CHAPTER 1

Quaternion algebras

This chapter will serve as an introduction to the theory of central simple algebras, by developing some aspects of the general theory in the simplest case of quaternion algebras. The results proved here will not really be used in the sequel, and many of them will be in fact substantially generalised by other means. Rather we would like to show what can be done "by hand", which may help appreciate the more sophisticated methods developed in the sequel.

Quaternions are historically very significant; since their discovery by Hamilton in 1843, they have played an influential role in various branches of mathematics. A particularity of these algebras is their deep relations with quadratic forms, which is not really a systematic feature of central simple algebras. For this reason, we will merely hint at the connections with quadratic form theory.

1. The norm form

All rings will be unital and associative (but often noncommutative!).

We fix a base field k. The set of nonzero elements of k equipped with the multiplication is a group, that we denote by $k^\times$. In this chapter we will assume that the characteristic of k is not equal to two.

Definition 1.1.1. Let $a, b \in k^\times$. We define a k-algebra (a, b) as follows. A basis of (a, b) as k-vector space is given by $1, i, j, ij$. The multiplication is determined by the rules $\lambda q = q\lambda$ for all $q \in (a, b)$ and $\lambda \in k$, and

$$i^2 = a, \quad j^2 = b, \quad ij = -ji. \tag{1.1.a}$$

We will call i, j the *standard generators* of (a, b). An algebra isomorphic to (a, b) for some $a, b \in k^\times$ will be called a *quaternion algebra*.

Lemma 1.1.2. *Let A be a 4-dimensional k-algebra such that $a\lambda = \lambda a$ for all $a \in A$ and $\lambda \in k$. If $i, j \in A$ satisfy the relations* (1.1.a) *for some $a, b \in k^\times$, then $A \simeq (a, b)$.*

Proof. It will suffice to prove that the elements $1, i, j, ij$ are linearly independent over k. Since i anticommutes with j, the elements $1, i, j$ must be linearly independent. Now assume that $ij = u + vi + wj$, with $u, v, w \in k$. Then

$$0 = i(ij + ji) = i(ij) + (ij)i = i(u + vi + wj) + (u + vi + wj)i = 2ui + 2av,$$

hence $u = v = 0$. So $ij = wj$, hence $ij^2 = wj^2$ and thus $bi = bw$, a contradiction. □

Lemma 1.1.3. *Let $a, b \in k^\times$. Then*

(i) $(a, b) \simeq (b, a)$,

(ii) $(a, b) \simeq (a\alpha^2, b\beta^2)$ *for any $\alpha, \beta \in k^\times$.*

PROOF. (i) : The isomorphism is given by exchanging i and j.
(ii) : The isomorphism is given by $i \mapsto \alpha i$ and $j \mapsto \beta j$. □

LEMMA 1.1.4. *For any $b \in k^\times$, the k-algebra $(1, b)$ is isomorphic to the algebra $M_2(k)$ of 2 by 2 matrices with coefficients in k.*

PROOF. The matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, J = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \in M_2(k)$$

satisfy $I^2 = 1, J^2 = b, IJ = -JI$. Thus the statement follows from Lemma 1.1.2. □

From now on, the letter Q will denote a quaternion algebra over k.

DEFINITION 1.1.5. An element $q \in Q$ such that $q^2 \in k$ and $q \notin k^\times$ will be called a *pure quaternion*.

LEMMA 1.1.6. *Let $a, b \in k^\times$ and $x, y, z, w \in k$. The element $x + yi + zj + wij$ in the quaternion algebra (a, b) is a pure quaternion if and only if $x = 0$.*

PROOF. This follows from the computation

$$(x + yi + zj + wij)^2 = x^2 + ay^2 + bz^2 - abw^2 + 2x(yi + zj + wij).$$ □

LEMMA 1.1.7. *The subset $Q_0 \subset Q$ of pure quaternions is a k-subspace, and we have $Q = k \oplus Q_0$ as k-vector spaces.*

PROOF. Letting $a, b \in k^\times$ be such that $Q \simeq (a, b)$, this follows from Lemma 1.1.6. □

It follows from Lemma 1.1.7 that every $q \in Q$ may be written uniquely as $q = q_1 + q_2$, where $q_1 \in k$ and q_2 is a pure quaternion. We define the *conjugate of* q as $\overline{q} = q_1 - q_2$. The following properties are easily verified:

(i) $q \mapsto \overline{q}$ is k-linear.
(ii) $\overline{\overline{q}} = q$ for all $q \in Q$.
(iii) $q = \overline{q} \iff q \in k$.
(iv) $q = -\overline{q} \iff q \in Q_0$.
(v) $q\overline{q} \in k$ for all $q \in Q$.
(vi) $\overline{pq} = \overline{q}\,\overline{p}$ for all $p, q \in Q$.

DEFINITION 1.1.8. We define the *(quaternion) norm map* $N: Q \to k$ by $q \mapsto q\overline{q}$.

For all $p, q \in Q$, we have $N(pq) = N(p)N(q)$ for all $p, q \in Q$. If $a, b \in k^\times$ are such that $Q = (a, b)$ and $q = x + yi + zj + wij$ with $x, y, z, w \in k$, then

$$N(q) = x^2 - ay^2 - bz^2 + abw^2. \tag{1.1.b}$$

LEMMA 1.1.9. *An element $q \in Q$ admits a two-sided inverse if and only if $N(q) \neq 0$.*

PROOF. If $N(q) \neq 0$, then q is a left inverse of $N(q)^{-1}\overline{q}$, hence a two-sided inverse by Remark 1.1.11. Conversely, if $pq = 1$, then $N(p)N(q) = 1$, hence $N(q) \neq 0$. □

We will give below a list of criteria for a quaternion algebra to be isomorphic to $M_2(k)$. In order to do so, we need some definitions.

DEFINITION 1.1.10. A ring (resp. a k-algebra) D is called *division* if it is nonzero and every nonzero element of D admits a two-sided inverse. Such rings are also called skew-fields in the literature.

REMARK 1.1.11. Let A be a finite dimensional k-algebra and $a \in A$. We claim that a left inverse of a is automatically a two-sided inverse. Indeed, assume that $u \in A$ satisfies $ua = 1$. Then the k-linear morphism $A \to A$ given by $x \mapsto ax$ is injective (as $ax = 0$ implies $x = uax = 0$), hence surjective by reasons of dimensions. In particular 1 lies in its image, hence there is $v \in A$ such that $av = 1$. Then $u = u(av) = (ua)v = v$.

DEFINITION 1.1.12. Let A be a commutative finite dimensional k-algebra. The (algebra) norm map $N_{A/k} \colon A \to k$ is defined by mapping $a \in A$ to the determinant of the k-linear map $A \to A$ given by $x \mapsto ax$.

It follows from the multiplicativity of the determinant that $N_{A/k}(ab) = N_{A/k}(a)N_{A/k}(b)$ for every $a, b \in A$.

When $a \in k$, we consider the field extension

$$k(\sqrt{a}) = \begin{cases} k & \text{if } a \text{ is a square in } k, \\ k[X]/(X^2 - a) & \text{if } a \text{ is not a square in } k. \end{cases}$$

In the second case, we will denote by $\sqrt{a} \in k(\sqrt{a})$ the element corresponding to X (this element is determined only up to sign by the field extension $k(\sqrt{a})/k$). Every element of $k(\sqrt{a})$ is represented as $x + y\sqrt{a}$ for uniquely determined $x, y \in k$, and

$$N_{k(\sqrt{a})/k}(x + y\sqrt{a}) = x^2 - ay^2.$$

PROPOSITION 1.1.13. *Let $a, b \in k^\times$. The following are equivalent.*

(i) $(a, b) \simeq M_2(k)$.
(ii) (a, b) *is not a division ring.*
(iii) The quaternion norm map $(a, b) \to k$ *has a nontrivial zero.*
(iv) We have $b \in N_{k(\sqrt{a})/k}(k(\sqrt{a}))$.
(v) There are $x, y \in k$ *such that* $ax^2 + by^2 = 1$.
(vi) There are $x, y, z \in k$*, not all zero, such that* $ax^2 + by^2 = z^2$.

PROOF. Next time. $\square$