = R \oplus Ri \subset K$, which may or may not be the full ring of integers $\mathfrak{o}_K$ of $K = F(i)$. If $\mathfrak{o}$ is a proper suborder of $\mathfrak{o}_K$, then $\mathcal{O}$ is a proper suborder of

$$\mathcal{O}' = \left\{ \begin{pmatrix} \alpha & b\beta \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathfrak{o}_K \right\}.$$

In the special case $R = \mathbb{Z}$ and $A = \mathbb{H}_{\mathbb{Q}} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$, this construction gives the order $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$, which is called the ring of **Lipschitz integers**. The Hurwitz integers $\mathcal{O}' = \mathbb{Z}[i, j\frac{1+i+j+k}{2}]$ from Exercise 4.1.3 are also an order, and $\mathcal{O}$ is a suborder of $\mathcal{O}'$.

Example 4.2.4. $M_n(R)$ is an order in $A = M_n(F)$. In particular, $M_n(\mathbb{Z})$ and $M_n(\mathbb{Z}_p)$ are orders in $M_n(\mathbb{Q})$ and $M_n(\mathbb{Q}_p)$ (taking $R = \mathbb{Z}$ and $R = \mathbb{Z}_p$, respectively). When $n = 1$, this just says R is an R-order in F.

We can also consider suborders of $M_n(R)$. For instance, let $\mathfrak{m}$ be an (integral) ideal in R, e.g., $m\mathbb{Z}$ if $R = \mathbb{Z}$. Let $\mathcal{O}(\mathfrak{m})$ be the subring of $M_n(R)$ consisting of the matrices which are upper triangular mod $\mathfrak{m}$, i.e., are congruent to upper triangular matrices mod $\mathfrak{m}$. (Reducing a matrix mod $\mathfrak{m}$ means reducing reducing each entry mod $\mathfrak{m}$.) For instance, if $n = 2$, we have

$$\mathcal{O}(\mathfrak{m}) = \begin{pmatrix} R & R \\ \mathfrak{m} & R \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, d \in R, \, c \in \mathfrak{m} \right\}$$

Then $\mathcal{O}(\mathfrak{m})$ is an order in A. When $n = 2$, these orders play an important role in the theory of modular forms (normally one looks at the group of determinant 1 elements, denoted $\Gamma_0(\mathfrak{m})$).

Exercise 4.2.1. (i) With notation as in the previous example, consider the subsets of $A = M_2(F)$ of the form $\mathcal{O} = \begin{pmatrix} \mathcal{I}_1 & \mathcal{I}_2 \\ \mathcal{I}_3 & \mathcal{I}_4 \end{pmatrix}$ where each $\mathcal{I}_i \in \{R, \mathfrak{m}\}$ and $\mathfrak{m}$ denotes a fixed nonzero proper ideal in R. Show that $\mathcal{O}$ is an R-lattice in A. Determine which $\mathcal{O}$ are orders in A.

(ii) Do the same for $A = M_3(F)$, except now allow each $\mathcal{I}_i \in \{R, \mathfrak{m}, \mathfrak{m}^2\}$.

Exercise 4.2.2. If $\mathcal{O}$ is an R-order in an F-algebra A, then for any $x \in A^\times$, show the conjugate $x\mathcal{O}x^{-1}$ is also an R-order in A.

This gives a way of constructing new orders from old ones.

Example 4.2.5. If $A = M_2(F)$, $\mathcal{O} = M_2(R)$, $m \in F^\times$ and $x = \begin{pmatrix} 1 & \\ & m \end{pmatrix} \in A^\times$, we see

$$x\mathcal{O}x^{-1} = \left\{ \begin{pmatrix} a & m^{-1}b \\ mc & d \end{pmatrix} : a, b, c, d \in R \right\}$$

is also an order in A.

To justify the notion of thinking of orders as integral version of algebras, we show that all elements of orders are integral. (Recall integrality is a condition about minimal polynomials, so even though you might naively think $\begin{pmatrix} 1 & 2 \\ \frac{1}{2} & 1 \end{pmatrix} \in M_2(\mathbb{Q})$ is should not be called integral, it is integral over $\mathbb{Z}$—it just happens to not lie in the particular order $M_2(\mathbb{Z})$, but rather a conjugate order (cf. the previous example).

Proposition 4.2.2. *Let $\mathcal{O}$ be an R-order in an F-algebra A. Then each $x \in \mathcal{O}$ is integral over R.*

Proof. For any $\alpha \in \mathcal{O}$, $R[\alpha]$ is a finitely-generated R module, thus integral by Proposition 4.1.1. □

Note that this is compatible with Exercise 4.2.2 as conjugate elements have the same minimal polynomials.

Thus R-orders in A are subrings $\mathcal{O}$ consisting of integral elements such that $F\mathcal{O} = A$. Though we do not do it here, one can prove the converse for *separable* F-algebras: any subring $\mathcal{O} \subset A$ contained in the integral closure of R such that $F\mathcal{O} = A$ is an order in A ([Rei03, Thm 10.3]). Here A being **separable** over F means that A is semisimple and the center of each simple component is a separable field extension of F. This holds, for instance, if A is any semisimple algebra and F has characteristic 0, or if F is any field and A is a

CSA over F. In particular, all of our cases of primary interest (CSAs over characteristic zero fields) satisfy this separability condition, which will arise in some other results we quote from [Rei03] below.

Since we will invoke other results from [Rei03] on separable algebras below, we will often assume A is separable, though this is not needed for everything we will do.

Here is another useful consequence of knowing integrality.

Corollary 4.2.3. *Suppose F is a p-adic or number field, A is an F-algebra and $\mathcal{O}$ is an $\mathfrak{o}_F$-order in A. Then $\mathcal{O} \cap F = \mathfrak{o}_F$ and $\mathcal{O}^\times \cap F^\times = \mathfrak{o}_F^\times$.*

Proof. Since $1 \in \mathcal{O}$ we know $\mathfrak{o}_F \cdot 1 = \mathfrak{o}_F \subset \mathcal{O}$. By the proposition, any element of $\mathcal{O} \cap F$ is an element of F which is integral over $\mathfrak{o}_F$. Since $\mathfrak{o}_F$ is integrally closed, we also get $\mathcal{O} \cap F \subseteq \mathfrak{o}_F$. The statement for $\mathcal{O}^\times \cap F^\times$ follows as this group is the same as $(\mathcal{O} \cap F)^\times$. □

Maximal orders

As mentioned in the previous section, one difficulty in moving from the study of arithmetic in fields to arithmetic in division, or more generally simple, algebras is the lack of a ring of integers, as the collection of all integral elements may not form a ring. Instead, we look at collections which do, and these are precisely the orders of A. The analogue of the ring of integers $\mathcal{O}_K$ of a field K is then the notion of a **maximal order**, i.e., an R-order in A which is maximal with respect to inclusion.

Corollary 4.2.4. *Suppose A is a commutative semisimple F-algebra. Then there is a unique maximal R-order $\mathcal{O}$ in A, namely the ring of all R-integral elements of A. In particular, finite degree field extensions of F have unique maximal R-orders.*

Proof. By Corollary 4.1.4 we know the set $\mathcal{O}$ of all integral elements in A is a ring. It is also an R-module. Since A is semisimple, it is a direct sum of extension fields K_i of F (as finite degree field extensions are the only commutative simple F-algebras by Wedderburn), say $A \simeq K_1 \oplus \cdots \oplus K_n$. From Exercise 4.1.4, $\mathcal{O} \simeq \mathcal{O}_{K_1} \oplus \cdots \mathcal{O}_{K_n}$. Since $F\mathcal{O}_{K_i} = K_i$ for each i, we see that $\mathcal{O}$ is a complete lattice in A, and thus an order. But the above proposition says that $\mathcal{O}$ contains all other orders. □

> **Example 4.2.6.** Let K be a number field, viewed as an $F = \mathbb{Q}$-algebra. Then the ring of integers $\mathcal{O}_K$ of K is the unique maximal $\mathbb{Z}$-order in K. There are other $\mathbb{Z}$-orders. For instance, if $K = \mathbb{Q}(\sqrt{-3})$ so $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, then $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ is a $\mathbb{Z}$-order in K.

In the previous example, we saw the non-maximal $\mathbb{Z}$-order $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ in $K = \mathbb{Q}(\sqrt{-3})$. The field of fractions of $\mathcal{O}$ is K, and you might wonder if you can look at $\mathcal{O}$-orders in K-algebras, just like you could look at $\mathcal{O}_K$ orders. Recall from Example 1.4.5 that $\mathcal{O}$ does not have prime factorization of ideals, and thus is not a Dedekind domain, so $\mathcal{O}$-orders are excluded from our setup.[2]

For your ease of mind, we state the following result, but will not prove it:

Theorem 4.2.5. *Any order in a separable (semisimple) F-algebra A is contained in a maximal order. In particular, A has at least one maximal order.*

Proof. See [Rei03, Cor 10.4]. The idea is to use Zorn's lemma and the fact that R is Noetherian. □

For noncommutative algebras, there may be many maximal orders, and we will see later that they need not even be isomorphic to each other. (Though it can happen that there is a unique maximal order in the noncommutative case—we will see this below for division algebras over p-adic fields.) Construction and determination of the maximal orders in an algebra is one of the basic problems in the arithmetic of algebras. We remark that for separable semisimple F-algebras, maximal orders will be direct sums of maximal orders of the simple components, and the study of maximal orders can be reduced to the case of (separable) simple algebras, and in fact to CSAs. At least for matrix algebras, there is an obvious construction.

Theorem 4.2.6. *Let D be a division algebra over F. If $\mathcal{O}_D$ is a maximal R-order in D, then $M_n(\mathcal{O}_D)$ is a maximal order in $M_n(D)$.*

Proof. In fact this is true with D replaced by an arbitrary algebra A; see [Rei03, Thm 8.7]. □

For applications to quaternion algebras, we only need to know the following special case:

> **Exercise 4.2.3.** Show $M_2(R)$ is a maximal R-order in $M_2(F)$.

> **Exercise 4.2.4.** Let $\mathcal{O}$ be a maximal order in A and $x \in A^\times$. Show $x\mathcal{O}x^{-1}$ is also a maximal order in A.

Theorem 4.2.7. *Let F be a p-adic field and A a CSA over F. Then all maximal orders in A are conjugate. In particular, any maximal order in $M_n(F)$ is conjugate to $M_n(\mathfrak{o}_F)$.*

Proof. See [Rei03, Thm 18.7]. □

One can also ask about constructing non-maximal orders. These are important in the theory of modular forms, for instance. One way to construct non-maximal orders is via intersection.

> **Exercise 4.2.5.** (i) Let $\mathcal{O}$ and $\mathcal{O}'$ be orders in A. Show $\mathcal{O} \cap \mathcal{O}'$ is also an order in A.
>
> (ii) The only thing that is not obvious is in (i) that the intersection must be a complete lattice. Indeed, show that the intersection of two complete $\mathbb{Z}$-lattices in $\mathbb{R}^n$ (submodules of $\mathbb{R}^n$ which are free of rank n) can be $\{0\}$. Why doesn't this conflict with (i)?

[2] I have not thought carefully about what will happen if one tries to work over non-Dedekind domains, but I suspect ideal theory for $\mathcal{O}$-orders will not be as nice as for $\mathcal{O}_K$-orders.

The intersection of two maximal orders in a quaternion algebra, called an **Eichler order**, is a type of order that plays a special role in number theory.

> **Example 4.2.7.** We know $\mathcal{O} = M_2(R)$ is a maximal order in $A = M_2(F)$. In Example 4.2.5, we considered the conjugate order
>
> $$\mathcal{O}' = \begin{pmatrix} 1 & \\ & m \end{pmatrix} \mathcal{O} \begin{pmatrix} 1 & \\ & m^{-1} \end{pmatrix} = \left\{ \begin{pmatrix} a & m^{-1}b \\ mc & d \end{pmatrix} : a, b, c, d \in R \right\},$$
>
> which is also a maximal order in A by Exercise 4.2.4. Suppose $m \in R - \{0\}$. Then
>
> $$\mathcal{O}(m) = \mathcal{O} \cap \mathcal{O}' = \left\{ \begin{pmatrix} a & b \\ mc & d \end{pmatrix} : a, b, c, d \in R \right\}$$
>
> is an Eichler order in A, which arose in Example 4.2.4. If $R = \mathbb{Z}$, the multiplicative subgroup of determinant 1 elements
>
> $$\mathcal{O}(m)^1 = \Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod m \right\}$$
>
> is a congruence subgroup that appears in the theory of modular forms.

Left and right orders

Here is another way to construct R-orders in an algebra A, which will be important for ideal theory. Let Λ be a complete R-lattice in A. The **left order** of Λ is

$$\mathcal{O}_l(\Lambda) = \{\alpha \in A : \alpha\Lambda \subset \Lambda\}.$$

Similarly, the **right order** of Λ is

$$\mathcal{O}_r(\Lambda) = \{\alpha \in A : \Lambda\alpha \subset \Lambda\}.$$

Proposition 4.2.8. *The left and right orders $\mathcal{O}_l(\Lambda)$ and $\mathcal{O}_r(\Lambda)$ are R-orders in A.*

Proof. It is clear that $\mathcal{O}_l(\Lambda)$ and $\mathcal{O}_r(\Lambda)$ are subrings of A. So it suffices to check $\mathcal{O}_l(\Lambda)$ is a complete R-lattice, with the case of $\mathcal{O}_r(\Lambda)$ being analogous.

Since Λ is complete, $1 \in x\Lambda$ for some $x \in F^\times$. For any $\alpha \in \mathcal{O}_l(\Lambda)$ we have $\alpha = \alpha \cdot 1 \in \alpha x\Lambda \subset x\Lambda$, i.e, $\mathcal{O}_l(\Lambda) \subset x\Lambda$. That is, $\mathcal{O}_l(\Lambda)$ is a submodule of the finitely-generated torsion-free R-module $x\Lambda$. Since A is torsion-free, so is $\mathcal{O}_l(\Lambda)$. Over Dedekind domains, any submodule of a finitely-generated module is also finitely-generated (this is the *Noetherian property* for modules), whence $\mathcal{O}_l(\Lambda)$ is a lattice. In the special case R is PID, one could instead use that $x\Lambda$ must be a free module of finite rank and its submodules are also free of finite rank (cf. Section 1.1.2), so $\mathcal{O}_l(\Lambda)$ is a lattice.

Now it suffices to show $\mathcal{O}_l(\Lambda)$ is complete. Take any $\alpha \in A$. Then $\alpha\Lambda$ is also a lattice in A. Fix a set of generators $g_1, \dots, g_k$ of $\alpha\Lambda$. Again, since Λ is complete, there exists $r \in R$ such that $rg_i \in \Lambda$ for each $1 \le i \le k$. Thus $r\alpha\Lambda \subset \Lambda$, i.e., $r\alpha \in \mathcal{O}_l(\Lambda)$. Hence $F\mathcal{O}_l(\Lambda) = A$. □

Exercise 4.2.6. Prove that same construction for $\mathcal{O}_l(\Lambda)$ need not be an order if Λ is not complete (defining $\mathcal{O}_l(\Lambda)$ in the same way).

Example 4.2.8. If $\mathcal{O}$ is an R-order, $1 \in \mathcal{O}$ implies that

$$\mathcal{O}_l(\mathcal{O}) = \mathcal{O}_r(\mathcal{O}) = \mathcal{O}.$$

In fact we have the following simple generalization:

Exercise 4.2.7. Let $\lambda \in F^\times$ and $\mathcal{O}$ be an R-order in the F-algebra A. Set $\Lambda = \lambda\mathcal{O}$. Show $\mathcal{O}_l(\Lambda) = \mathcal{O}_r(\Lambda) = \mathcal{O}$.

Exercise 4.2.8. Let $R = \mathbb{Z}$ consider the $\mathbb{Q}$-algebra $K = \mathbb{Q}(i)$ with lattice $\Lambda = 2\mathbb{Z} \oplus \mathbb{Z}i$. Determine $\mathcal{O}_l(\Lambda)$.

4.3 Orders in local division algebras

In this section, we assume F is a p-adic field, $R = \mathfrak{o}_F$ is its ring of integers and D is a division algebra over F (not necessarily central, so D could in fact be a p-adic field extension of F). If D is not central, we define the **reduced norm** $N = N_{D/F} := N_{K/F} \circ N_{D/K}$ where $K = Z(D)$.

Let $v = v_F : F \to \mathbb{Z} \cup \{\infty\}$ be the (normalized) $\mathfrak{p}$-adic valuation on F. Denote by $\mathfrak{p}$ the unique prime ideal of $\mathfrak{o}_F$ and by $\varpi = \varpi_F$ a uniformizer for $\mathfrak{o}_F$.

Proposition 4.3.1. *An element $\alpha \in D$ is $\mathfrak{o}_F$-integral if and only if the reduced norm $N(\alpha) \in \mathfrak{o}_F$.*

Proof. We've already observed that if α is integral, so is $N(\alpha)$. Conversely, suppose $N(\alpha) \in \mathfrak{o}_F$. Let $m_\alpha(x) = x^d + c_{d-1}x^{d-1} \cdots + c_1x + c_0$ be the minimal polynomial of α. Here $c_0 = \pm N(\alpha) \in \mathfrak{o}_F$. We claim that each $c_j \in \mathfrak{o}_F$, which will imply the proposition. Suppose not. Say j is minimal such that $v(c_j)$ is minimal and let $r = -v(c_j) > 0$. Then $\varpi^r m_\alpha(x) \in \mathfrak{o}_F[x]$ and

$$\varpi^r m_\alpha(x) \equiv \varpi^r c_{d-1}x^{d-1} + \cdots + \varpi^r c_j x^j \equiv x^j(\varpi^r c_{d-1}x^{d-r-1} + \cdots + \varpi^r c_j) \equiv \mod \mathfrak{p},$$

i.e., this polynomial is reducible mod $\mathfrak{p}$. Using Hensel's lemma, one can conclude that $\varpi^r m_\alpha(x)$ is reducible over $\mathfrak{o}_F$, contradicting the irreducibility of $m_\alpha(x)$. □

We define the **(normalized) valuation** on D to be the function $v_D : D \to \mathbb{Z} \cup \{\infty\}$ given by

$$v_D(\alpha) = v_F(N(\alpha)).$$

Then v_D satisfies the following properties:

(1) $v_D(\alpha) = \infty \iff \alpha = 0$;

(2) $v_D(\alpha) \geq 0 \iff \alpha$ is integral;

(3) $v_D(\alpha\beta) = v_D(\alpha) + v_D(\beta)$; and

(4) $v_D(\alpha + \beta) \geq \min \{v_D(\alpha), v_D(\beta)\}$.

(In Section 1.3, we only defined valuations on fields, but one can define them also for skew-fields by asking as functions satisfying properties (1), (3) and (4).)

Exercise 4.3.1. Check the above properties of v_D.

Theorem 4.3.2. *The set $\mathcal{O}_D = \{\alpha \in D : v_D(\alpha) \geq 0\}$ is the integral closure of $\mathfrak{o}_F$ in D. Thus $\mathcal{O}_D$ is the unique maximal $\mathfrak{o}_F$-order in D.*

Proof. Provided $\mathcal{O}_D$ is an order, it must contain all other orders in D by Proposition 4.2.2. It is clear from the properties of v_D that $\mathcal{O}_D$ is a ring. It is also a torsion-free $\mathfrak{o}_F$-module, so to show $\mathcal{O}_D$ is a lattice it suffices to show it is finitely generated. Showing finite generation does not require anything sophisticated, but is a little tedious and we refer to [Rei03, Thm 13.3]. □

This combined with results mentioned in the previous section yields:

Corollary 4.3.3. *Any maximal order in $M_n(D)$ is conjugate to $M_n(\mathcal{O}_D)$.*

We will now mention a few additional structural results on central $\mathfrak{p}$-adic division algebras.

Theorem 4.3.4. *Suppose D is a central division algebra over F of degree n. Then $v_D : D \to \mathbb{Z} \cup \{\infty\}$ is surjective, i.e., there exists $\varpi_D \in D$ such that $v(\varpi_D) = 1$.*

Proof. See [Rei03, Thm 14.3] or [Pie82, Sec 17.7]. □

In this setting, we call ϖ_D as above a **uniformizer** for D. As with $\mathfrak{p}$-adic fields, uniformizers are only unique up to multiplication elements of $\mathcal{O}_D^\times = \{\alpha \in D : v_D(\alpha) = 0\}$. Since $v_D(\varpi_F) = n = \deg D$, we have $\varpi_F \mathcal{O}_D = \varpi_D^n \mathcal{O}_D$. We will define ideals in non-commutative orders below, and this statement says that when we extend the prime ideal $\mathfrak{p}$ to $\mathcal{O}_D$, it is a power of the prime ideal $\mathfrak{P} = \varpi_D \mathcal{O}_D$. Thus in analogy with the field extension case, since $\mathfrak{p}\mathcal{O}_D = \mathfrak{P}^n$, we say D/F is **ramified** if $n > 1$.[3]

Any p-adic field F has a unique unramified extension of a given degree (this was stated in Theorem 1.2.10, though just for $F = \mathbb{Q}_p$).

Corollary 4.3.5. *Suppose D is a central division algebra over F of degree n. Then D contains, as a subfield, the unique unramified extension of F of degree n.*

[3] As with nonarchimedean field extensions, one can define ramification index and inertia degrees for nonarchimedean division algebras (see [Rei03] or [Pie82]), and in our setting both of these will be equal to n.

Proof. The idea is to use residue fields to show $K = F(\varpi_D)$ is a maximal subfield. Then K must be unramified becase $v(N_{K/F}(\varpi_D)) = v(N_{D/F}(\varpi_D)) = 1$. See [Rei03, Sec 14] or [Pie82, Cor 17.7a]. □

Corollary 4.3.6. *Suppose D is a central division algebra over F of degree n. Then the reduced norm $N : D \to F$ is surjective.*

In fact this is true for central simple algebras over p-adic fields (cf. [Wei95, Prop X.6]), though it is not true without the central hypothesis (cf. Theorem 1.2.14).

Proof. By Theorem 4.3.4, $N(\varpi_D) \in \varpi_F \mathfrak{o}_F^\times$, so it suffices to show the $N : \mathcal{O}_D^\times \to \mathfrak{o}_F^\times$ is surjective. By Corollary 4.3.5, D contains the unramified extension K/F of degree $\deg_F D$. But $N_{K/F} : \mathfrak{o}_K^\times \to \mathfrak{o}_F^\times$ is surjective, and Exercise 2.5.2 tells us $N_{K/F} = N_{D/F}$ for $\alpha \in K \subset D$, so we are done. □

Corollary 4.3.5 plays an important role in classifying the CSAs of degree n over p-adic fields, as we will explain later in the quaternion case. In fact a stronger statement is true.

Theorem 4.3.7. *Suppose D is a central division algebra over F of degree n and K/F any extension of $\mathfrak{p}$-adic fields of degree m. Then K is a subfield of D if and only if $m|n$.*

Proof. We already know $m|n$ is a necessary condition. That it is sufficient is [Pie82, Exer 17.10.4]. □

This says that, over $\mathfrak{p}$-adic fields, division algebras contain precisely the same subfields (i.e., all of them of the right degree) as matrix algebras $M_n(F)$.[4] This is not true over number fields—if K/F is an extension of number fields, for K to embed in a division algebra D/F, it is necessary that D splits wherever K does.

Using the maximal order, we can construct other orders in an analogous way to the case of number fields (cf. Proposition 1.4.3).

Exercise 4.3.2. Let D be a central division algebra over F. Show $\mathcal{O}_D(n) = \mathfrak{o}_F + \varpi_D^n \mathcal{O}_D$ is an order in D for $n \in \mathbb{N}$.

Exercise 4.3.3. Show $B = \left(\frac{2,3}{\mathbb{Q}_3}\right)$ is a division algebra over $F = \mathbb{Q}_3$. Consider the lattices of the form $3^{e_1}\mathbb{Z}_3 \oplus 3^{e_2}\mathbb{Z}_3 i \oplus 3^{e_3}\mathbb{Z}_3 j \oplus 3^{e_4}\mathbb{Z}_3 k$ where each $e_i \in \{0, 1\}$. Determine which of these are orders.

[4] In terms of algebraic groups over p-adic fields, this implies that, for any CSA A of degree n, $A^\times$ contains all possible anisotropic tori $K^\times$ of dimension n. This fact is important in making sense of the (local and global) Jacquet–Langlands correspondence, which relates representations of $A^\times$ to representations of $\mathrm{GL}(n)$. We'll discuss the Jacquet–Langlands correspondence briefly for GL(2) in Section 7.5.

4.4 Ideals

Suppose F is the fraction field of a Dedekind domain R. In this section, we will assume A is a separable F-algebra, e.g. A can be any semisimple algebra if F has characteristic 0 or A can be any CSA for arbitrary F.

Let $\mathcal{O}$ be an R-order in A. We can define ideals for $\mathcal{O}$ just like we defined them in the case of orders of number fields.

A **(left) (integral) ideal** in $\mathcal{O}$ is an additive subgroup $\mathcal{I}$ of $\mathcal{O}$ such that $\mathcal{O}\mathcal{I} \subset \mathcal{I}$. In particular, integral ideals consist of R-integral elements. A **(left) (fractional) ideal** of $\mathcal{O}$ in A is a subset of the form $\lambda\mathcal{I}$ where $\lambda \in F^\times$ and $\mathcal{I}$ is an integral ideal. For brevity, we sometimes say $\mathcal{O}$-ideal to mean an ideal of $\mathcal{O}$.

> **Exercise 4.4.1.** Show a subset $\mathcal{I} \subset A$ is a fractional ideal of $\mathcal{O}$ if and only if $\mathcal{I}\alpha$ is an integral ideal of $\mathcal{O}$ for some $\alpha \in A^\times$.

We can similarly define the notion of a right ideal, which is different in general than the notion of a left ideal since A may be noncommutative.

> **Example 4.4.1.** Let $A = M_2(F)$, $\mathfrak{p}$ a nonzero prime ideal in R, $\mathcal{O} = M_2(\mathfrak{o}_F)$ and $\mathcal{I} = \begin{pmatrix} \mathfrak{p} & \mathcal{O} \\ \mathfrak{p} & \mathcal{O} \end{pmatrix}$. Then $\mathcal{I}$ is a left $\mathcal{O}$-ideal but not a right $\mathcal{O}$-ideal.

As is our convention with ideals in F, if we just say an ideal, by default we mean a fractional left ideal (which includes the case of integral ideals). However, if we say an ideal *in* $\mathcal{O}$, rather than an ideal *of* $\mathcal{O}$, we mean an integral ideal (hopefully I won't make I make a typo!).

We can also define fractional ideals without resorting to using integral ideals. To see this, first note that an integral ideal $\mathcal{I} \subset \mathcal{O}$ is an R-lattice in A: since $R \subset \mathcal{O}$, $\mathcal{I}$ must be an R-module and it will be finitely generated because R is Noetherian.

Conversely, any R-lattice $\Lambda \subset A$, say generated by $x_1, \dots x_m$ as an R-module. Write $\mathcal{O} = R\langle e_1, \dots, e_n\rangle$. We can write any $x_i = \sum a_{ij}e_j$ for some $a_{ij} \in F$. Then there exists $z \in F$ such that $zx_i = \sum b_{ij}e_j$ with each $b_{ij} \in \mathfrak{o}_F$ so $zx_i \in \mathcal{O}$. We can in fact choose z such that $zx_i \in \mathcal{O}$ simultaneously for $1 \le i \le m$. Hence there exists $z \in F$ such that $z\Lambda \subset \mathcal{O}$, so Λ is a fractional ideal if and only if $\mathcal{O}\Lambda \subset \Lambda$.

Hence we have an equality

$$\{\text{fractional (left) ideals of } \mathcal{O} \text{ in } A\} = \{R\text{-lattices } \mathcal{I} \text{ in } A \text{ such that } \mathcal{O}\mathcal{I} \subset \mathcal{I}\}.$$

Even though a left $\mathcal{O}$-ideal is not always a right $\mathcal{O}$-ideal, it will be a right ideal for *some* order. In fact, this idea will allow us to talk about ideals without fixing orders. Recall for a complete R-lattice $\mathcal{I}$, we have associated orders, namely the left order

$$\mathcal{O}_l(\mathcal{I}) = \{\alpha \in A : \alpha\mathcal{I} \subset \mathcal{I}\}$$

of $\mathcal{I}$ and the right order

$$\mathcal{O}_r(\mathcal{I}) = \{\alpha \in A : \mathcal{I}\alpha \subset \mathcal{I}\}$$

of $\mathcal{I}$.

Proposition 4.4.1. *For any complete R-lattice $\mathcal{I}$ in A, $\mathcal{I}$ is a left $\mathcal{O}_l(\mathcal{I})$-ideal and a right $\mathcal{O}_r(\mathcal{I})$-ideal.*

Proof. It is clear from the definition that $\mathcal{O}_l(\mathcal{I})\mathcal{I} \subset \mathcal{I}$ and $\mathcal{I}\mathcal{O}_r(\mathcal{I}) \subset \mathcal{I}$. □

We say $\mathcal{I}$ is a **complete** (or **full**) ideal if it is complete as a lattice. Clearly the zero ideal is not complete. Here is less trivial example.

> **Example 4.4.2.** Let $\mathcal{O} = M_2(R)$ in $A = M_2(F)$. Then $\mathcal{I} = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} : a, c \in R \right\}$ is a left $\mathcal{O}$-ideal which is not complete.

Essentially the only way for an ideal not to be complete is if there are zero divisors.

> **Exercise 4.4.2.** Let D be a division algebra over F and $\mathcal{O}$ an order in D. Show any nonzero ideal $\mathcal{I}$ of $\mathcal{O}$ is complete.

We will just focus on complete ideals.

From now on, all ideals are assumed to be complete unless indicated otherwise.

In light of the above proposition, the collection of (complete) ideals of $\mathcal{O}$, ranging over all orders $\mathcal{O}$ in A, is precisely the collection of complete R-lattices in A (and sometimes authors define ideals this way), i.e.,

$$\bigcup_{\mathcal{O}} \{(\text{complete left})\ \mathcal{O}\text{-ideals}\} = \{\text{complete } R\text{-lattices}\},$$

where $\mathcal{O}$ ranges over the R-orders in A.

Consequently, we can talk about ideals without even specifying orders. This will be convenient for some things, such as for the notion of inverses. However, our primary interest in ideals is to understand the ideals of a given order $\mathcal{O}$ in order to understand the arithmetic of $\mathcal{O}$.

Note that if $\mathcal{I}$ is an ideal, then $\mathcal{O}_l(\mathcal{I})$ (resp. $\mathcal{O}_r(\mathcal{I})$) is the *largest* order for which $\mathcal{I}$ is a left (resp. right) ideal. So if $\mathcal{I}$ is a left $\mathcal{O}$-ideal, it need not be the case that $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}$, but by definition of the left order, we always have $\mathcal{O}_l(\mathcal{I}) \supset \mathcal{O}$. Conversely, if $\mathcal{I}$ is a complete R-lattice in A, then $\mathcal{I}$ is a left $\mathcal{O}$-ideal for any suborder $\mathcal{O} \subset \mathcal{O}_l(\mathcal{I})$.

We call left ideals and right ideals **one-sided ideals**. If $\mathcal{I}$ is both a left and right $\mathcal{O}$-ideal, we say $\mathcal{I}$ is a **two-sided $\mathcal{O}$-ideal**. (A two-sided ideal is also considered a one-sided ideal.)

We can rephrase the condition of a ideal being a two-sided ideal in terms of left and right orders. Say $\mathcal{I}$ be is a left $\mathcal{O}$-ideal. Then $\mathcal{I}$ is a two-sided $\mathcal{O}$-ideal if and only if $\mathcal{O}_r(\mathcal{I}) \supset \mathcal{O}$.[5]

Note that $\mathcal{O}$ is always a two-sided $\mathcal{O}$-ideal. If we don't require ideals to be complete, the zero ideal is also a two-sided $\mathcal{O}$-ideal. The two-sided ideals 0 and $\mathcal{O}$ are the **trivial** ideals. If these are the only two-sided ideals in $\mathcal{O}$, then recall that means $\mathcal{O}$ is a simple ring. However, $\mathcal{O}$ is usually not simple, even when A is. For instance, take $A = M_n(F)$ and $\mathcal{O} = M_n(R)$. If $\mathfrak{p}$ is a prime (or even just nontrivial) ideal in R, then $\mathfrak{p}\mathcal{O} = M_n(\mathfrak{p})$ is a nontrivial two-sided ideal in $\mathcal{O}$.

The theory of two-sided ideals is considerably nicer than the theory of one-sided ideals, though our main interest is in one-sided ideals (some of which happen to also be two-sided). However, I'll include some basic facts about two-sided ideals both so you can see what we're missing and because it will be helpful in understanding the structure of one-sided ideals.

We will denote the set of (fractional complete) left $\mathcal{O}$-ideals by $\mathrm{Frac}(\mathcal{O}) = \mathrm{Frac}_l(\mathcal{O})$ and the right $\mathcal{O}$-ideals by $\mathrm{Frac}_r(\mathcal{O})$. Similarly, denote the two-sided $\mathcal{O}$-ideals by $\mathrm{Frac}_2(\mathcal{O})$.

Multiplicative structure of ideals

In algebraic number fields, the most important thing about ideals is that one can multiply them and get (abelian) groups of ideals and ideal classes. Let's investigate what we can say about ideals in algebras.

Suppose $\mathcal{I}$ and $\mathcal{J}$ are complete R-lattices in A, i.e., (complete, say left) ideals for some orders in A. Then the product

$$\mathcal{I}\mathcal{J} = \left\{ \sum_{i=1}^{j} x_i y_i : x_i \in \mathcal{I}, y_i \in \mathcal{J}, j \in \mathbb{N} \right\}$$

is just given by finite sums of products of elements in $\mathcal{I}$ and $\mathcal{J}$.

Exercise 4.4.3. Check $\mathcal{I}\mathcal{J}$ is a complete R-lattice in A with $\mathcal{O}_l(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_l(\mathcal{I})$ and $\mathcal{O}_r(\mathcal{I}\mathcal{J}) \supset \mathcal{O}_r(\mathcal{J})$. In particular, if $\mathcal{I}$ and $\mathcal{J}$ are both left or both right $\mathcal{O}$-ideals, then $\mathcal{I}\mathcal{J}$ also is.

So we can multiply $\mathcal{O}$-ideals to get another $\mathcal{O}$-ideal.

We define the **inverse** of a complete R-lattice $\mathcal{I}$ to be

$$\mathcal{I}^{-1} = \{\alpha \in A : \mathcal{I}\alpha\mathcal{I} \subset \mathcal{I}\}$$

Exercise 4.4.4. Show $\mathcal{I}^{-1}$ is a complete R-lattice in A such that

$$\mathcal{O}_l(\mathcal{I}^{-1}) \supset \mathcal{O}_r(\mathcal{I}), \quad \mathcal{O}_r(\mathcal{I}^{-1}) \supset \mathcal{O}_l(\mathcal{I}), \quad \mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I}), \quad \mathcal{I}^{-1}\mathcal{I} \subset \mathcal{O}_r(\mathcal{I}).$$

If $\mathcal{I}$ is a 2-sided ideal of a maximal order $\mathcal{O}$, show that $\mathcal{I}^{-1}$ is also an $\mathcal{O}$-ideal such that $\mathcal{I}\mathcal{I}^{-1} = \mathcal{I}^{-1}\mathcal{I} = \mathcal{O}$. (Showing $\mathcal{I}\mathcal{I}^{-1}$ is all of $\mathcal{O}$ is nontrivial.)

[5] In [Rei03], a two-sided ideal $\mathcal{I}$ is defined to be one for which $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}_r(\mathcal{I})$. This is the same as our definition of a two-sided $\mathcal{O}$-ideal if $\mathcal{O}$ is a maximal order.

One can use these two exercises to show that the (complete) two-sided ideals of a maximal order $\mathcal{O} \subset A$ form a group, and in fact we can talk about prime factorization.

If $\mathcal{I}$, $\mathcal{J}$ are $\mathcal{O}$-ideals such that $\mathcal{I} \supset \mathcal{J}$, we say $\mathcal{I}$ divides $\mathcal{J}$ and write $\mathcal{I}|\mathcal{J}$ as in the commutative case. Suppose $\mathfrak{P}$ is a nontrivial two-sided ideal in $\mathcal{O}$. We say $\mathfrak{P}$ is **prime** if $\mathfrak{P}|\mathcal{I}\mathcal{J}$ implies $\mathfrak{P}|\mathcal{I}$ or $\mathfrak{P}|\mathcal{J}$ for any two-sided ideals $\mathcal{I}, \mathcal{J}$.

Theorem 4.4.2. *Suppose $\mathcal{O}$ is a maximal R-order in A. Then $\mathrm{Frac}_2(\mathcal{O})$ is an abelian group with respect to multiplication, and any proper ideal factors into a product of powers of prime ideals in a unique way. Further, if $\mathcal{O}'$ is another maximal R-order in A, then $\mathrm{Frac}_2(\mathcal{O}) \simeq \mathrm{Frac}_2(\mathcal{O}')$.*

Proof. See [Rei03, Thm 22.10 and Cor 22.12, or Thm 23.6] for the first part. For the latter, see [Rei03, Thm 22.21] or Exercise 4.4.7. □

Note $\mathrm{Frac}_2(\mathcal{O})$, as we defined it, need not form a group if $\mathcal{O}$ is not maximal—one needs to restrict to invertible ideals. Though we have defined a notion of the "inverse" of a complete R-lattice, it may not be a group-theoretic inverse, i.e., $\mathcal{I}\mathcal{I}^{-1}$ need not be $\mathcal{O}$—cf. Example 1.4.4. More generally, take $\mathcal{I} \in \mathrm{Frac}_2(\mathcal{O}')$ with $\mathcal{O}$ a proper suborder of $\mathcal{O}'$. Then $\mathcal{I} \in \mathrm{Frac}_2(\mathcal{O})$, but $\mathcal{I}\mathcal{I}^{-1}$ can't be both $\mathcal{O}$ and $\mathcal{O}'$.

Since A is not commutative, the fact that product of two-sided ideals is commutative is not obvious. However, here is an example where it is easy to see.

Example 4.4.3. Let D be a division algebra over a p-adic field F. Let

$$\mathfrak{P}_n = \{\alpha \in D : v_D(\alpha) \geq n\}.$$

Then $\mathfrak{P}_n$ is a two-sided $\mathcal{O}_D$-ideal in D for $n \in \mathbb{Z}$, with $\mathfrak{P}_1 = \mathfrak{P}$ being a (in fact the unique) prime ideal. It is easy to check any nonzero $\mathcal{O}_D$-ideal in D is complete and of the form $\mathfrak{P}_n$ for some $n \in \mathbb{Z}$,

$$\mathrm{Frac}(\mathcal{O}_D) = \mathrm{Frac}_2(\mathcal{O}_D) \simeq \mathbb{Z}.$$

The isomorphism is given by the "valuation" of an ideal $v_D(\mathcal{I}) := \min\{v_D(\alpha) : \alpha \in \mathcal{I}\}$.

Exercise 4.4.5. Let $R = \mathbb{Z}$. Determine the complete two-sided ideals of $\mathcal{O} = M_2(\mathbb{Z})$ in $A = M_2(\mathbb{Q})$ and describe the group structure. Also determine the two-sided ideals of $\mathcal{O}$ which are not complete.

Now, what kind of structure can we get for one-sided ideals? For simplicity, let's say $\mathcal{O}$ is a maximal order in A and $\mathcal{I}$, $\mathcal{J}$ are left $\mathcal{O}$-ideals. Then $\mathcal{I}\mathcal{J}$ is also a left $\mathcal{O}$-ideal, but $\mathcal{I}^{-1}$ is a left $\mathcal{O}' = \mathcal{O}_r(\mathcal{I})$ ideal, so $\mathcal{I}^{-1}$ cannot be a left $\mathcal{O}$-ideal unless $\mathcal{O}' = \mathcal{O}$ by maximality of $\mathcal{O}$. Thus the category of nonzero left $\mathcal{O}$-ideals do not form a group in general.

Instead, we can put a different kind of algebraic structure on the class of one-sided ideals of maximal orders. Ideals of maximal orders are called **normal**. There is no difference between being normal or normal integral as a left ideal or a right ideal:

Proposition 4.4.3. *Let $\mathcal{I}$ be a complete R-lattice in A. Then $\mathcal{O}_l(\mathcal{I})$ is a maximal order if and only if $\mathcal{O}_r(\mathcal{I})$ is. If $\mathcal{I}$ is normal with left order $\mathcal{O}$ and right order $\mathcal{O}'$, then $\mathcal{I}$ is integral as a left $\mathcal{O}$-ideal if and only if it is integral as a right $\mathcal{O}'$-ideal, i.e., $\mathcal{I} \subset \mathcal{O}$ if and only if $\mathcal{O} \subset \mathcal{O}'$.*

Proof. See [Rei03, Thm 23.10 and Thm 22.9]. □

If $\mathcal{I}$ is a normal ideal, we simply say it is **integral** (without reference to an order) if it is integral for its left order, which is the same as being integral for its right order.

If $\mathcal{I}$ and $\mathcal{J}$ are complete R-lattices in A, we say the product $\mathcal{I}\mathcal{J}$ is **proper** if $\mathcal{O}_r(\mathcal{I}) = \mathcal{O}_l(\mathcal{J})$.

Lemma 4.4.4. *Suppose $\mathcal{I}$ and $\mathcal{J}$ are integral normal ideals in A. If the product $\mathcal{I}\mathcal{J}$ is proper, it is also an integral ideal.*

Proof. If the product is proper, then $\mathcal{I} \subset \mathcal{O}_l(\mathcal{J})$, so $\mathcal{I}\mathcal{J} \subset \mathcal{J} \subset \mathcal{O}_r(\mathcal{J}) = \mathcal{O}_r(\mathcal{I}\mathcal{J})$. □

While one doesn't have a nice theory of one-sided prime ideals, one can still talk about factorizations into one-sided maximal integral ideals, where maximal integral ideal means an integral normal ideal which is maximal as a left ideal in its left order (or equivalently, as a right ideal in its right order).

Theorem 4.4.5. *Let $\mathcal{I}$ be a nontrivial integral ideal. Then $\mathcal{I}$ factors into a proper product of maximal integral ideals, and the number of factors is independent of the factorization.*

Proof. See [Rei03, Thm 22.18 and Thm 22.24]. □

In fact, one can say a little more. Each maximal integral ideal $\mathcal{M}$ can be associated to a unique (two-sided) prime ideal $\mathfrak{P}$, and the collection of associated prime ideals is independent of the factorization. The association is not hard:

Exercise 4.4.6. Let $\mathcal{M}$ be a maximal left ideal of a maximal order $\mathcal{O}$. Show that $\mathfrak{P} = \{\alpha \in \mathcal{O} : \alpha\mathcal{O} \subset \mathcal{M}\}$ is a prime ideal of $\mathcal{O}$.

So while the one-sided ideals do not naturally form a group, because of no unique two-sided identities, proper products of ideals behave relatively nicely. This notion was formalized by Brandt (in the context of quaternion algebra): The **Brandt groupoid** $\mathrm{BG}(A)$[6] of A, is the collection of normal ideals of A with respect to proper products (i.e., we do not allow products of ideals which are not proper in this structure). The Brandt groupoid satisfies the following properties:

(1) For each $\mathcal{I} \in \mathrm{BG}(A)$, there exist left and right identities $e_l = \mathcal{O}_l(\mathcal{I})$ and $e_r\mathcal{O}_r(\mathcal{I})$ such that
$$e_l\mathcal{I} = \mathcal{I}e_r = \mathcal{I}.$$

(2) If $\mathcal{I}_1\mathcal{I}_2$ and $\mathcal{I}_2\mathcal{I}_3$ are defined, then so are $(\mathcal{I}_1\mathcal{I}_2)\mathcal{I}_3$ and $\mathcal{I}_1(\mathcal{I}_2\mathcal{I}_3)$, and they are equal.

[6] This is not standard notation, and I don't plan to use it again, so don't bother remembering it.

(3) For each $\mathcal{I} \in \mathrm{BG}(A)$ with left and right identities e_l and e_r, there exists $\mathcal{I}^{-1}$ such that

$$\mathcal{I}\mathcal{I}^{-1} = e_l, \quad \mathcal{I}^{-1}\mathcal{I} = e_r.$$

The formal definition of a groupoid is perhaps most cleanly stated in terms of categories. (The informal definition of a groupoid, is something like a group, but with only a partial multiplication defined and various identity elements.)

A **groupoid** is a category whose objects form a set and a set of morphisms which are all invertible. A group G is a groupoid with a single object, G, viewing the elements of G as invertible morphisms from G to itself. The Brandt groupoid is similarly a category where the objects correspond to the maximal orders $\mathcal{O}$, and you can think of each ideal $\mathcal{I}$ as being a morphism from $\mathcal{O} = \mathcal{O}_l(\mathcal{I})$ to $\mathcal{O}' = \mathcal{O}_r(\mathcal{I})$. Specifically, the proper product $\mathcal{O}\mathcal{I}$ turns the right $\mathcal{O}$-ideal $\mathcal{O}$ into the right $\mathcal{O}'$-ideal $\mathcal{I} = \mathcal{O}\mathcal{I}$. More generally, if $\mathcal{J}$ is any two-sided $\mathcal{O}$-ideal, then the proper product $\mathcal{J}\mathcal{I}$ is a right $\mathcal{O}'$-ideal. Similarly, the proper product $\mathcal{I}^{-1}\mathcal{J}$ is a left $\mathcal{O}'$-ideal and the proper product $\mathcal{I}^{-1}\mathcal{J}\mathcal{I}$ is a two-sided $\mathcal{O}'$-ideal.

> **Exercise 4.4.7.** Let $\mathcal{O}$ and $\mathcal{O}'$ be maximal orders in A. Let $\mathcal{I} = \mathcal{O}\mathcal{O}'$. Show the map given by the proper product $\mathcal{J} \mapsto \mathcal{I}^{-1}\mathcal{J}\mathcal{I}$ defines an isomorphism $\mathrm{Frac}_2(\mathcal{O}) \simeq \mathrm{Frac}_2(\mathcal{O}')$.

You can visualize the Brandt groupoid as a multi-graph, where each vertex is indexed by a maximal order $\mathcal{O}$. The self-loops at $\mathcal{O}$, i.e., the morphisms from $\mathcal{O}$ to itself, is just the group of two-sided $\mathcal{O}$-ideals. If $\mathcal{I}$ is a one-sided ideal with left order $\mathcal{O}$ and right order $\mathcal{O}'$, you can think of $\mathcal{I}$ as defining one directed edge (morphism) from $\mathcal{O}$ to $\mathcal{O}'$, i.e., a transition map from the group of two-sided $\mathcal{O}$-ideals to the two-sided $\mathcal{O}'$-ideals via $\mathcal{J} \mapsto \mathcal{I}^{-1}\mathcal{J}\mathcal{I}$. Then $\mathcal{I}^{-1}$ will be an edge with the reverse orientation. I find this graphic visualization a useful indicator as to why proper products are nicer to consider than non-proper products of ideals. See Fig. 4.4.1.

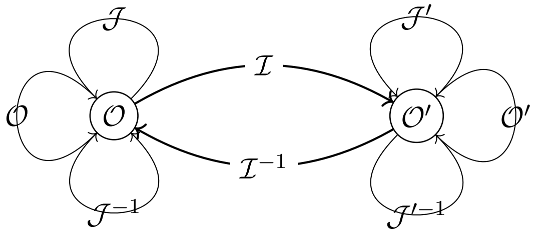

Figure 4.4.1: Part of a Brandt groupoid graph where $\mathcal{I}$ is a left $\mathcal{O}$- and right $\mathcal{O}'$-ideal, $\mathcal{J}$ is a 2-sided $\mathcal{O}$-ideal and $\mathcal{J}' = \mathcal{I}^{-1}\mathcal{J}\mathcal{I}$.

Note the proof that the groups of two-sided ideals for all maximal orders are isomorphic essentially uses the Brandt groupoid structure to transfer between groups for different maximal orders.

Ideal classes

Let $\mathcal{O}$ be an R-order in A and suppose $\mathcal{I}, \mathcal{J} \in \mathrm{Frac}(\mathcal{O})$. We say $\mathcal{I}$ and $\mathcal{J}$ are **equivalent** if $\mathcal{J} = \mathcal{I}\alpha$ for some $\alpha \in A^\times$, and write $\mathcal{I} \sim \mathcal{J}$ in this case. (Note $\mathcal{I}\alpha$ is a complete left

$\mathcal{O}$-ideal for any $\alpha \in A^\times$.) It is clear that $\sim$ defines an equivalence relation. The set of all left $\mathcal{O}$-ideals equivalent to $\mathcal{I}$ is called the **ideal class** of $\mathcal{I}$, which we denote by $[\mathcal{I}] = [\mathcal{I}]_l$. Let $\mathrm{Cl}(\mathcal{O}) = \mathrm{Cl}_l(\mathcal{O})$ denote the set of (left) ideal classes of $\mathcal{O}$, and define the (left) **class number** $h(\mathcal{O}) = \#\mathrm{Cl}(\mathcal{O})$ to be its cardinality.

One can similarly define the set $\mathrm{Cl}_r(\mathcal{O})$ of right ideal classes of $\mathcal{O}$.

Exercise 4.4.8. Suppose $\mathcal{O}$ is maximal. Show that $\mathcal{I} \mapsto \mathcal{I}^{-1}$ induces a bijection of $\mathrm{Cl}_l(\mathcal{O})$ with $\mathrm{Cl}_r(\mathcal{O})$. In particular, one does not need to distinguish between left and right class numbers.

Exercise 4.4.9. Suppose $\mathcal{O}$ and $\mathcal{O}'$ are maximal orders in A. Show $h(\mathcal{O}) = h(\mathcal{O}')$.

Note that a particular consequence is that, the class number is the same for all maximal orders. Thus it makes sense to call the class number of a maximal order the **class number** of A, and denote it h_A.

Unlike in the commutative case, one-sided ideal classes do not form a group in general.[7] One can still think of $\mathrm{Cl}(\mathcal{O})$ as ideals modulo principal ideals, but one has to be a little more careful.

A (complete left) **principal ideal** of $\mathcal{O}$ is a (complete) ideal generated by a single element, i.e., an ideal of the form $\mathcal{J} = \mathcal{O}\alpha$ for some $\alpha \in A^\times$. Note $\mathcal{O}_l(\mathcal{O}\alpha) = \mathcal{O}$ but

$$\mathcal{O}\alpha x \subset \mathcal{O}\alpha \implies x \in \alpha^{-1}\mathcal{O}\alpha$$

so $\mathcal{O}_r(\mathcal{O}\alpha) = \alpha^{-1}\mathcal{O}\alpha$. In particular $\mathcal{O}\alpha$ is not a two-sided $\mathcal{O}$-ideal unless α stabilizes $\mathcal{O}$ (under the action of $A^\times$ on A by conjugation), i.e., unless $\alpha\mathcal{O} = \mathcal{O}\alpha$. Write $\mathrm{Stab}_{A^\times}(\mathcal{O})$ for the set of such α. Note $\mathrm{Stab}_{A^\times}(\mathcal{O}) \supset Z(A)^\times\mathcal{O}^\times$.

Exercise 4.4.10. Show $\mathrm{Stab}_{A^\times}(\mathcal{O}) = Z(A)^\times\mathcal{O}^\times$ if A is a division algebra over a p-adic field.

Now if $\mathcal{I} \in \mathrm{Frac}(\mathcal{O})$, then we do not have $\mathcal{I}\alpha = \mathcal{I}\mathcal{O}\alpha$ in general, but we can always say $\mathcal{I}\alpha = \mathcal{I}(\mathcal{O}_r(\mathcal{I})\alpha)$. Thus the class $[\mathcal{I}]$ is the collection of left $\mathcal{O}$-ideals which are obtained from $\mathcal{I}$ by right multiplication by principal left $\mathcal{O}_r(\mathcal{I})$-ideals. Hence we may think of the ideal classes $H_l(\mathcal{O})$ as the left $\mathcal{O}$-ideals "properly" modulo principal ideals on the right, where "properly" modulo means one only considers proper products of left $\mathcal{O}$-ideals with principal ideals. (Though we only defined proper products in the case of normal ideals, we more generally say the product $\mathcal{I}\mathcal{J}$ is **proper** if $\mathcal{O}_l(\mathcal{J}) = \mathcal{O}_r(\mathcal{I})$.) In other words, ideal classes are ideals modulo principal ideals within the Brandt groupoid (again, one can consider a Brandt groupoid for nonmaximal orders with this more general definition of proper product).

On the other hand, if we restrict to two-sided ideal classes of a maximal order $\mathcal{O}$, we do get a group. Namely, suppose $\mathcal{I}$, $\mathcal{J}$ are two-sided $\mathcal{O}$-ideals. Then $\mathcal{I} \sim \mathcal{J}$ means $\mathcal{J} = \mathcal{I}\alpha$ for some $\alpha \in A^\times$. However,

$$\mathcal{O} = \mathcal{O}_r(\mathcal{J}) = \mathcal{O}_r(\mathcal{I}\alpha) = \alpha^{-1}\mathcal{O}_r(\mathcal{I})\alpha = \alpha^{-1}\mathcal{O}\alpha,$$

[7] It is possible to define a weaker notion of equivalence, stable equivalence (or isomorphism), of left $\mathcal{O}$-ideals, which does admit an abelian group structure. See [Rei03, Sec 35].

i.e. $\alpha \in \mathrm{Stab}_{A^\times}(\mathcal{O})$. Consider the **two-sided ideal class** $[\mathcal{I}]_2 = \{\mathcal{I}\alpha : \alpha \in \mathrm{Stab}_{A^\times}(\mathcal{O})\}$, which is the set of all two-sided $\mathcal{O}$-ideals equivalent to $\mathcal{I}$. Then the collection $H_2(\mathcal{O})$ of two-sided ideal classes forms a group, called the **two-sided (ideal) class group**, namely it is the group of two-sided ideals modulo the (necessarily normal because two-sided ideals form an abelian group) subgroup of two-sided ideals of the form $\{\alpha\mathcal{O} = \mathcal{O}\alpha : \alpha \in \mathrm{Stab}_{A^\times}(\mathcal{O})\}$. Denote by $h_2(\mathcal{O})$ the cardinality of $\mathrm{Cl}_2(\mathcal{O})$, which we call the **two-sided class number**. It follows from Exercise 4.4.7 that if $\mathcal{O}$ and $\mathcal{O}'$ are maximal orders, then $\mathrm{Cl}_2(\mathcal{O}) = \mathrm{Cl}_2(\mathcal{O}')$. Thus it makes sense to define the **two-sided class number** $h_{2,A}$ of A as $h_2(\mathcal{O})$ where $\mathcal{O}$ is a maximal order of A.

Since $\mathcal{J} \in [\mathcal{I}]_2$ implies $\mathcal{J} \in [\mathcal{I}]$, we necessarily have $h_2(\mathcal{O}) \leq h(\mathcal{O})$. Under reasonable hypotheses, class numbers are finite.

> **Example 4.4.4.** Let F be a p-adic field and D a division algebra over F. Recall that all one-sided ideals of $\mathcal{O}_D$ are two-sided ideals, and all of the form $\varpi_D^n\mathcal{O}_D$. Hence all are principal, and we have that $h_D = h(\mathcal{O}) = h_{2,D} = h_2(\mathcal{O}) = 1$.

Ideal classes and class numbers for maximal orders in matrix rings are not so exciting.

> **Exercise 4.4.11.** Let $\mathcal{O} = M_n(R)$ in $A = M_n(F)$. Show the two-sided ideals of $\mathcal{O}$ are all of the form $M_n(\mathcal{I})$ where $\mathcal{I}$ is an ideal of R. Conclude $h_{2,A} = h_2(\mathcal{O}) = h(R)$.

> **Exercise 4.4.12.** Let $\mathcal{O} = M_n(R)$ in $A = M_n(F)$.
>
> (a) Show the left ideals of $\mathcal{O}$ are in one-to-one correspondence with the R-submodules of R^n.
>
> (b) Show $h_A = h(\mathcal{O}) = h(R)$.

The example above generalizes to the following.

Proposition 4.4.6. *Let A be a central simple algebra over a p-adic field. Then $h_A = h_{2,A} = 1$.*

Proof (Sketch). We may assume $A = M_n(D)$ for some division algebra D over a p-adic field. Then $\mathcal{O} = M_n(\mathcal{O}_D)$ is a maximal order. By a generalization of Exercise 4.4.12 to the case where R is noncommutative, one deduces $h(\mathcal{O}) = h(\mathcal{O}_D) = 1$. Thus also $h_2(\mathcal{O}) = 1$ as $h_2(\mathcal{O}) \leq h(\mathcal{O})$. □

Thus over p-adic fields, all normal ideals are principal. Over archimedean fields, we don't even talk about class numbers or orders because $\mathbb{R}$ and $\mathbb{C}$ are not Dedekind domains. Over number fields, normal ideals need not be principal, i.e., class numbers can be greater than 1, as you know from the case of number fields. But we do have the following finiteness result.

Theorem 4.4.7 (Jordan–Zassenhaus)**.** *Let F be a number field and A a semisimple F-algebra. Let $\mathcal{O}$ be an $\mathfrak{o}_F$-order in A. Then $h(\mathcal{O}) < \infty$.*

This true more generally for global fields, i.e., also for function fields.

Proof. See [Rei03, Sec 26] or [CR06, Sec 79]. When A is a division algebra, we will also sketch an adelic argument below. □

This finiteness results will be refined for most CSAs over number fields using Eichler's theorem below.

Remark 4.4.8. Suppose $\mathcal{O}$ is a maximal order of A and $h(\mathcal{O}) = 1$. Then one has a factorization theory for elements of $\mathcal{O} \cap A^\times$. Namely, $\alpha \in \mathcal{O} \cap A^\times$ which is a nonunit (in $\mathcal{O}$) can be decomposed into a product of irreducible elements $\alpha = \prod \alpha_i$, where each $\mathcal{O}\alpha_i$ is a maximal left $\mathcal{O}$-ideal. While the α_i's are not uniquely determined up to units (and α_i's cannot be reordered arbitrarily), the associated two-sided prime ideals are uniquely determined. See [Rei03, p. 230] for a brief discussion in this generality, and [CS03] for a more detailed discussion of factorization problems when $A = \mathbb{H}_\mathbb{Q}$. Eventually I may add something along the lines of [CS03] to Chapter 6.

Ideal norms and Eichler's theorem

The above exercises can be generalized to determine class numbers for maximal orders for most CSAs over number fields.

Let F be a number field and A be a CSA over F of degree n. Let S be the set of infinite places v at which $A_v \simeq M_{n/2}(\mathbb{H})$ (so necessarily $F_v \simeq \mathbb{R}$) and put

$$F^{S,+} = \left\{ x \in F^\times : \sigma_v(x) > 0 \text{ for all } v \in S \right\}.$$

Thus S is the set of infinite places at which A ramifies, i.e., is not split.

For $\mathcal{I}$ is an ideal of A, the **(reduced) norm** $N(\mathcal{I})$ of $\mathcal{I}$ is the ideal of $\mathfrak{o}_F$ generated by $\{N(\alpha) : \alpha \in \mathcal{I}\}$. Note that if $\mathcal{I}$ is an integral ideal, so is $N(\mathcal{I})$. For an order $\mathcal{O}$, $1 \in \mathcal{O}$ implies that $N(\mathcal{O}) = \mathfrak{o}_F$.

Exercise 4.4.13. Suppose that $\mathcal{I}$ and $\mathcal{J}$ are normal ideals in A and the product $\mathcal{I}\mathcal{J}$ is proper. Show $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$.

We say a CSA A/F satisfies **Eichler's condition** if it is not a **totally definite** quaternion algebra, i.e., if there is an infinite place v of F such that $A_v = A \otimes_F F_v \not\simeq \mathbb{H}$. Thus A satisfies Eichler's condition if and only if $n \neq 2$ or S does not contain all infinite places.

Theorem 4.4.9 (Eichler)**.** *Suppose A satisfies Eichler's condition. Then a normal ideal $\mathcal{I}$ of A is principal if and only if $N(\mathcal{I}) = \lambda\mathfrak{o}_F$ for some $\lambda \in F^{S,+}$.*

Consequently if $\mathcal{O}$ is a maximal $\mathfrak{o}_F$-order in A, and $\mathcal{I}$, $\mathcal{J}$ are left $\mathcal{O}$-ideals, then $\mathcal{I} \sim \mathcal{J}$ if and only if $N(\mathcal{J}) = \lambda N(\mathcal{I})$ for some $\lambda \in F^{S,+}$.

Eichler also gave an example of a definite quaternion algebra A over a number field F such that a nonprincipal ideal of A has a norm which is a principal ideal.

Proof. See [Rei03, Sec 34]. The proof is fairly involved. □

Let us call a nonzero principal ideal of $\mathfrak{o}_F$ S-positive if it is of the form $\lambda\mathfrak{o}_F$ for some $\lambda \in F^{S,+}$. Let $\mathrm{Cl}^{S,+}(\mathfrak{o}_F)$ denote the nonzero fractional ideals of $\mathfrak{o}_F$ modulo the S-positive principal ideals, and set $h_F^{S,+} = |\mathrm{Cl}^{S,+}(\mathfrak{o}_F)|$. This quotient is a special case of the ray class group discussed towards the end of Section 1.5, and $h_F^{S,+}$ is finite. If S is empty, then we just have $h_F^{S,+} = h_F$, the usual class number. If F is totally real and S contains all infinite places, then $h_F^{S,+} = h_F^+$, the narrow class number. In general, we have $h_F \le h_F^{S,+} \le h_F^+$, and $h_F^{S,+}$ will be a power of 2 times h_F.

The following result says, if $\mathcal{O}$ is a maximal $\mathfrak{o}_F$-order, then the image of principal left $\mathcal{O}$-ideals under the reduced norm is exactly the set of S-positive principal ideals of $\mathfrak{o}_F$.

Theorem 4.4.10 (Hasse–Schilling–Maass). *The reduced norm $N : A^\times \to F$ surjects onto the set $F^{S,+}$.*

This is a global analogue of Corollary 4.3.6.

Proof. See [Rei03, Thm 33.15] or [Wei95, Prop XI.3]. □

Hence, if we know that all fractional ideals of $\mathfrak{o}_F$ arise as reduced norms of left $\mathcal{O}$-ideals, then Eichler's theorem tells us there is a bijection between left $\mathcal{O}$-ideal classes and ideals of $\mathfrak{o}_F$ modulo S-positive principal ideals. This is in fact true.

Corollary 4.4.11. *Suppose A satisfies Eichler's condition. If $\mathcal{O}$ is a maximal $\mathfrak{o}_F$-order, then the reduced norm induces a bijection $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^{S,+}(\mathfrak{o}_F)$. In particular, $h(\mathcal{O}) = h_F^{S,+}$.*

> **Exercise 4.4.14.** Deduce the above corollary. (*Hint:* use Theorem 4.4.5.)

In fact, when A satisfies Eichler's condition, one can more or less directly define an abelian group structure on the left $\mathcal{O}$-ideal classes and prove an isomorphism of groups of ideal classes. See [Rei03, Sec 35].

By the corollary, the only truly interesting case of class numbers of (maximal orders of) central simple algebras over number fields are class numbers (or ray class numbers) of number fields and class numbers of definite quaternion algebras. We will look at class numbers of definite quaternion algebras later.

4.5 Local–global properties and ideles

Now we assume F is a number field, and want to say something about the orders and ideals of an F-algebra A. Here we will take $R = \mathfrak{o}_F$ and assume A is central simple. In particular, A is F-separable, so the results of the previous section apply.

Given any $\mathfrak{o}_F$-lattice Λ in A, we can consider the local completion

$$\Lambda_v = \Lambda \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_v} \subset A_v = A \otimes_F F_v$$

for any nonarchimedean place v of F. This is a finitely-generated $\mathfrak{o}_{F_v}$-module, and thus an $\mathfrak{o}_{F_v}$-lattice in A_v. Moreover, Λ_v is complete if and only if Λ is.

Lemma 4.5.1. *Let Λ be an $\mathfrak{o}_F$-lattice in A and fix a place $v < \infty$. Then Λ is complete if and only if Λ_v is.*

Proof. Note $F\Lambda$ is an F-subspace of A, and similarly for $F_v\Lambda_v \subset A_v$. It suffices to show $\dim_F F\Lambda = \dim_{F_v} F_v\Lambda_v$. This is true by Corollary 1.1.9 as $F_v\Lambda_v \simeq F\Lambda \otimes_F F_v$. □

One deduces that if $\mathcal{O}$ is an $\mathfrak{o}_F$-order in A and $\mathcal{I}$ is a (complete left) $\mathcal{O}$-ideal, then $\mathcal{O}_v$ is an $\mathfrak{o}_{F_v}$-order in A_v and $\mathcal{I}_v$ is a (complete left) $\mathcal{O}_v$-ideal for each $v < \infty$.

There are various local-global properties for orders. Here is a basic one.

Proposition 4.5.2. *An order $\mathcal{O}$ in A is maximal if and only if $\mathcal{O}_v$ is a maximal order in A_v for all $v < \infty$.*

Proof. See [AG60, Sec 1]. □

Let $\mathcal{O}$ be a maximal order in A and $\mathcal{I}$ be an arbitrary (not necessarily complete) left $\mathcal{O}$-ideal. We say $\mathcal{I}$ is **locally principal** (with respect to $\mathcal{O}$) if, for all $v < \infty$, $\mathcal{I}_v = \mathcal{O}_v\alpha_v$ for some $\alpha_v \in A_v^\times$.

Proposition 4.5.3. *An arbitrary (not necessarily complete) left ideal $\mathcal{I}$ of a maximal order $\mathcal{O}$ is complete if and only if it is locally principal.*

Proof. Locally principal ideals of $\mathcal{O}$ are locally complete, and thus complete. Conversely, suppose $\mathcal{I}$ is complete and let $v < \infty$. Then $A_v \simeq M_n(D_v)$ for some p-adic division algebra D_v. By Corollary 4.3.3, $\mathcal{O}_v$ is conjugate to $M_n(\mathcal{O}_{D_v})$. By Proposition 4.4.6, $\mathcal{O}_v$ has class number 1. Thus $\mathcal{I}_v = \mathcal{O}_v\alpha_v$ for some $\alpha_v \in A_v^\times$. □

Remark 4.5.4. This need not be true if $\mathcal{O}$ is not maximal. Remember the ides of Example 1.4.5! Here is another example, coming from Kaplansky [Kap69], where a local complete ideal can be invertible but not principal for a non-maximal order. Consider

$$\mathcal{O} = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p & p\mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p & p\mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}, \quad \mathcal{I} = \begin{pmatrix} p\mathbb{Z}_p & p\mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & p\mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}.$$

Then $\mathcal{O}$ is a non-maximal order in the local algebra $M_3(\mathbb{Q}_p)$, and $\mathcal{I}$ is a complete and invertible $\mathcal{O}$-ideal, but $\mathcal{I}$ is not principal.

Note we have not defined invertibility of ideals, per se, though for ideals of maximal orders, the defining property is in Exercise 4.4.4. In general, we say a lattice $\mathcal{I}$ is **left invertible** if $\mathcal{I}\mathcal{I}^{-1} \subset \mathcal{O}_l(\mathcal{I})$. Right invertibility is defined similarly, and $\mathcal{I}$ is **invertible** if it is both left and right invertible. In general, left invertibility and right invertibility are not equivalent (see [Kap69] for an example). This is another reason it is simpler to work with maximal orders in general, however ideal theory is for non-maximal orders of quaternion algebras is not too much more complicated than the theory for maximal orders.

As in the number field case, we can study ideals and ideal classes adelically.

For simplicity, we will assume $\mathcal{O}$ is a maximal order of our CSA A/F for the rest of this section.

Define the **adelic points** of A (with respect to $\mathcal{O}$) to be

$$A(\mathbb{A}) = A(\mathbb{A})_{\mathcal{O}} = \{(\alpha_v) \in A_v : \alpha_v \in \mathcal{O}_v \text{ a.a. } v\},$$

i.e., $A(\mathbb{A})$ is the restricted direct product of the A_v's with respect to $\mathcal{O}_v$. (Here v in the product ranges over all places of F, though $\mathcal{O}_v$ is only defined for $v < \infty$, but this causes no issue as the condition on $\mathcal{O}_v$ is only at almost all places.)

Exercise 4.5.1. Show the unit group of $A(\mathbb{A})$ is

$$A^\times(\mathbb{A}) = \left\{(\alpha_v) \in A_v^\times : \alpha_v \in \mathcal{O}_v^\times \text{ a.a. } v\right\}.$$

Note if $A = F$, then $A(\mathbb{A}) = \mathbb{A}_F$ and $A^\times(A) = \mathbb{A}_F^\times$.

The next exercise says that the dependence on the choice of maximal order is unimportant. Consequently, we sometimes will talk about the adelic (or idelic) points of algebras without reference to a maximal order.

Exercise 4.5.2. Let $\mathcal{O}'$ be another maximal order of A. Show that there exists $x \in \prod A_v^\times$ such that $A(\mathbb{A})_{\mathcal{O}'} = xA(\mathbb{A})_{\mathcal{O}}x^{-1}$. In particular, $A(A)_{\mathcal{O}} \simeq A(\mathbb{A})_{\mathcal{O}'}$.

As with the case of number fields, we can decompose $A^\times(\mathbb{A})$ into the **finite** and **infinite idelic** parts

$$A^\times(\mathbb{A}) = \hat{A}^\times A_\infty^\times = A^\times(\mathbb{A}_f)A^\times(\mathbb{A}_\infty)$$

where

$$\hat{A}^\times = A^\times(\mathbb{A}_f) = \left\{(\alpha_v)_{v<\infty} \in A_v^\times : \alpha_v \in \mathcal{O}_v^\times \text{ a.a. } v\right\},$$

and

$$A_\infty^\times = A^\times(\mathbb{A}_\infty) = \prod_{v|\infty} A_v.$$

It will also be convenient to denote the **idelic integral units**

$$\hat{\mathcal{O}}^\times = \prod_{v<\infty} \mathcal{O}_v^\times.$$

One can similarly define finite and infinite adelic parts and order $\hat{A} = A(\mathbb{A}_f)$, $A_\infty = A(\mathbb{A}_\infty)$ and $\hat{\mathcal{O}}$, though it is the multiplicative idelic groups that we are more concerned with.[8]

[8] Most people would call the multiplicative groups adelic rather than idelic, e.g., say $A^\times(\mathbb{A})$ is an adelic algebraic group, but etymologically idelic makes more sense to me. (Remember, the 'a' in adele is for additive.) Anyway, when I speak, I'll try to mumble so you can never tell if I'm saying adelic or idelic. And sometimes I'll forget my principles and out of habit write adelic when I mean idelic.

Proposition 4.5.5. *We have a natural bijection*

$$\begin{aligned} \mathrm{Frac}(\mathcal{O}) &\simeq \hat{\mathcal{O}}^\times \backslash \hat{A}^\times \\ \mathcal{I} &\mapsto (\alpha_v), \qquad \mathcal{I}_v = \mathcal{O}_v \alpha_v. \end{aligned}$$

The inverse map is given by $\mathcal{I} = \bigcap \mathcal{O}_v \alpha_v$. *This bijection induces a natural bijection*

$$\mathrm{Cl}(\mathcal{O}) \simeq \hat{\mathcal{O}}^\times \backslash \hat{A}^\times / A^\times$$

Similarly, there are natural bijections $\mathrm{Frac}_r(\mathcal{O}) \simeq \hat{A}^\times / \hat{\mathcal{O}}^\times$ *and* $\mathrm{Cl}_r(\mathcal{O}) \simeq A^\times \backslash \hat{A}^\times / \hat{\mathcal{O}}^\times$.

The proof is similar to the number field case, making use of the previous proposition.

Exercise 4.5.3. Prove the above proposition.

The following result then gives an adelic approach to finiteness of class groups for division algebras. We define an adelic absolute norm on a CSA A/F by $N(\alpha) = \prod |N(\alpha_v)|_v$ for $\alpha = (\alpha_v) \in A(\mathbb{A})$. Let $A(\mathbb{A})^1$ denote the kernel of this map restricted to $\mathbb{A}^\times(\mathbb{A}) \to \mathbb{R}_{>0}$. Then we have the following analogue of Theorem 1.5.7.

Theorem 4.5.6 (Fujisaki)**.** *Let D be a central division algebra over F. Then $D(\mathbb{A})^1/D^\times$ is compact.*

Proof. See [MR03, Sec 7.7] or [Vig80, Thm III.1.4] for the case where D is a quaternion algebra. See [Wei95, Thm IV.4] for the general case. □

Note $\mathbb{A}_F^\times$ is the center of $D^\times(\mathbb{A})$.

Here the topology on $D^\times(\mathbb{A})$ is defined similar to how we defined the topology for $\mathbb{A}_F^\times$. Namely, first define topologies on each D_v (give D_v the natural topology as a finite-dimensional vector space over F_v) and restrict them to $D_v^\times$. Then let a basis of open sets for $D^\times(\mathbb{A})$ be given by sets of the form $\prod U_v$ where U_v is an open set in $D_v^\times$ and $U_v = \mathcal{O}_v^\times$ for almost all v.

We remark $D^\times$ is a discrete subgroup of $D(\mathbb{A})^1$.

Corollary 4.5.7. *Let D be a central division algebra over F. Then $h_D < \infty$.*

Proof. Let $\mathcal{O}$ be a maximal order of D. As in the number field case, we have a bijection of sets $\hat{\mathcal{O}}^\times \backslash \hat{D}^\times / D^\times$ and $\hat{\mathcal{O}}^\times D_\infty^1 \backslash D(\mathbb{A})^1/D^\times$, so $\mathrm{Cl}(\mathcal{O})$ is in bijection with a compact quotient modulo an open subgroup, and thus finite. □

Remark 4.5.8. Roughly the only way for a (reductive) algebraic group to fail to be compact is for it to contain a line (minus a point) $F^\times$. In particular if D_v/F_v is a central division algebra, then $D_v^\times/F_v^\times$ is compact. For a non-division CSA A, one does not get a compactness result as above. However, there is a general theorem of Borel and Harish-Chandra about adelic algebraic groups which implies that $A(\mathbb{A})^1/A^\times$ has "finite volume." This is sufficient to get finiteness of the class number.

One might ask if there are any relations between the class *group* $\mathrm{Cl}(\mathfrak{o}_F)$ and the class (in general just a) set $\mathrm{Cl}(\mathcal{O})$ or the 2-sided class group $\mathrm{Cl}_2(\mathcal{O})$. (Recall that if $A = M_n(F)$ then $h(\mathcal{O}) = h(\mathfrak{o}_F)$ by Exercise 4.4.12.)

Suppose $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{o}_F$. Then we get an $\mathcal{O}$-ideal by taking $\mathcal{I} = \mathcal{O}\mathfrak{a}$. In fact $\mathcal{I} \in \mathrm{Frac}_2(\mathcal{O})$ since $\mathfrak{a} \subset Z(A)$. If $\mathfrak{b} = \mathfrak{a}x$ ($x \in F^\times$) is another $\mathfrak{o}_F$-ideal equivalent to $\mathfrak{a}$, then it gets associated to $\mathcal{J} = \mathcal{O}\mathfrak{b} = \mathcal{O}\mathfrak{a}x$, which is equivalent to the $\mathcal{O}$-ideal $\mathcal{I}$. Hence we get a map

$$\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}_2(\mathcal{O}),$$

and it is easy to see this is a group homomorphism.

Since $\mathrm{Cl}_2(\mathcal{O}) \subset \mathrm{Cl}(\mathcal{O})$ (as sets), we can extend this to a map from $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$. Adelically, this map can be described from by noting the embedding $\hat{F}^\times \to \hat{A}^\times$ induces the map

$$\begin{aligned} &\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O}) \\ &\hat{\mathfrak{o}}_F^\times z F^\times \mapsto \hat{\mathcal{O}}^\times z A^\times, \quad z \in \hat{F}^\times, \end{aligned}$$

which is well defined because $\hat{\mathfrak{o}}_F^\times \subset \hat{\mathcal{O}}^\times$ and $F^\times \subset A^\times$.

We can describe the "kernel" of the map (of sets) $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ adelically as follows (this will be the kernel of the group homomorphism $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}_2(\mathcal{O})$). Suppose $z, z' \in \hat{F}^\times$ map to the same ideal class in $\mathrm{Cl}(\mathcal{O})$. Then $\hat{\mathcal{O}}^\times z A^\times = \hat{\mathcal{O}}^\times z' A^\times$ implies $z(z')^{-1} \in \hat{\mathcal{O}}^\times A^\times$. Let $\mathcal{K} = \hat{\mathcal{O}}^\times A^\times \cap \hat{F}^\times$, which can be viewed as a union of ideal classes in $\mathrm{Cl}(\mathfrak{o}_F)$. Then we get an injective map $\mathrm{Cl}(\mathfrak{o}_F)/\mathcal{K} \to \mathrm{Cl}(\mathcal{O})$.

The point is the map $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ need not be injective, i.e., the homomorphism $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}_2(\mathcal{O})$ need not be injective. If we do not assume A is central, it is easy to find such an example.

> **Example 4.5.1.** Let $F = \mathbb{Q}(\sqrt{-5})$ and consider the quadratic field extension $A = K = F(i)$. Take $\mathcal{O} = \mathfrak{o}_K$. Note F has class number 2 and K has class number 1, so the map $\mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathfrak{o}_K) \simeq \{1\}$ cannot be injective.

In the central case, such examples require more work to find. Fortunately I know people who are skilled in computing with quaternion algebras.

> **Example 4.5.2.** Let $F = \mathbb{Q}(\sqrt{10})$ and $B = \left(\frac{-1,-1}{F}\right)$. Then $h_F = 2$ but any $\mathfrak{o}_F$-ideal extended to an ideal of a maximal order $\mathcal{O}$ of B becomes principal. (Thanks to John Voight for finding this example for me.)

We remark that this can be generalized as follows: if $B \subset A$ is a subalgebra (not necessarily central) and $\mathfrak{o}$ is an order in B such that $\mathfrak{o} \subset \mathcal{O}$, then one similarly gets a map $\mathrm{Cl}(\mathfrak{o}) \to \mathrm{Cl}(\mathcal{O})$ (though one does not get the a map into $\mathrm{Cl}_2(\mathcal{O})$ unless $B \subset Z(A)$). In general, these maps are neither injective nor surjective, but are important because they encode deep arithmetic of A and B. We will discuss this later in the context of imaginary quadratic fields inside definite quaternion algebras.

Returning to the case of $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$, we can use the reduced norm to say it is injective in some situations.

Proposition 4.5.9. *Suppose A satisfies Eichler's condition. The kernel $\mathcal{K}$ of the map $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ is contained in the set of ideal classes of $\mathfrak{o}_F$ of order dividing n. In particular, if n is relatively prime to h_F, the map $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ is injective.*

Proof. Compose the map $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ with the reduced norm map. This sends any nonzero ideal $\mathfrak{a}$ of $\mathfrak{o}_F$ to $\mathfrak{a}^n$. In particular, if $\mathfrak{a} \in \mathcal{K}$, then $\mathfrak{a}^n$ must lie in the trivial class of $\mathrm{Cl}^{S,+}(\mathfrak{o}_F)$ by Eichler's theorem (with S as in the previous section). In particular $\mathfrak{a}^n = [\mathfrak{o}_F] \in \mathrm{Cl}(\mathfrak{o}_F)$. □

By Corollary 4.4.11, when A satisfies Eichler's condition $h(\mathcal{O})$ is a multiple of (in fact, a power of 2 times) h_F. Alternatively, if $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ is injective (whether or not A satisfies Eichler's condition), we can deduce that $h(\mathcal{O}_F)$ is a multiple of h_F.

Exercise 4.5.4. Suppose the map $\mathrm{Cl}(\mathfrak{o}_F) \to \mathrm{Cl}(\mathcal{O})$ is injective. Then show $\mathrm{Cl}(\mathfrak{o}_F)$ acts freely on $\mathrm{Cl}(\mathcal{O})$ by

$$\begin{aligned} \mathrm{Cl}(\mathfrak{o}_F) \times \mathrm{Cl}(\mathcal{O}) &\to \mathrm{Cl}(\mathcal{O}) \\ (z, \hat{\mathcal{O}}^\times x A^\times) &\mapsto \hat{\mathcal{O}}^\times z x A^\times. \end{aligned}$$

In particular, the class number $h(\mathcal{O})$ is a multiple of h_F.

Remark 4.5.10. One can also use the idelic approach to study ideals of non-maximal orders. In this case Proposition 4.5.3 does not hold, but one can still get a correspondence of idele classes $\hat{\mathcal{O}}^\times \backslash \hat{A}^\times$ with locally principal ideal classes. Note the idelic group $\hat{A}^\times$ (a priori, mildly dependent on $\mathcal{O}$) will be the same as in the case of maximal orders: if $\mathcal{O}$ is a non-maximal order contained in a maximal order $\mathcal{O}'$, then one still has that $\mathcal{O}_v = \mathcal{O}'_v$ for almost all v, so $A^\times(\mathbb{A})_{\mathcal{O}} = A^\times(\mathbb{A})_{\mathcal{O}'}$.