Brauer Groups of fields

Olivier Haution

Ludwig-Maximilians-Universität München

Winter semester 2020/2021

Contents

Note on the literature

The main references that we used in preparing these notes is the book of Gille and Szamuely [**GS17**]. As always, Serre's books [**Ser62, Ser02**] provide excellent accounts. There is also very useful material contained in the Stack's project [**Sta**] (available online). Kersten's book [**Ker07**] (in German, available online) provides a very gentle introduction to the subject.

For the first part (on noncommutative algebra), we additionally used Draxl's [**Dra83**] and Pierce's [**Pie82**], as well as Lam's book [**Lam05**] (which uses the language of quadratic forms) for quaternion algebras. For the second part (on torsors), we used the book of involutions [**KMRT98**, Chapters V and VII].

Part 1

Noncommutative Algebra

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 assumed to be unital and associative (but often noncommutative!). The set of elements of a ring R admitting a two-sided inverse is a group, that we denote by $R^\times$.

We fix a base field k. A k-algebra is a ring A equipped with a structure of k-vector space such that the multiplication map $A \times A \to A$ is k-bilinear. A morphism of k-algebras is a ring morphism which is k-linear. If A is nonzero, the map $k \to A$ given by $\lambda \mapsto \lambda 1$ is injective, and we will view k as a subring of A. Observe that the bilinearity of the multiplication map implies that for any $\lambda \in k$ and $a \in A$

$$\lambda a = (\lambda a)1 = a(\lambda 1) = a\lambda. \tag{1.1.a}$$

In this chapter on quaternion algebras, we will assume that the characteristic of k is not equal to two (i.e. $2 \neq 0$ in k).

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 $1, i, j, ij$. It is easy to verify that (a, b) admits a unique k-algebra structure such that

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

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. If $i, j \in A$ satisfy the relations (1.1.b) 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 (recall that the characteristic of k differs from 2). 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 $u = v = 0$ by linear independence of $1, i$. So $ij = wj$, hence $ij^2 = wj^2$ and thus $bi = bw$, a contradiction with the linear independence of $1, i$. □

The following observations will be used without explicit mention.

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) : We let i', j' be the standard generators of (b, a), and apply Lemma 1.1.2 with $i = j'$ and $j = i'$.

(ii): We let i'', j'' be the standard generators of $(a\alpha^2, b\beta^2)$, and apply Lemma 1.1.2 with $i = \alpha^{-1}i''$ and $j = \beta^{-1}j''$. □

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, for any $p, q \in Q$:

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

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

Observe that the norm map is multiplicative:

$$N(pq) = N(p)N(q) \quad \text{for all } p, q \in Q.$$

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

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

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 two-sided inverse of $N(q)^{-1}\overline{q}$. Conversely, if $p \in Q$ is such that $pq = 1$, 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 first 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 dimensional reasons. In particular 1 lies in its image, hence there is $v \in A$ such that $av = 1$. Then $u = u(av) = (ua)v = v$.

A similar argument shows that a right inverse of a is automatically a two-sided inverse.

DEFINITION 1.1.12. Let A be a commutative finite-dimensional k-algebra. The (algebra) norm map $\mathrm{N}_{A/k} : A \to k$ 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

$$\mathrm{N}_{A/k}(ab) = \mathrm{N}_{A/k}(a)\,\mathrm{N}_{A/k}(b) \quad \text{for all } a, b \in A.$$

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, let $\alpha \in k(\sqrt{a})$ be such that $\alpha^2 = a$ (such an element is determined only up to sign by the field extension $k(\sqrt{a})/k$). Every element of $k(\sqrt{a})$ is represented as $x + y\alpha$ for uniquely determined $x, y \in k$, and

$$\mathrm{N}_{k(\sqrt{a})/k}(x + y\alpha) = x^2 - ay^2. \tag{1.1.d}$$

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 $b \in \mathrm{N}_{k(\sqrt{a})/k}(k(\sqrt{a}))$.
(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. (i) $\Rightarrow$ (ii) : The nonzero matrix
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(k)$$
is not invertible.

(ii) $\Rightarrow$ (iii) : This follows from Lemma 1.1.9.

(iii) $\Rightarrow$ (iv) : We may assume that a is not a square in k, and choose $\alpha \in k(\sqrt{a})$ such that $\alpha^2 = a$. Let $q = x + yi + zj + wij$ be a nontrivial zero of the norm map, where $x, y, z, w \in k$. Then by the formula (1.1.c)
$$0 = x^2 - ay^2 - bz^2 + abw^2,$$
hence $x^2 - ay^2 = b(z^2 - aw^2)$. Assume that $z^2 - aw^2 = 0$. Then $z = w = 0$, because a is not a square. Also $x^2 - ay^2 = 0$, and for the same reason $x = y = 0$. Thus $q = 0$, a contradiction. Therefore $z^2 - aw^2 \neq 0$, and by (1.1.d)
$$b = \frac{x^2 - ay^2}{z^2 - aw^2} = \frac{\mathrm{N}_{k(\sqrt{a})/k}(x + y\alpha)}{\mathrm{N}_{k(\alpha)/k}(z + w\alpha)} = \mathrm{N}_{k(\alpha)/k}\left(\frac{x + y\alpha}{z + w\alpha}\right).$$

(iv) $\Rightarrow$ (v) : Let $\alpha \in k(\sqrt{a})$ be such that $\alpha^2 = a$. If $\alpha \in k$, then we may take $x = \alpha^{-1}$ and $y = 0$. If $\alpha \notin k$, then by (iv) there are $u, v \in k$ such that $b = \mathrm{N}_{k(\sqrt{a})/k}(u + v\alpha)$. Then $b = u^2 - av^2$ by (1.1.d). If $u \neq 0$, we may take $x = vu^{-1}$ and $y = u^{-1}$. Assume that $u = 0$. Then $b = -av^2$, and in particular $v \neq 0$. Let
$$x = \frac{a+1}{2a} \quad \text{and} \quad y = \frac{a-1}{2av}.$$
Then
$$ax^2 + by^2 = ax^2 - av^2y^2 = \frac{a^2 + 2a + 1}{4a} - \frac{a^2 - 2a + 1}{4a} = 1.$$

(v) $\Rightarrow$ (vi) : Take $z = 1$.

(vi) $\Rightarrow$ (i) : By Lemma 1.1.4 (and Lemma 1.1.3 (ii)) we may assume that a is not a square in k, so that $y \neq 0$. Applying Lemma 1.1.14 below with $u = xy^{-1}, v = zy^{-1}$ and $c = b$ yields $(a, b) \simeq (a, b^2)$. Since $(a, b^2) \simeq (1, a)$ (by Lemma 1.1.3), we obtain (i) using Lemma 1.1.4. □

LEMMA 1.1.14. *Let $a, b, c \in k^\times$, and assume that $au^2 + c = v^2$ for some $u, v \in k$. Then $(a, b) \simeq (a, bc)$.*

PROOF. Denote by i', j' the standard generators of (a, bc). Set
$$i = i', \quad j = c^{-1}(vj' + ui'j') \in (a, bc).$$
The relation $i'j' + j'i' = 0$ implies that $ij + ji = 0$. We have $i^2 = i'^2 = a$, and
$$j^2 = c^{-2}(bcv^2 - abcu^2) = bc^{-1}(v^2 - au^2) = b.$$
It follows from Lemma 1.1.2 that $(a, bc) \simeq (a, b)$. □

DEFINITION 1.1.15. A quaternion algebra satisfying the conditions of Proposition 1.1.13 will be called *split* (observe that this does not depend on the choice of $a, b \in k^\times$).

EXAMPLE 1.1.16. Assume that k is *quadratically closed*, i.e. that every element of k is a square. Then for every $a, b \in k^\times$, we have $(a, b) \simeq (1, b) \simeq M_2(k)$ by Lemma 1.1.4 (and Lemma 1.1.3 (ii)). Therefore every quaternion k-algebra splits.

Example 1.1.17. Assume that the field k is finite, with q elements. As the group $k^\times$ is cyclic of order $q-1$, there are exactly $1+(q-1)/2$ squares in k. Thus the sets $\{ax^2|x \in k\}$ and $\{1-by^2|y \in k\}$ both consist of $1+(q-1)/2$ elements; as subsets of the set k having q elements, they must intersect. It follows from the criterion (v) in Proposition 1.1.13 that (a,b) splits. Therefore *every quaternion algebra over a finite field is split.*

Example 1.1.18. Let $k=\mathbb{R}$. The quaternion algebra $(-1,-1)$ is not split, by Proposition 1.1.13 (v). Since $k^\times/k^{\times 2} = \{1,-1\}$, and taking into account Lemma 1.1.4 (as well as Lemma 1.1.3), we see that there are exactly two isomorphism classes of k-algebras, namely $M_2(k)$ and $(-1,-1)$.

Let us record another useful consequence of Lemma 1.1.14.

Proposition 1.1.19. *Let $a,b,c \in k^\times$. If (a,c) is split, then $(a,bc) \simeq (a,b)$.*

Proof. Since (a,c) is split, by Proposition 1.1.13 (iv) and (1.1.d) there are $u,v \in k$ such that $c = v^2 - au^2$. The statement follows from Lemma 1.1.14. □

Bibliography

[Dra83] P. K. Draxl. *Skew fields*, volume 81 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017.

[Ker07] Ina Kersten. *Brauergruppen*. Universitätsverlag Göttingen, Göttingen, 2007. `https://univerlag.uni-goettingen.de/bitstream/handle/3/isbn-978-3-938616-89-5/brauergruppen.pdf`.

[KMRT98] Max-Albert Knus, Alexander S. Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions. With a preface by J. Tits.* Providence, RI: American Mathematical Society, 1998.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[Pie82] Richard S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982. Studies in the History of Modern Science, 9.

[Ser62] Jean-Pierre Serre. *Corps locaux*. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.

[Sta] The Stacks Project Authors. Stacks Project. `http://stacks.math.columbia.edu`.