Brief introduction to quaternion algebras.
Notes for the Isogeny-based Cryptography School 2020 in Bristol

Laia Amorós, Aalto University, Finland

July 2021

These notes are a brief introduction to quaternion algebras and their arithmetic. The goal is to give the reader a quick overview about orders and ideals in quaternion algebras over $\mathbb{Q}$ and point towards useful references on the way. For a more detailed approach, the reader can take a look at the classical notes of Marie-France Vignerás [Vig80]. A more recent and very complete source for quaternion algebras from all possible points of view is [Voi21]. For a nice introduction to the arithmetic of quaternion algebras with many examples and explicit computations one can also see [AB04]. The reader is also encouraged to explore explicit examples of the elements introduced in this text with SageMath [1].

1 Introduction to quaternion algebras

In 1843, William R. Hamilton came up with an extension of the complex numbers, today called *Hamilton quaternions*, that is a 4-dimensional associative algebra over $\mathbb{R}$. We denote Hamilton quaternions as $\mathbb{H}$. Frobenius theorem (1877) characterises finite-dimensional associative division algebras over $\mathbb{R}$. According to this result, every such algebra is isomorphic to one of the following: $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. We can represent a quaternion $h \in \mathbb{H}$ as $h = a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$ and $i^2 = j^2 = -1$ and $ij = -ji = k$. The story gets more interesting if we consider quaternion algebras over other fields other than $\mathbb{R}$.

1.1 Basic definitions

Definition 1.1. Let F denote a field of characteristic $\neq 2$. A *quaternion algebra* over F is a central simple algebra of dimension 4 over F. For $a, b \in F^\times$ we denote by $\left(\frac{a,b}{F}\right)$ the F-algebra generated by a basis $\{1, i, j, k\}$ such that $i^2 = a, j^2 = b$, and $ij = -ji = k$.

A quaternion algebra is either a division algebra (i.e. a non-commutative field), or a matrix algebra.

Example 1.2. The $\mathbb{R}$-algebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is the algebra of (real) Hamilton quaternions $\mathbb{H}$.

Example 1.3. The ring $\mathrm{M}_2(F)$ of 2×2 matrices with coefficients in F is a quaternion algebra over F isomorphic to $\left(\frac{1,1}{F}\right)$ given by: $i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

[1] `https://doc.sagemath.org/html/en/reference/quat_algebras/index.html`

Quaternion algebras behave well with respect to fields inclusion. If we have a field extension $F \subset F'$, then there is a canonical isomorphism

$$\left(\frac{a,b}{F}\right) \otimes_F F' \simeq \left(\frac{a,b}{F'}\right).$$

Given a quaternion algebra $B = \left(\frac{a,b}{F}\right)$ over F there is a natural embedding

$$\begin{array}{rccc} \lambda: & B & \hookrightarrow & \mathrm{M}_2(F(\sqrt{a})) \\ & x + yi + zj + tk & \mapsto & \begin{pmatrix} x + y\sqrt{a} & b(z + t\sqrt{a}) \\ z - t\sqrt{a} & x - y\sqrt{a} \end{pmatrix}. \end{array} \tag{1}$$

One can also consider another embedding, which does not favour i over j, but might be inconvenient in some cases.

$$\begin{array}{rccc} \lambda': & B & \hookrightarrow & \mathrm{M}_2(F(\sqrt{a}, \sqrt{b})) \\ & x + yi + zj + tk & \mapsto & \begin{pmatrix} x + y\sqrt{a} & \sqrt{b}(z + t\sqrt{a}) \\ \sqrt{b}(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}. \end{array}$$

Thus B can be viewed as a subalgebra of $\mathrm{M}_2(\sqrt{a})$.

Definition 1.4. Every quaternion algebra B over F is provided with an F-endomorphism called *conjugation* and denoted by $\beta \mapsto \overline{\beta}$. If $\beta = x + yi + zj + tk \in B$, with $x, y, z, t \in F$, then $\overline{\beta} = x - yi - zj - tk$. The *reduced trace* of β is defined as $\mathrm{trd}(\beta) = \beta + \overline{\beta} = 2x$ and the *reduced norm* of β is defined as $\mathrm{nrd}(\beta) = \beta\overline{\beta} = x^2 - ay^2 - bz^2 + abt^2$.

The reduced norm of B defines a quadratic form (a homogeneous degree 2 polynomial in 4 variables), the *norm form of B*. The structure of a quaternion algebra is thus related to the properties of its norm form. For example, the norm form of a definite quaternion algebra (see 1.2 below) is positive definite, and its indefinite for an indefinite quaternion algebra. More about this can be found in [AB04, Ch. 3].

1.2 Ramification

In order to simplify the exposition of results, we will focus on quaternion algebras over $\mathbb{Q}$. Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ denote a quaternion algebra over $\mathbb{Q}$, with nonzero $a, b \in \mathbb{Z}$. For any prime p we define $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$, for the *infinite prime* ∞ we define $B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R}$.

Definition 1.5. A quaternion algebra B is *ramified* or *non split* at p (resp. at ∞) if B_p is a division algebra, and is *unramified* or *split* at p (resp. at ∞) if $B_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ (resp. $\mathrm{M}_2(\mathbb{R})$). If B is ramified at ∞, it is called a *definite* quaternion algebra. Otherwise is called *indefinite.*

The *reduced discriminant* D_B of B is the product of all ramified primes in B.

In this notes we are interested in definite quaternion algebras.

Proposition 1.6 (Pizer)**.** *Let p be a prime and let $B_{p,\infty} = \left(\frac{a,b}{\mathbb{Q}}\right)$ denote the (definite) quaternion algebra of discriminant $D = p$ over $\mathbb{Q}$. Then we can choose the following presentation for the algebra:*

- $B_{p,\infty} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ *if* $p = 2$*;*
- $B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 3 \pmod 4$*;*
- $B_{p,\infty} = \left(\frac{-2,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 5 \pmod 8$*;*
- $B_{p,\infty} = \left(\frac{-r,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 1 \pmod 8$*, where* r *is a prime such that* $r \equiv 3 \pmod 4$ *and* $\left(\frac{r}{p}\right) = -1$*.*

Remark 1.7. The quaternion algebra $B_{p,\infty}$ is unique up to isomorphism, and it is only ramified at p and ∞.

2 Arithmetic of quaternion algebras

Like number fields, quaternion algebras come equipped with a rich arithmetic, with the main difference of this being non-commutative. Instead of a unique ring of integers, quaternion algebras can have many, these are known as maximal orders.

2.1 Maximal orders and Eichler orders

Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ denote a quaternion algebra with nonzero $a, b \in \mathbb{Z}$. A quaternion $\beta \in B$ is said to be *integral* over $\mathbb{Z}$ if $\operatorname{nrd}(\beta), \operatorname{trd}(\beta) \in \mathbb{Z}$. Unfortunately, as opposed to the number fields case, when combining all integral elements in B one does not obtain a ring, there are simply too many of them.

Definition 2.1. An *order* $\mathcal{O}$ over $\mathbb{Z}$ in a quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ is a $\mathbb{Z}$-lattice that is also a subring of B. Equivalently an order $\mathcal{O} \subset B$ over $\mathbb{Z}$ is a subring of B that contains $\mathbb{Z}$, whose elements are integral over $\mathbb{Z}$ and such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = B$.

More generally, let R denote a ring with field of fractions F, and let B denote a quaternion algebra over F. Then an R-*order* $\mathcal{O}$ in B is an R-lattice that is also a subring of B.

Example 2.2. The *natural* order of a quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ is defined as $\mathcal{O} = \mathbb{Z}[1, i, j, k]$.

The property of being an order is a local property, i.e. if $\mathcal{O} \subset B$ is an order, then $\mathcal{O}_p$ is an order in B_p.

Definition 2.3. Let $\mathcal{O} = \mathbb{Z}[\beta_1, \beta_2, \beta_3, \beta_4]$ be a quaternion order, with $\beta_i \in B$, $i = 1, \ldots, 4$. The discriminant $\operatorname{disc}(O)$ of $\mathcal{O}$ is defined as the ideal of $\mathbb{Z}$ generated by

$$\det(\operatorname{trd}(\beta_i \beta_j))_{i,j=1,\ldots,4} \subseteq \mathbb{Z}.$$

As $\mathbb{Z}$ is a PID, we can identify the discriminant with a positive generator of the above ideal. $\operatorname{disc}(\mathcal{O})$ is always a square, so we define $\operatorname{discrd}(\mathcal{O})$ by $\operatorname{discrd}(\mathcal{O})^2 = \operatorname{disc}(\mathcal{O})$. We can measure how *big* an order is with its discriminant. An order is *maximal* if it is not properly contained in any other order.

Remark 2.4. To check the maximality of $\mathcal{O}$ one can use the fact that an order $\mathcal{O}$ in B is maximal if and only if $\operatorname{discrd}(\mathcal{O}) = D_B$ (see [AB04], Prop. 1.50). Note that, unlike in number fields, maximal orders in quaternion algebras are not necessarily unique [Vig80], but they all have the same discriminant, which coincides with the discriminant of the algebra.

Given a maximal order $\mathcal{O}$, we can always conjugate it with any quaternion $\beta \in B^\times$ and obtain another (possibly the same) order $\beta^{-1}\mathcal{O}\beta$. Two orders $\mathcal{O}, \mathcal{O}' \subset B$ are *of the same type* if they are conjugated by some $\beta \in B^\times$. If we consider all maximal quaternion orders up to conjugation in B, we obtain a finite number of conjugacy classes of maximal orders, known as the *type number* of B.

We can show a basis for a maximal order in the quaternion algebras from Prop. 1.6.

Proposition 2.5 ([Piz80], Prop 5.2)**.** *Let $B_{p,\infty}$ denote the definite quaternion algebra of discriminant p, where p is a prime. A maximal order of B is given by*
- $\mathbb{Z}[1, i, j, \frac{1+i+j+k}{2}]$, *if* $p = 2$;
- $\mathbb{Z}[1, i, \frac{i+j}{2}, \frac{1+k}{2}]$, *if* $p \equiv 3 \pmod 4$;
- $\mathbb{Z}[1, \frac{1+i+j}{2}, j, \frac{2+i+k}{4}]$ *if* $p \equiv 5 \pmod 8$;
- $\mathbb{Z}[1, \frac{1+j}{2}, \frac{j+ak}{2}, k]$ *if* $p \equiv 1 \pmod 8$, *where r is a prime such that* $r \equiv 3 \pmod 4$ *and* $\left(\frac{r}{p}\right) = -1$.

Another notion worth mentioning is that of Eichler orders.

Definition 2.6. An *Eichler order* is an order that is the intersection of two maximal orders.

The property of being an Eichler order is also a local property. The following result enlightens why we are interested in these kind of orders. Let $\mathbb{Q}_\ell$ denote the field of ℓ-adic numbers, for some prime integer ℓ.

Proposition 2.7 ([Voi21, Prop. 23.4.3])**.** *Consider the quaternion algebra $B = \mathrm{M}_2(\mathbb{Q}_\ell)$ and let $\mathcal{O} \subset B$ denote a $\mathbb{Z}_\ell$-order. Then the following are equivalent:*

(*a*) *$\mathcal{O}$ is an Eichler order;*

(*b*) $\mathcal{O} \simeq \begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ \ell^e\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix}$, *called the standard order of level* ℓ^e;

(*c*) *$\mathcal{O}$ contains a $\mathbb{Z}_\ell$-subalgebra that is $B^\times$-conjugate to* $\mathcal{O} \simeq \begin{pmatrix} \mathbb{Z}_\ell & 0 \\ 0 & \mathbb{Z}_\ell \end{pmatrix}$;

(*d*) *$\mathcal{O}$ is the intersection of a uniquely determined pair of maximal orders (not necessarily distinct).*

This characterisation of Eichler orders in the the local quaternion algebra $B = \mathrm{M}_2(\mathbb{Q}_\ell)$ gives rise to a very useful combinatorial construction that keeps track of the containments of orders in $B = \mathrm{M}_2(\mathbb{Q}_\ell)$, the so-called *Bruhat-Tits tree* for $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. Supersingular isogeny graphs are closely connected to Bruhat-Tits trees. For a comprehensive review on this connection the reader is referred to [AIL$^+$21].

2.2 Left- right- and two-sided ideals

Let B denote a quaternion algebra over $\mathbb{Q}$. Every maximal order in B behaves as a non-commutative ring of integers of the quaternion algebra. Ideals are next to be presented. An *ideal* I of B is a $\mathbb{Z}$-lattice of rank 4. They come in different flavours.

Definition 2.8. Let B denote a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ denote an order of B. An ideal I of B is a *left-ideal* (resp. *right-ideal*) of $\mathcal{O}$ if $\mathcal{O}I := \{xI : x \in \mathcal{O}\} \subset I$ (resp. $I\mathcal{O} := \{Ix : x \in \mathcal{O}\} \subset I$). If $I \subset \mathcal{O}$ the ideal is an *integral* ideal of $\mathcal{O}$.

The *reduced norm* $\mathrm{nrd}(I)$ of an ideal I is defined as $\gcd\{\mathrm{nrd}(\beta) : \beta \in I\}$.

Any ideal $I \subset B$ has two associated orders:

- the *left-order* of I: $\mathcal{O}_l(I) := \{x \in B : xI \subseteq I\}$;
- the *right-order* of I: $\mathcal{O}_r(I) := \{x \in B : Ix \subseteq I\}$.

An ideal $I \subset B$ such that $\mathcal{O}_l(I) = \mathcal{O}_r(I)$ is called a *two-sided* ideal.

Note that not all ideals are compatible with respect to multiplication. The product $I \cdot J$ of two ideals $I, J \subset B$ makes sense provided that $\mathcal{O}_r(I) = \mathcal{O}_l(J)$.

We can also consider ideal classes just like in the number fields case.

Definition 2.9. Two ideals $I,\ J \subset B$ belong to the same *left-ideal class* (resp. *right-ideal class*) if there exists $\beta \in B^\times$ such that $I = J\beta$ (resp. $I = \beta J$). Given a maximal order $\mathcal{O}$, we denote by $\mathrm{Cl}_l(\mathcal{O})$ the set of *left-ideal classes of* $\mathcal{O}$ (and by $\mathrm{Cl}_r(\mathcal{O})$ its set of *right-ideal classes*).

The number of left-ideal classes of an order $\mathcal{O}$ in B (which could be infinite a priori) is a finite number, and it coincides with the number of right-ideal classes of $\mathcal{O}$. We call this number the *ideal class number of* $\mathcal{O}$. All maximal orders in a quaternion algebra have the same ideal class number. The *class number* of a quaternion algebra B is the left-ideal class number of a maximal order in B. For more details check [Voi21, Ch. 17].

Exercises

Exercise 1. The elements $a, b \in F^\times$ are not unique in determining the isomorphism class of a quaternion algebra.

(i) Show that

$$\left(\frac{a, b}{F}\right) \simeq \left(\frac{a, -ab}{F}\right) \simeq \left(\frac{b, -ab}{F}\right).$$

(ii) Let $c, d \in F^\times$. Show that

$$\left(\frac{a, b}{F}\right) \simeq \left(\frac{ac^2, bd^2}{F}\right).$$

This shows, in particular, that any quaternion algebra B over $\mathbb{Q}$ is isomorphic to $\left(\frac{a,b}{\mathbb{Q}}\right)$ for some $a, b \in \mathbb{Z}$.

Hint: You might want to use the *Hilbert symbol* (cf. [Voi21, 12.4]).

Exercise 2. Show that a quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ is definite if and only if $a, b < 0$, where $a, b \in \mathbb{Z}$.

Exercise 3. Show that, for any $\beta \in B$ we have $\mathrm{trd}(\beta) = \mathrm{Tr}(\lambda(\beta)) = \mathrm{Tr}(\lambda'(\beta))$ and $\mathrm{nrd}(\beta) = \det(\lambda(\beta)) = \det(\lambda'(\beta))$.

Exercise 4. Consider the quaternion algebra $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$. Prove that the order $\mathbb{Z}[1, i, j, k]$ is not maximal. Prove that $\mathbb{Z}[1, i, j, \frac{1+i+j+k}{2}]$ is maximal. This order is known as the *Hurwitz order*.

Exercise 5 (Units)**.** The *units* of an order $\mathcal{O}$ of a quaternion algebra over some field F are the elements $u \in \mathcal{O}$ such that its inverse is also in $\mathcal{O}$. They form a group denoted by $\mathcal{O}^\times$. The units with reduced norm 1 form a subgroup in $\mathcal{O}^\times$ denoted by $\mathcal{O}^1$.

(i) Show that an element in $\mathcal{O}$ is a unit if and only if its reduced norm is a unit in $\mathbb{Z}_F$, the ring of integers of F.

(ii) Compute the units of the Hurwitz order.

Exercise 6. Choose a quaternion algebra with prime discriminant and compute a maximal order $\mathcal{O}$. Use Sage to compute a representative for every left ideal class of $\mathcal{O}$ and then compute the right orders for this ideals. (Note: If the discriminant is very small you might only have one ideal class.)

References

[AB04] Montserrat Alsina and Pilar Bayer, *Quaternion orders, quadratic forms, and shimura curves* (American Math. Soc., ed.), Providence, RI, vol. 22, CRM Monograph Series, 2004. ↑(document), 1.1, 2.4

[AIL+21] Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková, *Explicit connections between supersingular isogeny graphs and bruhat–tits trees*, Women in Numbers Europe III: Research Directions in Number Theory (2021). ↑2.1

[Piz80] Arnold Pizer, *An algorithm for computing modular forms on* $\gamma_0(n)$, Journal of Algebra **Vol. 64, Issue 2** (1980). ↑2.5

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, 1980. ↑(document), 2.4

[Voi21] John Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer International Publishing, 2021. `https://math.dartmouth.edu/~jvoight/quat.html`. ↑(document), 2.7, 2.2, 1