Chapter 6

Arithmetic of quaternion algebras

Here we'll investigate some arithmetic properties and consequences of quaternion algebras. Namely, we'll try to get a more concrete understanding of orders and ideals in quaternion algebras, including a class number formula and questions of factorization. We'll also give some applications to ternary and quaternary quadratic forms, with more impressive applications to follow in Chapter 7.

The primary references are Vigneras [Vig80] and some papers of Pizer [Piz76], [Piz77], [Piz80]. Note that some of what we do will be in greater generality than these references (e.g., Pizer's paper are just over $\mathbb{Q}$ and Vigneras restricts to Eichler orders for some things), and some things we cover are not treated by Vigneras or Pizer.

Our focus is on explaining (some of) what is known and how to do concrete computations rather than giving complete proofs. (In other words, I don't have time to prove everything. Proofs of some results, e.g. mass and class number formulas, involve a fair amount of auxiliary material.)

Throughout this chapter, F is a local or global field of characteristic 0 unless stated otherwise. The letter B will denote a quaternion algebra over F. If F is a p-adic or number field, $\mathfrak{o}_F$ denotes the ring of integers of F, and $\mathcal{O}$ will be an order in B. (Unless stated otherwise all orders are $\mathfrak{o}_F$-orders, including the discussion of orders in other fields K which contain F.) If F is a p-adic field, $\varpi = \varpi_F$ is a uniformizer for F and $\mathfrak{p} = \varpi \mathfrak{o}_F$ is the unique maximal ideal in $\mathfrak{o}_F$. If B is a p-adic division algebra, then ϖ_B, then $\mathcal{O}_B$ denotes the unique maximal order and $\mathfrak{P} = \varpi_B \mathcal{O}_B$ denotes the unique maximal 2-sided ideal in $\mathcal{O}_B$.

6.1 Quaternionic orders

We have defined orders, ideals and (reduced) norms of ideals, ideal classes and class numbers for central simple algebras. For the arithmetic of quaternion algebras, we will want a couple more notions: discriminants and levels. We will define level below, first locally, then globally. Now we give a uniform definition of discriminant.

Let F be a number or p-adic field, B/F be a quaternion algebra, and $\mathcal{O}$ an order of B. The **dual lattice** to $\mathcal{O}$ is

$$\mathcal{O}^{\perp} = \{\alpha \in B : \mathrm{tr}(\alpha \mathcal{O}) \subset \mathfrak{o}_F\}.$$

This is the algebraic notion of a dual space with respect to a bilinear form where the bilinear form is the trace form defined in Exercise 3.2.3.

Lemma 6.1.1. *The dual $\mathcal{O}^\perp$ is a 2-sided $\mathcal{O}$-ideal and its inverse $(\mathcal{O}^\perp)^{-1}$ is a 2-sided integral ideal, called the* **different** *of $\mathcal{O}$.*

> **Exercise 6.1.1.** Prove this lemma.

The **discriminant** $\operatorname{disc}\mathcal{O}$ of $\mathcal{O}$ is the (reduced) norm $N((\mathcal{O}^\perp)^{-1})$ of the different of $\mathcal{O}$, i.e., the (integral) ideal of $\mathfrak{o}_F$ generated by $N(x)$ for $x \in (\mathcal{O}^\perp)^{-1}$. In the cases $F = \mathbb{Q}$ or $F = \mathbb{Q}_p$, $n \in \mathbb{N}$ and $\operatorname{disc}\mathcal{O} = n\mathbb{Z}$ or $\operatorname{disc}\mathcal{O} = n\mathbb{Z}_p$, we sometimes simply say the discriminant is n.

These definitions of different and discriminant are analogous to the case of number and p-adic field extensions K/F: the dual lattice (ideal) $\mathfrak{a}^\perp$ of an ideal $\mathfrak{a} \subset \mathfrak{o}_K$ with respect to the trace form is the inverse different and the norm of the different from K/F is shown to to be the discriminant of $\mathfrak{a}$.

Recall that an order $\mathcal{O}$ is not necessarily a free $\mathfrak{o}_F$-module. In general, it may not be if F is a number field with class number > 1. However, $\mathcal{O}$ is free if $\mathfrak{o}_F$ is a PID, i.e., if F is p-adic or $h_F = 1$. In these cases, it is easier to compute discriminants:

Proposition 6.1.2. *Suppose $\mathfrak{o}_F$ is a PID and $\mathcal{O}$ an order in B with $\mathfrak{o}_F$-basis $\alpha_1, \dots, \alpha_4$ as a free module. Then* $\operatorname{disc}\mathcal{O} = (\det(\alpha_i\alpha_j)_{i,j})^2$.

Proof. See [Vig80, Lem I.4.7]. □

Proposition 6.1.3. *Suppose $\mathcal{O}$ and $\mathcal{O}'$ are orders of B. Then $\mathcal{O} \subset \mathcal{O}'$ implies* $\operatorname{disc}\mathcal{O} \subset \operatorname{disc}\mathcal{O}'$*, i.e.,* $\operatorname{disc}\mathcal{O}' | \operatorname{disc}\mathcal{O}$*, with* $\operatorname{disc}\mathcal{O} = \operatorname{disc}\mathcal{O}'$ *if and only if $\mathcal{O} = \mathcal{O}'$.*

Proof. See [Vig80, Cor I.4.8]. □

This proposition is useful in determining if an order is a maximal order, just like the discriminant is a useful tool to determine if an order is the full ring of integers in a number field. E.g., we will use this in Theorem 6.1.15 below.

Of course it may be that $\mathcal{O}$ and $\mathcal{O}'$ have the same discriminant if one is not contained in the other—this happens for instance when $\mathcal{O}$ and $\mathcal{O}'$ conjugate orders. We'll compute discriminants for orders "with level" below, and see that the discriminant is the level. This includes the case of maximal orders, and the discriminant will be independent of the choice of a maximal order, and we will define the discriminant of these quaternion algebras to be the discriminant of a maximal order.

> **Exercise 6.1.2.** Let $F = \mathbb{Q}$ and $B = \mathbb{H}_\mathbb{Q} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, and consider the orders $\mathcal{O} = \mathbb{Z}[i,j,k]$ (the Lipschitz integers) and $\mathcal{O}' = \mathbb{Z}[i,j,\frac{1+i+j+k}{2}]$ (the Hurwitz integers). Using Proposition 6.1.2, show $\operatorname{disc}\mathcal{O} = 4$ and $\operatorname{disc}\mathcal{O}' = 2$.

Note this is compatible with Proposition 6.1.3. We will use this discriminant calculation in Example 6.1.5 below to conclude the Hurwitz integers are a maximal order in $\mathbb{H}_\mathbb{Q}$.

6.1.1 Local orders

In this section, let F be a p-adic field and B be a quaternion algebra over F. Then, up to isomorphism, either $B = D$ (nonsplit) or $B = M_2(F)$ (split), where D denotes the unique quaternion division algebra over F. Here we summarize the theory of (a large class of) $\mathfrak{o}_F$-orders in B.

First we will describe the maximal orders.

Recall from Lemma 5.1.2, the unique quaternion division algebra D/F contains the unique quadratic unramified field extension $K = F(\sqrt{u})$. Since ϖ is not a norm from K, by Proposition 3.3.7, we can express

$$D = \left(\frac{u, \varpi}{F}\right) = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\} \subset M_2(K), \tag{6.1.1}$$

where $\alpha \mapsto \overline{\alpha}$ denotes Galois conjugation in K/F.

Lemma 6.1.4. *With D as in (6.1.1), the order in D given by*

$$\mathcal{O}_D = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathfrak{o}_K \right\},$$

consists of all $\mathfrak{o}_F$-integral elements of D.

Proof. It is easy to see that $\mathcal{O}_D$ is an order, so we will just check the integrality assertion.

Write $\alpha = x + y\sqrt{u}$ and $\beta = z + w\sqrt{u}$, where $u \in \mathfrak{o}_F^\times$ is a nonsquare. Note the element $\gamma = \begin{pmatrix} \alpha & \varpi\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} \in D$ is integral if and only if $\operatorname{tr}\gamma = \operatorname{tr}\alpha = 2x \in \mathfrak{o}_F$ and $\det\gamma = N\alpha - \varpi N\beta \in \mathfrak{o}_F$. Since K/F is unramified, the image of the norm map is precisely the set of elements of even valuation, so $\det\gamma \in \mathfrak{o}_F$ if and only if the "parts of even and odd valuation" $N\alpha$ and $\varpi N\beta$ lie in $\mathfrak{o}_F$, i.e., if and only if $N\alpha, N\beta \in \mathfrak{o}_F$, i.e., if and only if $v(N\alpha) = 2v_K(\alpha) \geq 0$ and $v(N\beta) = 2v_K(\beta) \geq 0$, i.e., if and only if $\alpha, \beta \in \mathfrak{o}_K$. □

For global applications, it will also useful to describe maximal orders in terms of realizations of D in $M_2(K)$ where K/F is a ramified quadratic extension.

> **Exercise 6.1.3.** Let p be an odd rational prime, and u a nonsquare in $\mathbb{Z}_p^\times$. Let $\varpi \in \{p, up\}$ and $K = \mathbb{Q}_p(\sqrt{\varpi})$ the associated ramified quadratic extension. First check that the quaternion division algebra $D/\mathbb{Q}_p$ can be realized as the set of matrices $\begin{pmatrix} \alpha & u\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}$, where $\alpha, \beta \in K$ and bar denotes Galois conjugation in K. Then show the maximal order $\mathcal{O}_D$ of D is given by the set of such matrices with $\alpha, \beta \in \mathfrak{o}_K$. (Recall Exercise 1.2.11.)

Theorem 6.1.5. *When $B = D$, there is a unique maximal order $\mathcal{O}_D$, consisting of all $\mathcal{O}_F$-integral elements. When $B = M_2(F)$, any maximal order $\mathcal{O}_B$ is $\mathrm{GL}_2(F)$-conjugate to $M_2(\mathcal{O}_F)$.*

Proof. The case of $B = D$ follows from the above lemma together with Proposition 4.2.2. It is also a special case of Theorem 4.3.2. When $B = M_2(F)$, this is a special case of Theorem 4.2.7. See also [Vig80, Sec 2.1, 2.2] or [MR03, Sec 6.4, 6.5] for complete proofs in just the quaternionic setting. □

Example 6.1.1. Let $g_n = \begin{pmatrix} \varpi^n & \\ & 1 \end{pmatrix}$ for some $n \in \mathbb{Z}$. Then $\mathcal{O}_n = g_n M_2(\mathcal{O}_F) g_n^{-1} = \begin{pmatrix} \mathcal{O}_F & \mathfrak{p}^n \\ \mathfrak{p}^{-n} & \mathcal{O}_F \end{pmatrix}$ is a maximal order in $M_2(F)$. (We essentially saw this in Example 4.2.5.)

Thus the maximal orders of B are easy to describe. What about non-maximal orders? In the split case, we can construct other orders by intersecting two or more maximal orders. Orders in B which are the intersection of two maximal orders play a special role in number theory, and are called **Eichler orders** (cf. Section 4.2). The two maximal orders need not be distinct, so Eichler orders include maximal orders.

Example 6.1.2. Let $B = M_2(F)$ and recall $\mathcal{O}_n$ from Example 6.1.1. Then $\mathcal{O}_B(n) = \mathcal{O}_0 \cap \mathcal{O}_{-n} = \begin{pmatrix} \mathcal{O}_F & \mathcal{O}_F \\ \mathfrak{p}^n & \mathcal{O}_F \end{pmatrix}$ is an Eichler order for $n \geq 0$. We say this order is of **level** $\mathfrak{p}^n$. It arises often in the theory of modular forms.

Of course this idea of intersecting orders won't give us anything so far in the nonsplit case as there is only one maximal order. Still, one can construct something analogous in terms of matrices to the order $\mathcal{O}_B(n)$ in the split case.

Example 6.1.3. Let E/F be the unramified quadratic extension, so ϖ is still a uniformizer for E. Then, as a vector space, we can write $D = E \oplus Ej$ for some j in D. In fact, we may assume j is integral over $\mathfrak{o}_F$ and $j^2 = \varpi$. In matrix form, we may write

$$D = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in E \right\}.$$

(So $j = \begin{pmatrix} & \varpi \\ 1 & \end{pmatrix}$ in this representation.) Then consider lattice in D given by

$$\mathcal{O}_D(2n+1) = \mathfrak{o}_E \oplus \varpi^n \mathfrak{o}_E j = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_E, \beta \in \varpi^n \mathfrak{o}_E \right\}$$

for $n \geq 0$. A simple matrix computation shows this set is closed under multiplication, and thus and order in D. We say this order has **level** $\mathfrak{p}^{2n+1}$.

More generally, we define level as follows.

Definition 6.1.6. *Let $\mathcal{O}$ be a $\mathfrak{o}_F$-order in B. We say $\mathcal{O}$ has* **level** $\mathfrak{p}^n$ *(or level q^n) if $\mathcal{O}$ is isomorphic (as a ring and an $\mathfrak{o}_F$-module) to $\mathcal{O}_B(n)$. We write* $\operatorname{lev}\mathcal{O}$ *for the level of $\mathcal{O}$.*

As an aside, we remark that in the nonsplit setting, this means every order containing the maximal unramified quadratic order has level:

Proposition 6.1.7. *Let B be the nonsplit quaternion algebra D and $\mathcal{O}$ an order in B. Let E/F be the unramified quadratic field extension. Then $\mathcal{O} \simeq \mathcal{O}_D(2n+1)$ for some n if and only if $\mathcal{O}$ contains $\mathfrak{o}_E$ for some embedding of E into B.*

Proof. See [Piz77, Prop 2.2] for a proof when $F = \mathbb{Q}$. See [MR03, Exer 6.4.1] in the general setting. $\square$

When B is split, the notion of level is only defined for Eichler orders.

Exercise 6.1.4. Let $B = M_2(F)$. Show that any Eichler order $\mathcal{O}$ is conjugate to $\mathcal{O}_m \cap \mathcal{O}_n$ for some m, n. Determine the level of $\mathcal{O}_m \cap \mathcal{O}_n$, i.e., the r such that $\mathcal{O}_m \cap \mathcal{O}_n = \mathcal{O}_B(r)$.

The following exercise implies not all orders are Eichler orders.

Exercise 6.1.5. Let $B = M_2(F)$. Show that an order $\mathcal{O}$ is an Eichler order if and only if $\mathcal{O}$ contains $\mathfrak{o}_F \oplus \mathfrak{o}_F$. Construct an order which is not Eichler order. (*Suggestion:* Take the intersection of an Eichler order with another order.)

The first part of this exercise is due to Hijikata—see e.g. [Vig80, Lem II.2.4].

Proposition 6.1.8. *Let $\mathcal{O}$ be an order in B of level $\mathfrak{p}^n$. Then* $\operatorname{disc} \mathcal{O} = \mathfrak{p}^n$.

Proof. First suppose $B = M_2(F)$. Then we may assume $\mathcal{O} = \begin{pmatrix} \mathfrak{o}_F & \mathfrak{o}_F \\ \mathfrak{p}^n & \mathfrak{o}_F \end{pmatrix}$. Then it is easy to check that $\mathcal{O}^\perp = \begin{pmatrix} \mathfrak{o}_F & \mathfrak{p}^{-n} \\ \mathfrak{o}_F & \mathfrak{o}_F \end{pmatrix}$. Then $(\mathcal{O}^\perp)^{-1}$ is the set of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$\begin{pmatrix} \mathfrak{o}_F & \mathfrak{p}^{-n} \\ \mathfrak{o}_F & \mathfrak{o}_F \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathfrak{o}_F & \mathfrak{p}^{-n} \\ \mathfrak{o}_F & \mathfrak{o}_F \end{pmatrix} \subset \begin{pmatrix} \mathfrak{o}_F & \mathfrak{p}^{-n} \\ \mathfrak{o}_F & \mathfrak{o}_F \end{pmatrix},$$

and it is easy to check this means

$$(\mathcal{O}^\perp)^{-1} = \begin{pmatrix} \mathfrak{p}^n & \mathfrak{o}_F \\ \mathfrak{p}^n & \mathfrak{p}^n \end{pmatrix},$$

which has norm (determinant) $\mathfrak{p}^n$.

Next suppose $B = D$ is division and $\mathcal{O} = \mathcal{O}_D(2m+1)$, where $n = 2m+1$. Let E/F be the unramified quadratic extension, so we can realize

$$\mathcal{O} = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_E, \beta \in \varpi^m \mathfrak{o}_E \right\}.$$

It is easy to see that

$$\mathcal{O}^\perp = \left\{ \begin{pmatrix} \alpha & \varpi\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha \in \mathfrak{o}_E^\perp, \beta \in (\varpi^{m+1} \mathfrak{o}_E)^\perp \right\}.$$

Since E/F is unramified, this means $\alpha \in \mathfrak{o}_E$ and $\beta \in \varpi^{-m-1}\mathfrak{o}_E$. One checks the inverse of $\mathcal{O}^\perp$ is all matrices of the above form with $\alpha \in \varpi^{2m+1}\mathfrak{o}_E$ and $\beta \in \varpi^m \mathfrak{o}_E$. This yields that the discriminant is $\mathfrak{p}^{2m+1}$. $\square$

Corollary 6.1.9. *Let $\mathcal{O}$ be a maximal order in B. Then*

$$\operatorname{lev} \mathcal{O} = \operatorname{disc} \mathcal{O} = \begin{cases} \mathfrak{o}_F & B \simeq M_2(F) \\ \mathfrak{p} & \textit{else.} \end{cases}$$

Just like with the class number, we define the **discriminant** of B, denoted $\operatorname{disc} B$, to be the discriminant of a maximal order of B.

6.1.2 Global orders

Now let B be a quaternion algebra over a number field F. By an order in B, we mean an $\mathfrak{o}_F$-order in B. Recall that for a finite place v of F and $\mathcal{O}$ an order (or more generally an $\mathfrak{o}_F$-lattice) in B, the local completion $\mathcal{O}_v = \mathcal{O} \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_v}$. For a finite place v, denote the associated integral ideal of $\mathfrak{o}_F$ by $\mathfrak{p}_v$.

Proposition 6.1.10. *Let $\mathcal{O}$ be an order in B. Then $\mathcal{O}$ is maximal (resp. Eichler) if and only if $\mathcal{O}_v$ is for each $v < \infty$.*

Recall the maximal part was a special case of Proposition 4.5.2, for which we outsourced the proof. I'll leave the proof to you (cf. [Vig80, Sec III.5]):

> **Exercise 6.1.6.** Prove the above proposition.

Definition 6.1.11. *Let $\mathcal{O}$ be an order in B and $\mathfrak{N}$ an integral ideal in $\mathfrak{o}_F$. We say $\mathcal{O}$ has* **level** $\mathfrak{N}$ *and write* $\operatorname{lev}\mathcal{O} = \mathfrak{N}$ *if, for each $v < \infty$, $\mathcal{O}_v$ has level $\mathfrak{p}_v^{n_v}\mathfrak{o}_{F_v}$ and $\mathfrak{N} = \prod \mathfrak{p}_v^{n_v}$. If $F = \mathbb{Q}$, $N \in \mathbb{N}$, and $\mathcal{O}$ has level $N\mathbb{Z}$, we simply say* $\operatorname{lev}\mathcal{O} = N$.

Thus the notion of level is a local notion, and it is defined if and only if $\mathcal{O}_v$ is Eichler for each finite place v such that B_v is split. In particular, the notion of level makes sense if $\mathcal{O}$ is an Eichler order, though it is defined for more general orders. Note that, from the case of local nonsplit quaternion algebras, for any v such that B_v is nonsplit, the level must be of the form $\mathfrak{p}_v^{n_v}$ where n_v is an odd positive integer.

Proposition 6.1.12. *Let $\mathcal{O}$ be an order in B. Then* $\operatorname{disc}\mathcal{O} = \prod_{v<\infty} \operatorname{disc}\mathcal{O}_v$.

Proof. See [Vig80, Cor III.5.2]. □

Corollary 6.1.13. *Let $\mathcal{O}$ be an order in B with level $\mathfrak{N}$. Then* $\operatorname{disc}\mathcal{O} = \mathfrak{N}$.

Proof. This is an immediate consequence of the previous proposition and Proposition 6.1.8. □

> **Example 6.1.4.** Let $F = \mathbb{Q}$, and $B = M_2(F)$. Then $\mathcal{O} = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & \mathbb{Z} \end{pmatrix}$ has level and discriminant N.

You might wonder why we have the notion of level at all if it agrees with discriminant whenever level is defined. First, orders with level are easier to understand than arbitrary orders. Second, it turns out that the orders with level are precisely the orders we want to use when defining quaternionic modular forms.

Here is another consequence of the above proposition.

Corollary 6.1.14. *Let $\mathcal{O}$ be an order in B. Then* $\operatorname{disc}\mathcal{O} = \prod \mathfrak{p}_v$ *where v runs over the finite primes in* $\operatorname{Ram}(B)$ *if and only if $\mathcal{O}$ is a maximal order.*

Proof. If $\mathcal{O}$ is maximal, this is an immediate consequence of the above proposition and Corollary 6.1.9. If $\mathcal{O}$ is not maximal, it lies in a maximal $\mathcal{O}'$, and by Proposition 6.1.3 we know $\operatorname{disc}\mathcal{O} \neq \operatorname{disc}\mathcal{O}'$. □

In particular, the discriminant of maximal order does not depend upon the choice of the maximal order and tells us precisely the finite ramification of B. Define the **discriminant** $\operatorname{disc} B$ of B to be the discriminant of a maximal order. Consequently, from our classification results, if $F = \mathbb{Q}$, then knowing $\operatorname{disc} B$ together with whether B is definite or indefinite determines B up to isomorphism.

Example 6.1.5. Let $B = \mathbb{H}_{\mathbb{Q}} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Since $\operatorname{Ram}(B) = \{2, \infty\}$, $\operatorname{disc} B = 2$. Hence an order $\mathcal{O}$ in B is maximal if and only if $\operatorname{disc}\mathcal{O} = 2$. In particular, the Hurwitz integers are a maximal order in B by Exercise 6.1.2.

For rational quaternion algebras of prime discriminant, explicit descriptions of maximal orders were given independently at about the same time by Pizer [Piz80] and by Hashimoto [Has80]. The following formulation can be found in [Piz80].

Theorem 6.1.15. *Let B be the definite quaternion algebra over $\mathbb{Q}$ ramified at p and infinity. Then we can write $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ and find a maximal order $\mathcal{O}$ according to the following cases:*

(1) If $p = 2$, then $B = \mathbb{H}_{\mathbb{Q}} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\mathcal{O} = \mathbb{Z}\langle 1, i, j, \frac{1+i+j+k}{2}\rangle$ is a maximal order.

(2) If $p \equiv 3 \bmod 4$, then $B = \left(\frac{-1,-p}{\mathbb{Q}}\right)$ and $\mathcal{O} = \mathbb{Z}\langle 1, i, \frac{1+j}{2}, \frac{i+k}{2}\rangle$ is a maximal order.

(3) If $p \equiv 5 \bmod 8$, then $B = \left(\frac{-2,-p}{\mathbb{Q}}\right)$ and $\mathcal{O} = \mathbb{Z}\langle 1, j, \frac{1+j+k}{2}, \frac{i+2j+k}{4}\rangle$ is a maximal order.

(4) If $p \equiv 1 \bmod 8$, then $B = \left(\frac{-p,-q}{\mathbb{Q}}\right)$ where q is a prime that is $3 \bmod 4$ and $\left(\frac{p}{q}\right) = -1$. Moreover, if $m \in \mathbb{N}$ such that $q|(m^2p+1)$, then $\mathcal{O} = \mathbb{Z}\langle k, \frac{1+j}{2}, \frac{i+k}{2}, \frac{j+mk}{q}\rangle$ is a maximal order.

Proof. That the stated Hilbert symbol fits the bill can be deduced from the work in Section 5.2. To check that the given order is maximal, by the latest corollary, it suffices to check $\operatorname{disc}\mathcal{O} = p$. We just illustrate details in the Case (1).

Assume $\operatorname{Ram}(B) = \{2, \infty\}$. Since no odd primes are ramified in $\mathbb{H}_{\mathbb{Q}} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, we know $B \simeq \mathbb{H}_{\mathbb{Q}}$ (cf. Exercise 5.2.3). Then $\operatorname{disc}\mathbb{Z}\langle i, j, k\frac{1+i+j+k}{2}\rangle$ by Exercise 6.1.2. □

Exercise 6.1.7. Prove the above theorem when $p \equiv 3 \bmod 4$.

Further results on explicit constructions of maximal orders for definite quaternion algebras over $\mathbb{Q}$ are given in [Ibu82]. An algorithm for computing maximal orders over an arbitrary number field is presented John Voight's thesis [Voi05, Sec 4.3].

The next exercise describes some simple non-maximal orders in $\mathbb{H}_{\mathbb{Q}}$.

Exercise 6.1.8. Let $B = \mathbb{H}_{\mathbb{Q}} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and m an odd integer. Show the $\mathbb{Z}$-lattices $\mathcal{O}_{1,m}$ for $m \geq 1$ and $\mathcal{O}_{2,m}$ for $m \geq 3$ in B with respective bases $\{1, i, mj, mk\}$ and $\left\{1, i, mj, \frac{1+i+mj+mk}{2}\right\}$ are non-maximal orders in B.

Here is another way to explicitly construct (Eichler or maximal) orders. Our main goal is to illustrate this method, so we will just do this under certain simplifying assumptions.

Proposition 6.1.16. *Let B be a definite quaternion algebra over $\mathbb{Q}$ with $\mathrm{Ram}(B) = \{p_1, p_2, \dots, p_r\}$ such that $d = p_1 \cdots p_r \equiv 7 \bmod 8$. Let $K = \mathbb{Q}(\sqrt{-d})$ and represent*

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

where $b \in \mathbb{Z}$ such that $\gcd(b, d) = 1$ and $\left(\frac{-d}{p}\right) = 1$ for each $p|b$. Then

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

is an Eichler order in B of level $\prod p_i \cdot \prod_{p|b} p^{v_p(b)}$.

Note in order for $\mathrm{Ram}(B) = \{p_1, \dots, p_r\}$, there's also a "hidden" condition that b is a nonsquare mod each p_i (cf. Exercise 5.1.3). As in the proof of Theorem 5.2.4 for $F = \mathbb{Q}$, Dirichlet's theorem on primes in arithmetic progressions implies there always exists some such b which is prime. If each $p_i \equiv 3 \bmod 4$, then we can take $b = -1$ to get a maximal order.

Proof. It suffices to show $\mathcal{O}_p$ is a maximal order for each $p \nmid b$, and Eichler of level $p^{v_p(b)}$ for each $p|b$. The conditions on d mean that $\mathrm{Ram}(K) = \mathrm{Ram}(B)$ and 2 splits in K. The conditions on b means that $b \in \mathbb{Z}_p^\times$ for any p such that $K_p/\mathbb{Q}_p$ is non-split.

First suppose $p = p_i$ for some $i = 1, 2 \dots, r$. Then $K_p/\mathbb{Q}_p$ is ramified and $b \in \mathbb{Z}_p^\times$ must be a nonsquare, so $\mathcal{O}_p$ is maximal by Exercise 6.1.3.

Now let's consider a prime p such that $K_p/\mathbb{Q}_p$ is split. Then $K_p \simeq \mathbb{Q}_p \oplus \mathbb{Q}_p$ and $\mathfrak{o}_{K_p} = \mathfrak{o}_K \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$ (Exercise 4.1.4), so

$$\mathcal{O}_p \simeq \left\{ \begin{pmatrix} (x, y) & b(z, w) \\ (w, z) & (y, x) \end{pmatrix} : x, y, z, w \in \mathbb{Z}_p \right\}$$

(cf. Exercise 3.1.4). We can identify these matrices of pairs with pairs of matrices $\left(\begin{pmatrix} x & bz \\ w & y \end{pmatrix}, \begin{pmatrix} y & bw \\ z & x \end{pmatrix}\right)$, and we see

$$\mathcal{O}_p \simeq \left\{ \begin{pmatrix} x & bz \\ w & y \end{pmatrix} : x, y, z, w \in \mathbb{Z}_p \right\},$$

which is an Eichler order of level $p^{v_p(b)}$ in $B_p = M_2(\mathbb{Q}_p)$.

Finally suppose $p \notin \mathrm{Ram}(B)$ such that $K_p/\mathbb{Q}_p$ is a field extension. Then by assumption $K_p/\mathbb{Q}_p$ is the unique unramified quadratic extension and $B_p \simeq M_2(\mathbb{Q}_p)$. Since $b \in \mathbb{Z}_p^\times$ and

$K_p/\mathbb{Q}_p$ is unramifed (or if you prefer, since $B_p \simeq \left(\frac{-d,b}{\mathbb{Q}_p}\right)$ is split), it must be that b is a norm from $\mathfrak{o}_{K_p}^\times$. Write $b = u\overline{u}$ for some $u \in \mathfrak{o}_{K_p}^\times$. Then making the substitution $\beta \mapsto \overline{u}^{-1}\beta$, we have

$$B_p = \left\{ \begin{pmatrix} \alpha & u\beta \\ u^{-1}\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in K_p \right\},$$

and $\mathcal{O}_p$ is the set of such matrices with $\alpha, \beta \in \mathfrak{o}_{K_p}$. Letting $g = \begin{pmatrix} \sqrt{-d} & -\sqrt{-d} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & \\ & 1 \end{pmatrix}$ and writing $\alpha = x + y\sqrt{-d}$, $\beta = z + w\sqrt{-d}$ we compute

$$g \begin{pmatrix} \alpha & u\beta \\ u^{-1}\overline{\beta} & \overline{\alpha} \end{pmatrix} g^{-1} = \begin{pmatrix} x - z & -d(y+w) \\ y - w & x + z \end{pmatrix}.$$

This conjugation gives an explicit isomorphism of B_p (realized as above) with $M_2(\mathbb{Q}_p)$ such that

$$g\mathcal{O}_p g^{-1} = M_2(\mathbb{Z}_p)$$

(cf. Exercise 1.2.11). Hence $\mathcal{O}_p$ is a maximal order, as desired. $\square$

See also [Has95] for explicit construction of Eichler orders in indefinite rational quaternion algebras.

6.2 Ideals

Recall from Section 4.4 our convention that (unless otherwise qualified) an *ideal* $\mathcal{I}$ of B just means an $\mathfrak{o}_F$-lattice in B. This will be a complete left (resp. right) fractional ideal for $\mathcal{O} = \mathcal{O}_l(\mathcal{I})$ (resp. $\mathcal{O} = \mathcal{O}_r(\mathcal{I})$). Recall an ideal $\mathcal{I}$ is called normal if its left (or equivalently right) order is a maximal order in B.

Let F be a p-adic or number field. The **(reduced) norm** of an ideal $\mathcal{I}$ in B is the ideal $N(\mathcal{I})$ of F generated by the reduced norms $N(\alpha)$ as α runs over $\mathcal{I}$. (This ideal norm was already defined over number fields in a more general context in Section 4.4.) Even though the collection of ideals of B do not form a group, we can multiply ideals of B and the norm map is a multiplicative function from the set of (fractional) ideals of B to the group of (fractional) ideals of F.

6.2.1 Local ideals

Let F be a p-adic field. Then $B = D$ or $B = M_2(F)$, where D is the unique quaternion division algebra over F.

We recall that the ideals of the unique maximal order $\mathcal{O}_D$ of D are easy to describe: they are precisely the lattices of the form $\varpi_D^n \mathcal{O}_D = \{x \in B : v_D(x) \geq n\}$ for $n \in \mathbb{Z}$. These are all two-sided ideals and their (one- and two-sided) class numbers are 1, which just means that for any $x \in B$, there is a unique $n \in \mathbb{Z}$ such that $x = u\varpi_B^n = \varpi_B^n u'$ for some $u, u' \in \mathcal{O}_D^\times$.

For $B = M_2(F)$, all maximal orders are conjugate to the standard one, $M_2(\mathfrak{o}_F)$. The following describes the integral ideals in the standard maximal order.