Chapter 8

Orders

8.1 Integral structures

Inside the rational numbers $\mathbb{Q}$ are the integers $\mathbb{Z}$; inside a number field is its ring of integers. What happens if we concern ourselves with a notion of integrality for possibly noncommutative algebras? In this chapter, we consider some basic questions of this nature that work without hypothesis on the field.

First we have to understand the linear algebra aspects: these are modules inside a vector space. Then the algebra structure is a multiplication law on this lattice, and is called an *order* because something.

Some properties of orders can be deduced from the commutative case: orders still consist of *integral* elements, satisfying a monic polynomial with coefficients in $\mathbb{Z}$.

The matrix ring over a field are endomorphisms of a vector space; the orders in a matrix ring should look like endomorphisms of a lattice (perhaps with extra structure).

Do some examples over $\mathbb{Z}$.

8.2 Lattices

Throughout this chapter, let R be a noetherian domain with field of fractions F. To avoid trivialities, we assume $R \neq F$.

Definition 8.2.1. Let V be a finite-dimensional F-vector space. An R-*lattice* of V is a finitely generated R-submodule $M \subseteq V$ with $MF = V$.

Remark 8.2.2. Other authors omit the second condition in the definition of an R-lattice and say that I is *full* if $MF = V$. We will not encounter R-lattices that are not full (and when we do, we call them finitely generated R-submodules), so we avoid this added nomenclature.

By definition, an R-lattice contains a basis of V, and it can be thought of an R-submodule that "allows bounded denominators", as follows.

Lemma 8.2.3. *Let M be an R-lattice. Then for any $y \in V$, there exists $0 \neq r \in R$ such that $ry \in M$. Moreover, if J is a finitely generated R-submodule of V, then*

there exists $0 \neq r \in R$ *such that* $rJ \subseteq M$*, and* J *is an* R*-lattice if and only if there exists* $0 \neq r \in R$ *such that* $rM \subseteq J \subseteq r^{-1}M$.

Proof. Since $FM = V$, the R-lattice M contains an F-basis $x_1, \ldots, x_n$ for V, so in particular $M \supset Rx_1 \oplus \cdots \oplus Rx_n$. Writing $y \in V$ in the basis $x_1, \ldots, x_n$, clearing denominators we see that there exists $0 \neq r \in R$ such that $rx \in M$.

For the second statement, let y_i be a set of R-module generators for J; then there exist $r_i \in R$ such that $r_i y_i \in M$ hence $0 \neq r = \prod_i r_i$ satisfies $rJ \subseteq M$, so $J \subseteq r^{-1}M$. Repeating this argument with M interchanged with J and taking the product of the two, we have the result. □

8.3 Orders

Let B be an F-algebra.

Definition 8.3.1. An R-*order* $\mathcal{O} \subseteq B$ is an R-lattice that is also a subring of B.

In particular, if $\mathcal{O}$ is an R-order then we insist that $1 \in \mathcal{O}$.

8.3.2. An R-*algebra* is a ring $\mathcal{O}$ equipped with an embedding $R \hookrightarrow \mathcal{O}$ whose image lies in the center of $\mathcal{O}$. An R-order $\mathcal{O}$ is an R-algebra, and if $\mathcal{O}$ is an R-algebra that is finitely generated as an R-module, then $\mathcal{O}$ is an R-order of $B = \mathcal{O} \otimes_R F$.

Example 8.3.3. The matrix algebra $\mathrm{M}_n(F)$ has the R-order $\mathrm{M}_n(R)$. The subring $R[G] = \bigoplus_g Rg$ is an R-order in the group ring $F[G]$.

Example 8.3.4. Let $a, b \in R \setminus \{0\}$ and consider the quaternion algebra $B = \left(\frac{a,b}{F}\right)$. Then $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rij$ is an R-order.

Let $I \subseteq B$ be an R-lattice in the F-algebra B.

8.3.5. An important construction of orders comes as follows. Define the set

$$\mathcal{O}_{\mathrm{L}}(I) = \{\alpha \in B : \alpha I \subseteq I\}.$$

Then $\mathcal{O}_{\mathrm{L}}(I)$ is an R-submodule of B which is a ring. We show it is also an R-lattice. For any $\alpha \in B$, by Lemma 8.2.3 there exists $0 \neq r \in R$ such that $r(\alpha I) \subseteq I$, hence $\mathcal{O}_{\mathrm{L}}(I)F = B$. Also by this lemma, there exists $0 \neq s \in R$ such that $s = s \cdot 1 \in I$; thus $\mathcal{O}_{\mathrm{L}}(I)s \subseteq I$ so $\mathcal{O}_{\mathrm{L}}(I) \subseteq s^{-1}I$. Since R is noetherian and $s^{-1}I$ is an R-lattice so finitely generated, we conclude that $\mathcal{O}_{\mathrm{L}}(I)$ is finitely generated and is thus an R-lattice.

It follows that every F-algebra B has an R-order, since if $B = \bigoplus_i F\alpha_i$ then $I = \bigoplus_i R\alpha_i$ is an R-lattice.

Definition 8.3.6. The order

$$\mathcal{O}_{\mathrm{L}}(I) = \{\alpha \in B : \alpha I \subseteq I\}$$

is called the *left order* of I. We similarly define the *right order* of I by

$$\mathcal{O}_{\mathrm{R}}(I) = \{\alpha \in B : I\alpha \subseteq I\}.$$

Orders are composed of integral elements, defined as follows. If $\alpha \in B$, we denote by $R[\alpha] = \sum_d R\alpha^d$ the (commutative) R-subalgebra of B generated by α.

Definition 8.3.7. An element $\alpha \in B$ is *integral* over R if α satisfies a monic polynomial with coefficients in R.

Lemma 8.3.8. *For $\alpha \in B$, the following are equivalent:*

(i) *α is integral over R;*

(ii) *$R[\alpha]$ is a finitely generated R-module;*

(iii) *α is contained in a subring A which is a finitely generated R-module.*

Proof. If $\alpha \in B$ is integral and is a root of $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$, then obviously $R[\alpha] = R + R\alpha + \cdots + R\alpha^{n-1}$. Conversely, if $R[\alpha]$ is finitely generated, then α satisfies the characteristic polynomial of left multiplication by α on a basis for B consisting of elements of $\mathcal{O}$. This proves (i) $\Leftrightarrow$ (ii).

For the final equivalence, we see that (ii) $\Rightarrow$ (iii) is immediate, and for the converse, if $\mathcal{O} \subseteq B$ is an R-order, then every $\alpha \in \mathcal{O}$ is integral over R, since $R[\alpha]$ is a submodule of $\mathcal{O}$ so (since R is noetherian) $R[\alpha]$ is finitely generated. □

Corollary 8.3.9. *If $\mathcal{O}$ is an R-order, then every $\alpha \in \mathcal{O}$ is integral over R.*

We say R is *integrally closed* (in F) if any $\alpha \in F$ integral over R has $\alpha \in R$.

Inside the field F, the set of elements integral over R (the *integral closure* of R in F) forms a ring: if α, β are integral over R then $\alpha + \beta$ and $\alpha\beta$ are integral since they lie in $R[\alpha, \beta]$ which is a finitely generated submodule of F. This ring is itself integrally closed.

Lemma 8.3.10. *Suppose that R is integrally closed. Then $\alpha \in B$ is integral over R if and only if the minimal polynomial of α over F has coefficients in R.*

Proof. Let $f(x) \in R[x]$ be a monic polynomial that α satisfies, and let $g(x) \in F[x]$ be the minimal polynomial of α. Let K be a splitting field for $g(x)$, and let $\alpha_1, \ldots, \alpha_n$ be the roots of $g(x)$ in K. Since $g(x) \mid f(x)$, each such α_i is integral over R, and the set of elements in K integral over R forms a ring, so each coefficient of g is integral over R and belongs to F; but since R is integrally closed, these coefficients must belong to R, so $g(x) \in R[x]$. □

Corollary 8.3.11. *If B is an F-algebra with a standard involution, and R is integrally closed, then $\alpha \in B$ is integral over R if and only if $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in R$.*

The integral closure of R in F is the largest ring containing integral elements. Accordingly, we make the following more general definition.

Definition 8.3.12. An R-order is *maximal* if it is not properly contained in another R-order.

If B is a commutative F-algebra and R is integrally closed in F, then the integral closure S of R in K is integrally closed and therefore S is a maximal R-order in K. However, if B is noncommutative, then the set of elements in B integral over R is no longer necessarily itself a ring, and so the theory of maximal orders is more complicated. (This may seem counterintuitive at first, but certain aspects of the noncommutative situation are indeed quite different!)

Example 8.3.13. Let $B = \mathrm{M}_2(\mathbb{Q})$ and let $\alpha = \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix}$ and $\beta = \begin{pmatrix} 0 & 0 \\ 1/2 & 0 \end{pmatrix}$. Then $\alpha^2 = \beta^2 = 0$, so α, β are integral over $R = \mathbb{Z}$, but $\alpha + \beta$ is not integral since $\mathrm{nrd}(\alpha + \beta) = -1/4$ (Corollary 8.3.11). Such a counterexample does not require the existence of zerodivisors: see Exercise 8.9.

The problem in the noncommutative setting is that although $R[\alpha]$ and $R[\beta]$ may be finitely generated as R-modules, this need not be the case for the R-algebra generated by α and β: indeed, in the example above, it is not!

The structure of (maximal) orders in a quaternion algebra over the domains of arithmetic interest is the subject of the second Part of this text. To conclude this chapter, we discuss some special cases over the next few sections.

8.4 Orders in separable algebras

We have also the following characterization of orders in separable algebras.

Lemma 8.4.1. *Let $\mathcal{O} \subseteq B$ be a subring of a separable F-algebra B such that $\mathcal{O}F = B$. Then $\mathcal{O}$ is an R-order if and only if every $\alpha \in \mathcal{O}$ is integral.*

Proof. Let $\mathcal{O} \subseteq B$ be a subring of an F-algebra B such that $\mathcal{O}F = B$. Recall that a separable F-algebra is a semisimple F-algebra such that the symmetric bilinear pairing $(\alpha, \beta) \mapsto \mathrm{trd}(\alpha\beta)$ is nondegenerate.

We need to show that $\mathcal{O}$ is finitely generated. Let $\alpha_1, \ldots, \alpha_n$ be an F-basis for B contained in $\mathcal{O}$. If $\beta \in \mathcal{O}$ then $\beta = \sum_i a_i\alpha_i$ with $a_i \in F$. We have $\beta\alpha_i \in \mathcal{O}$ since $\mathcal{O}$ is a ring, so $\mathrm{trd}(\beta\alpha_i) = \sum_j a_j \mathrm{trd}(\alpha_j\alpha_i)$ with $\mathrm{trd}(\alpha_j\alpha_i) \in R$. Now since B is separable, the matrix $(\mathrm{trd}(\alpha_i\alpha_j))_{i,j=1,\ldots,n}$ is invertible, say $r = \det(\mathrm{trd}(\alpha_i\alpha_j))$, so we can solve these equations for a_j using Cramer's rule and we find that $a_j \in r^{-1}R$. Consequently $\mathcal{O} \subseteq r^{-1}(R\alpha_1 \oplus \cdots \oplus R\alpha_n)$ is a submodule of a finitely generated module so (since R is noetherian) we have that $\mathcal{O}$ is finitely generated. □

Remark 8.4.2. It follows from Lemma 8.4.1 that a separable F-algebra B has a maximal order. By Paragraph 8.3.5, B has an R-order $\mathcal{O}$ (since it has a lattice, taking the R-span of any F-basis), so the collection of R-orders containing $\mathcal{O}$ is nonempty. Given any chain of R-orders containing $\mathcal{O}$, by Lemma 8.4.1 the union of these orders is again an R-order. Since R is noetherian, there exists a maximal element in any chain. [[Ref in comment]] (More generally, the conclusion follows by applying Zorn's lemma.) See also Proposition 14.2.17.

8.5 Orders in a matrix ring

Next, we study orders in a matrix ring. The matrix ring over F is just the endomorphism ring of a finite-dimension vector space over F, and we seek a similar description for orders as endomorphism rings of lattices, following Paragraph 8.3.5.

Let V be an F-vector space with $\dim_F V = n$ and let $B = \mathrm{End}_F(V)$. Choosing a basis of V gives an identification $B = \mathrm{End}_F(V) \simeq \mathrm{M}_n(F)$. Given an R-lattice $I \subseteq V$, we define

$$\mathrm{End}_R(I) = \{f \in \mathrm{End}_F(V) : f(I) \subseteq I\} \subset B.$$

Note that the definition of $\mathrm{End}(I)$ differs from that of the left order (8.3.5): we do not take $B = V$, but rather, consider endomorphisms of lattices of smaller rank.

Example 8.5.1. If $V = Fx_1 \oplus \cdots \oplus Fx_n$ and $I = Rx_1 \oplus \cdots \oplus Rx_n$, then we have $\mathrm{End}_R(I) \simeq \mathrm{M}_n(R)$.

More generally, if I is *completely decomposable*, i.e. $I = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n$ with $\mathfrak{a}_i$ projective R-submodules of F, then $\mathrm{End}_R(J) \subseteq \mathrm{M}_n(F)$ consists of those matrices whose ijth entry lies in $\mathrm{Hom}_R(\mathfrak{a}_i, \mathfrak{a}_j) \subseteq \mathrm{Hom}_F(F, F) = F$. For example, if $n = 2$ then

$$\mathrm{End}_R(I) \simeq \begin{pmatrix} R & \mathrm{Hom}_R(\mathfrak{a}_2, \mathfrak{a}_1) \\ \mathrm{Hom}_R(\mathfrak{a}_1, \mathfrak{a}_2) & R \end{pmatrix} \subset \mathrm{M}_2(F).$$

Lemma 8.5.2. *Let I be an R-lattice of V. Then $\mathrm{End}_R(I)$ is an R-order in $B = \mathrm{End}_F(V)$.*

Proof. As in Paragraph 8.3.5, we have $\mathrm{End}_R(I)F = B$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an F-basis for V and let $J = R\alpha_1 \oplus \cdots \oplus R\alpha_n$. Then by Lemma 8.2.3 there exists $0 \neq r \in R$ such that $rJ \subseteq I \subseteq r^{-1}J$. Therefore $\mathrm{End}_R(rJ) = r^n \mathrm{End}_R(J) \subseteq \mathrm{End}_R(I) \subseteq r^{-n} \mathrm{End}_R(J)$, and so $\mathrm{End}_R(I)$ is an R-order in B. □

Lemma 8.5.3. *Let $\mathcal{O} \subseteq B = \mathrm{End}_F(V)$ be an R-order. Then $\mathcal{O} \subseteq \mathrm{End}_R(I)$ for some R-lattice $I \subseteq V$.*

Proof. Let J be any R-lattice in V, and let $I = \{\alpha \in J : \mathcal{O}\alpha \subseteq J\}$. Then I is an R-submodule of J with $FI = V$ (as in Paragraph 8.3.5), so I is an R-lattice in V and $\mathcal{O} \subseteq \mathrm{End}_R(I)$. □

Corollary 8.5.4. *If R is a PID, then every maximal R-order $\mathcal{O} \subseteq B \simeq \mathrm{M}_n(F)$ is conjugate in B to $\mathrm{M}_n(R)$.*

Proof. The isomorphism $B \simeq \mathrm{M}_n(F)$ arises from a basis $x_1, \ldots, x_n$; letting $J = \bigoplus_i Rx_i$ we have $\mathrm{End}_R(J) \simeq \mathrm{M}_n(R)$. Now the R-order $\mathrm{M}_n(R)$ is maximal by Exercise 8.6, since a PID is integrally closed. By the lemma, we have $\mathcal{O} \subseteq \mathrm{End}_R(I)$ for some R-lattice $I \subseteq V$, so if $\mathcal{O}$ is maximal then $\mathcal{O} = \mathrm{End}_R(I)$. If R is a PID then $I = Ry_1 \oplus \cdots \oplus Ry_n$, and the change of basis matrix from x_i to y_i realizes $\mathrm{End}_R(I)$ as a conjugate of $\mathrm{End}_R(J) \simeq \mathrm{M}_n(R)$. □

An order $\mathcal{O} \subseteq \mathrm{End}_R(I)$ can be thought of as a subring of endomorphisms of a lattice preserving some extra structure. We consider this matter in detail in the quaternionic context of 2×2-matrices in Chapter 18.

8.6 Quadratic forms

In setting up an integral theory, we will also have need of an extension of the theory of quadratic forms over a PID; these notions generalize those over fields (Section 4.2) in a straightforward way.

Let R be a PID.

Definition 8.6.1. A *quadratic form* over R is a map $Q : M \to R$ where M is a (free) R-module satisfying:

(i) $Q(rx) = r^2 Q(x)$ for all $r \in R$ and $x \in R^n$; and

(ii) The map $T : R^n \times R^n \to R$ defined by

$$T(x, y) = Q(x + y) - Q(x) - Q(y)$$

is R-bilinear.

T is called the *associated bilinear map* .

8.6.2. Let $Q : V \to F$ be a quadratic form with F the field of fractions of R. Let $M \subseteq V$ be a finitely generated R-lattice such that $Q(M) \subseteq R$. Then the restriction $Q|_M : M \to R$ is a quadratic form. Conversely, if $Q : M \to R$ is a quadratic form over R, then the extension $Q : M \otimes_R F \to F$ is a quadratic form over F.

Definition 8.6.3. A *similarity* between quadratic forms $Q : M \to R$ and $Q' : M' \to R$ is an isomorphism $f : M \xrightarrow{\sim} M'$ and $u \in R^\times$ such that $Q(f(x)) = uQ'(x)$ for all $x \in M$. An *isometry* between quadratic forms is a similarity with $u = 1$.

Let $Q : M \to R$ be a quadratic form over R. Then Q is *nondegenerate* if the extension $Q : M \otimes_R F \to F$ is nondegenerate. [[Nonsingular?]] From now on, suppose that $M \simeq R^n$ is free of finite rank n in the basis $e_1, \ldots, e_n$. We then define the *discriminant* $\mathrm{disc}(Q)$ as the (half-)determinant of the *Gram matrix* $(T(e_i, e_j))_{i,j}$, as in Definition 4.2.9. [[Nonsingular? and differences between them?]]

8.7 Extensions and further reading

8.7.1. The hypothesis that R is noetherian is used in Paragraph 8.3.5; it seems possible that the left order may not be finitely generated. Perhaps noetherian induction will work? [[Used in other places?]].

Exercises

Let R be a noetherian domain with field of fractions F.

8.1. Let L, M be R-lattices in a vector space V with $\dim_F V < \infty$. Show that $L + M$ and $L \cap M$ are R-lattices.

8.2. Let B be an F-algebra and let $I \subset B$ be an R-lattice. Show that there exists a nonzero $r \in R \cap I$.

8.3. Let $\mathfrak{c} \subseteq R$ be a nonzero ideal. Show that

$$\begin{pmatrix} R & R \\ \mathfrak{c} & R \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(R) : c \in \mathfrak{c} \right\} \subseteq \mathrm{M}_2(R)$$

is an R-order in $\mathrm{M}_2(F)$.

8.4. Let $\mathcal{O}, \mathcal{O}' \subseteq B$ be R-orders. Show that $\mathcal{O} \cap \mathcal{O}'$ is an R-order.

8.5. Let $A_1, \dots, A_r$ be F-algebras and let $B = A_1 \times \cdots \times A_r$. Show that $\mathcal{O} \subseteq B$ is an R-order if and only if $\mathcal{O} \cap A_i$ is an R-order for each i.

8.6. Let R be integrally closed. Show that $\mathrm{M}_n(R)$ is a maximal R-order in $\mathrm{M}_n(F)$.

8.7. Let $B = \left(\frac{K, b}{F}\right)$ with $b \in R$ and let S be an R-order in K. Let $\mathcal{O} = S + Sj$. Show that $\mathcal{O}$ is an R-order in B.

8.8. Let B be an F-algebra with a standard involution and let $\alpha \in B$. Show that if α is integral over R then $\mathrm{trd}(\alpha^n) \in R$ for all $n \in \mathbb{Z}_{\geq 0}$. Is the converse true?

8.9. Generalize Example 8.3.13 as follows.

a) Find an algebra B over a field F and elements $\alpha, \beta \in B$ such that α, β are integral over $R \subseteq F$ but $\alpha\beta$ is not.

b) Find a division ring D over a field F and elements $\alpha, \beta \in D$ such that α, β are integral over $R \subseteq F$ but $\alpha + \beta$ is not.

8.10. Give an example of a non-noetherian ring R and modules $J \subset I$ such that I is finitely generated but J is not finitely generated. Does this yield an example where $\mathcal{O}_{\mathrm{L}}(I)$ is not an R-lattice (cf. Paragraph 8.3.5)?

8.11. Let $\alpha \in \mathrm{M}_n(F)$ have characteristic polynomial with coefficients in R. Show that α is conjugate by an element $\beta \in \mathrm{GL}_n(F)$ to an element of $\mathrm{M}_n(R)$. Explicitly, how do you find such a matrix β?

8.12. Let B be an F-algebra and let $I \subseteq B$ be an R-lattice. Show that $\mathcal{O}_{\mathrm{L}}(I)$ is a maximal R-order if and only if $\mathcal{O}_{\mathrm{R}}(I)$ is a maximal R-order. [[Not sure it is true in this generality. Exercise I.4.1 in Vigneras.]]

8.13. Let $\mathcal{O} \subseteq B$ be an R-order.