Galois cohomology

Olivier Haution

Ludwig-Maximilians-Universität München

Summer semester 2020

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 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 (unital associative) 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 $A \neq 0$, 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.

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

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

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. 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. $\square$

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 $j \mapsto \beta j$. $\square$

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. $\square$

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

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

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. $\square$

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* $N \colon Q \to k$ 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

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

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 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 $N(q) \neq 0$. $\square$

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. (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. 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. Thus $x^2 - ay^2 = 0$, and for the same reason $x = y = 0$. Thus $q = 0$, a contradiction. Therefore $z^2 - aw^2 \neq 0$, and

$$b = \frac{x^2 - ay^2}{z^2 - aw^2} = \frac{N_{k(\sqrt{a})/k}(x + y\sqrt{a})}{N_{k(\sqrt{a})/k}(z + w\sqrt{a})} = N_{k(\sqrt{a})/k}\Big(\frac{x + y\sqrt{a}}{z + w\sqrt{a}}\Big).$$

(iv) $\Rightarrow$ (v) : There are $u, v \in k$ such that $b = N_{k(\sqrt{a})/k}(u + v\sqrt{a}) = u^2 - av^2$, so we may take $x = vu^{-1}$ and $y = u^{-1}$.

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

(vi) $\Rightarrow$ (i) : By Lemma 1.1.4 we may assume that a is not a square in k, so that $y \neq 0$. Let i, j be the standard generators of (a, b), and set in (a, b)

$$i' = i, \quad j' = b^{-1}y^{-1}(zj + xij).$$

The relation $ij + ji = 0$ implies that $i'j' + j'i' = 0$. We have $i'^2 = i^2 = a$, and

$$j'^2 = b^{-2}y^{-2}(bz^2 - abx^2) = b^{-1}y^{-2}(z^2 - ax^2) = 1$$

By Lemma 1.1.2, we have $Q \simeq (a, 1) \simeq (1, a)$, and (i) follows from Lemma 1.1.4. □

DEFINITION 1.1.14. 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 1.1.15. Assume 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. Therefore every quaternion k-algebra splits.

EXAMPLE 1.1.16. 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 1.1.17. 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, 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 the argument used to prove the implication (vi) $\Rightarrow$ (i) in Proposition 1.1.13:

PROPOSITION 1.1.18. *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) there are $\alpha, \beta \in k$ such that $c = \alpha^2 - a\beta^2$. Let $Q = (a, bc)$ with its standard generators i', j'. Set

$$i = i', \quad j = c^{-1}(\alpha j' + \beta i'j') \in Q.$$

The relation $i'j' + j'i' = 0$ implies that $ij + ji = 0$. We have $i^2 = i'^2 = a$, and

$$j^2 = c^{-2}(bc\alpha^2 - abc\beta^2) = bc^{-1}(\alpha^2 - a\beta^2) = b.$$

It follows from Lemma 1.1.2 that $Q \simeq (a, b)$. □

PROPOSITION 1.1.19. *Let Q, Q' be quaternion algebras, with pure quaternion subspaces Q_0, Q_0'. Then $Q \simeq Q'$ if and only if there is a k-linear map $\varphi\colon Q_0 \to Q_0'$ such that $\varphi(q)^2 = q^2 \in k$ for all $q \in Q_0$.*

Proof. Let $\psi\colon Q \to Q'$ be an isomorphism of k-algebras. If $q \in Q_0$, then

$$\psi(q)^2 = \psi(q^2) = q^2 \in k, \quad \text{and } \psi(q) \notin \psi(k^\times) = k^\times,$$

so that $\psi(q) \in Q_0'$. So we may take for φ the restriction of ψ.

Conversely, let $\varphi\colon Q_0 \to Q_0'$ be a k-linear map such that $\varphi(q)^2 = q^2 \in k$ for all $q \in Q_0$. We may assume that $Q = (a,b)$ with its standard generators i,j. We have $\varphi(i)^2 = i^2 = a$ and $\varphi(j)^2 = j^2 = b$, and

$$\varphi(i)\varphi(j) + \varphi(j)\varphi(i) = \varphi(i+j)^2 - \varphi(i)^2 - \varphi(j)^2 = (i+j)^2 - i^2 - j^2 = ij + ji = 0.$$

By Lemma 1.1.2 (applied to the elements $\varphi(i), \varphi(j) \in Q'$), we have $Q' \simeq (a,b)$. $\square$

The norm map $N\colon Q \to k$ is in fact a quadratic form. The next corollary is a reformulation of Proposition 1.1.19, assuming some basic quadratic form theory. It can be safely ignored, and will not be used in the sequel.

Corollary 1.1.20. *Two quaternion algebras are isomorphic if and only if their norm forms are isometric.*

Proof. Let Q be a quaternion algebra and $N\colon Q \to k$ its norm form. Note that $N(q) = -q^2$ for all $q \in Q_0$. The subspaces k and Q_0 are orthogonal in Q with respect to the norm form N, and $N|_k = \mathrm{id}_k$. So we have a decomposition $N \simeq \langle 1 \rangle \perp (N|_{Q_0})$. This quadratic form is nondegenerate (e.g. by (1.1.c)), hence a morphism φ as in Proposition 1.1.19 is automatically an isometry. The corollary follows, by Witt's cancellation Theorem (see for instance [**Lam05**, Theorem 4.2]). $\square$

2. Quadratic splitting fields

Definition 1.2.1. The *center* of a ring R is the set of elements $r \in R$ such that $rs = sr$ for all $s \in R$. As observed in (1.1.a), the center of a nonzero k-algebra always contains k. A k-algebra is called *central* if it is nonzero and its center equals k.

Lemma 1.2.2. *Every quaternion algebra is central.*

Proof. We may assume that the algebra is equal to (a,b) with $a,b \in k^\times$. Consider an arbitrary element $q = x+yi+zj+wij$ of (a,b), where $x,y,z,w \in k$. Easy computations show that $qi = iq$ if and only if $z = w = 0$, and that $qj = jq$ if and only if $y = w = 0$. $\square$

Remark 1.2.3. Let $a,b \in k^\times$. We claim that (a,b) contains a subfield isomorphic to $k(\sqrt{a})$. To see this, we may assume that a is not a square in k. Then the morphism of k-algebras $k(\sqrt{a}) = k[X]/(X^2 - a) \to (a,b)$ given by $X \mapsto i$ is injective.

Proposition 1.2.4. *Let D be a central division k-algebra of dimension 4. Assume that D contains a k-subalgebra isomorphic to $k(\sqrt{a})$ for some $a \in k$ which is not a square in k. Then $D \simeq (a,b)$ for some $b \in k^\times$.*

Proof. Let $L \subset D$ be a subalgebra isomorphic to $k(\sqrt{a})$, and $\alpha \in L$ such that $\alpha^2 = a$. Since α does not lie in the center of D, there is $x \in D$ such that $x\alpha \neq \alpha x$. Then $\beta = \alpha^{-1}x\alpha - x$ is nonzero. Using the fact that $\alpha^2 = a$ is in the center of D, we see that

$$\beta\alpha = \alpha^{-1}x\alpha^2 - x\alpha = \alpha x - x\alpha = -\alpha\beta.$$

Multiplying with β on the left, resp. right, we obtain $\beta^2\alpha = -\beta\alpha\beta$, resp. $\beta\alpha\beta = -\alpha\beta^2$. It follows that β^2 commutes with α. Since β does not commute with α, we have $\beta \notin L$. Therefore the L-subspace of D generated by $1, \beta$ has dimension two over L, hence coincides with D by dimensional reasons. In particular the k-algebra D is generated by α, β. Since β^2 commutes with α and β, it lies in center of D, so that $b = \beta^2 \in k^\times$. It follows from Lemma 1.1.2 (applied with $i = \alpha, j = \beta$) that $D \simeq (a, b)$. $\square$

LEMMA 1.2.5. *Let D be a central division k-algebra of dimension 4 and $d \in D - k$. Then the k-subalgebra of D generated by d is a quadratic field extension of k.*

PROOF. The powers d^i for $i \in \mathbb{N}$ are linearly dependent over k (as D is finite-dimensional), hence there is a nonzero polynomial $P \in k[X]$ such that $P(d) = 0$. Since D contains no nonzero zerodivisors (being division), we may assume that P is irreducible. Then $X \mapsto d$ defines a morphism of k-algebras $k[X]/P \to D$. Since $k[X]/P$ is a field, this morphism is injective. Its image L is a field, and coincides with the k-subalgebra of D generated by d. Now D is a vector space over L, and $\dim_L D \cdot \dim_k L = \dim_k D = 4$. We cannot have $\dim_k L = 4$, for $D = L$ would then be commutative, and so would not be central over k. The case $\dim_k L = 1$ is also excluded, since by assumption $d \notin k$. So we must have $\dim_k L = 2$. $\square$

COROLLARY 1.2.6. *Every central division k-algebra of dimension 4 is a quaternion algebra.*

PROOF. Since k has characteristic different from 2, every quadratic extension of k has the form $k(\sqrt{a})$ for some $a \in k^\times$. Thus D contains such an extension by Lemma 1.2.5, and the statement follows from Proposition 1.2.4. $\square$

If L/k is a field extension and Q is a quaternion k-algebra, then $Q_L = Q \otimes_k L$ is naturally a quaternion L-algebra. Note that for any $q \in Q$ and $\lambda \in L$ we have

$$\overline{q \otimes \lambda} = \overline{q} \otimes \lambda \quad ; \quad N(q \otimes \lambda) = N(q) \otimes \lambda^2. \tag{1.2.d}$$

DEFINITION 1.2.7. We will say that Q *splits over* L, or that L is a splitting field for Q, if the quaternion L-algebra Q_L is split.

EXAMPLE 1.2.8. Let Q be a quaternion k-algebra which splits over the purely transcendental extension $k(t)$. By Proposition 1.1.13, this means that $ax^2 + by^2 = z^2$ has a nontrivial solution in $k(t)$. Clearing denominators we may assume that $x, y, z \in k[t]$, and that one of x, y, z is not divisible by t. Then $x(0), y(0), z(0)$ is a nontrivial solution in k, hence Q splits. Therefore *every quaternion algebra splitting over $k(t)$ splits over k.*

PROPOSITION 1.2.9. *Let $a \in k^\times$ and Q be a quaternion algebra. Then the following are equivalent:*

(i) $Q \simeq (a, b)$ *for some* $b \in k^\times$.
(ii) Q *splits over* $k(\sqrt{a})$.
(iii) *The k-algebra Q contains a subalgebra isomorphic to $k(\sqrt{a})$.*

PROOF. (i) $\Rightarrow$ (ii) : Since a is a square in $k(\sqrt{a})$, we have $(a, b) \simeq (1, b)$ over $k(\sqrt{a})$, which splits by Lemma 1.1.4.

(ii) $\Rightarrow$ (iii) : If Q is split, then $Q \simeq (1, a) \simeq (a, 1)$ by Lemma 1.1.4, and (iii) was observed in Remark 1.2.3. Thus we assume that Q is division. Then there are $p, q \in Q$ not both zero such that $N(p \otimes 1 + q \otimes \sqrt{a}) = 0$ by Proposition 1.1.13. Set $r = p\overline{q} \in Q$. In view of (1.2.d), we have

$$0 = (p \otimes 1 + q \otimes \sqrt{a})(\overline{p} \otimes 1 + \overline{q} \otimes \sqrt{a}) = (N(p) + aN(q)) \otimes 1 + (r + \overline{r}) \otimes \sqrt{a}.$$

We deduce that $N(p) = -aN(q)$ and that r is a pure quaternion. Now

$$r^2 = -r\overline{r} = -p\overline{q}q\overline{p} = -N(p)N(q) = aN(q)^2.$$

Note that $N(q) \neq 0$, for otherwise $N(p) = -aN(q) = 0$, and thus $q = p = 0$ (by Lemma 1.1.9, as Q is division), contradicting the choice of p, q. The element $s = N(q)^{-1}r \in Q$ satisfies $s^2 = a$. Mapping X to s yields a morphism of k-algebras $k[X]/(X^2 - a) \to Q$, and (iii) follows.

(iii) $\Rightarrow$ (i) : If Q is not division, then $Q \simeq (1, a) \simeq (a, 1)$ by Lemma 1.1.4, so we may take $b = 1$ in this case. If Q is division, the implication has been proved in Proposition 1.2.4. □

3. Biquaternion algebras

Let Q, Q' be quaternion algebras. Denote by Q_0, Q'_0 the respective subspaces of pure quaternions.

Definition 1.3.1. The *Albert form* associated with the pair (Q, Q') is the quadratic form $Q_0 \oplus Q'_0 \to k$ defined by $q + q' \mapsto q'^2 - q^2$ for $q \in Q_0$ and $q' \in Q'_0$.

Theorem 1.3.2 (Albert). *Let Q, Q' be quaternion algebras. The following are equivalent:*

(i) The ring $Q \otimes_k Q'$ is not division.
(ii) There exist $a, b', b \in k^\times$ such that $Q \simeq (a, b)$ and $Q' \simeq (a, b')$.
(iii) The Albert form associated with (Q, Q') has a nontrivial zero.

Proof. (ii) $\Rightarrow$ (iii) : If $i \in Q_0$ and $i' \in Q'_0$ are such that $i^2 = a = i'^2$, then $i - i' \in Q_0 \oplus Q'_0$ is a nontrivial zero of the Albert form.

(iii) $\Rightarrow$ (i) : If $q \in Q_0$ and $q' \in Q'_0$ are such that $q^2 = q'^2 \in k$, we have

$$(q \otimes 1 - 1 \otimes q')(q \otimes 1 + 1 \otimes q') = 0.$$

As $Q_0 \cap k = 0$ in Q (see Lemma 1.1.7) we have $(Q_0 \otimes_k k) \cap (k \otimes_k Q'_0) = 0$ in $Q \otimes_k Q'$ (exercise), hence $q \otimes 1 \neq \pm 1 \otimes q'$. Thus the above relation shows that $q \otimes 1 - 1 \otimes q'$ is a nonzero noninvertible element of $Q \otimes_k Q'$.

(i) $\Rightarrow$ (ii) : We assume that (ii) does not hold, and show that $Q \otimes_k Q'$ is division. In view of Lemma 1.1.4 none of the algebras Q, Q' is isomorphic to $M_2(k)$, so Q and Q' are division by Proposition 1.1.13. We may assume that $Q' = (a, b)$ for some $a, b \in k^\times$, and consider the standard generators $i, j \in Q'$. The subalgebra L of Q generated by i is a field isomorphic to $k(\sqrt{a})$ (Remark 1.2.3). Since (ii) does not hold, Proposition 1.2.9 implies that the ring $Q \otimes_k L$ remains division.

In view of Remark 1.1.11, it will suffice to show that any nonzero $x \in Q \otimes_k Q'$ admits a left inverse. Since $1, j$ is an L-basis of Q', we may write $x = p_1 + p_2(1 \otimes j)$ where $p_1, p_2 \in Q \otimes_k L$. If $p_2 = 0$, then x belongs to the division algebra $Q \otimes_k L$, hence admits a left inverse. Thus we may assume that p_2 is nonzero, hence invertible in the division algebra $Q \otimes_k L$. Replacing x by $p_2^{-1}x$, we come to the situation where $p_2 = 1$. So we find $q_1, q_2 \in Q$ such that

$$x = q_1 \otimes 1 + q_2 \otimes i + 1 \otimes j.$$

Assume that $q_1q_2 = q_2q_1$. Let K be the k-subalgebra of Q generated by q_1, q_2. We claim that if $K \neq k$, then K is a quadratic field extension of k. Indeed, this is true by Lemma 1.2.5 if $q_1 \in k$. Otherwise the k-subalgebra K_1 of Q generated by q_1 is a quadratic field extension of k, by the same lemma. If $q_2 \notin K_1$, then $1, q_2$ is a K_1-basis of Q, so that

$K = Q$. This is not possible since q_1 and q_2 commute (as Q is central). Thus $q_2 \in K_1$, and $K = K_1$ is as required, proving the claim. Proposition 1.2.9 implies that Q splits over K, and since (ii) does not hold, by the same proposition $K \otimes_k Q'$ must remain division. Thus $x \in K \otimes_k Q'$ admits a left inverse.

So we may assume that $q_1q_2 \neq q_2q_1$. Let $y = q_1 \otimes 1 - q_2 \otimes i - 1 \otimes j$. Then

$$\begin{aligned} yx &= (q_1 \otimes 1 - q_2 \otimes i - 1 \otimes j)(q_1 \otimes 1 + q_2 \otimes i + 1 \otimes j) \\ &= (q_1 \otimes 1 - q_2 \otimes i)(q_1 \otimes 1 + q_2 \otimes i) - 1 \otimes j^2 \qquad \text{as } ji = -ij \\ &= q_1^2 \otimes 1 - aq_2^2 \otimes 1 + (q_1q_2 - q_2q_1) \otimes i - b \otimes 1. \end{aligned}$$

Thus yx belongs to the division subalgebra $Q \otimes_k L$. This element is also nonzero (since $q_1q_2 \neq q_2q_1$), hence admits a left inverse. Therefore x admits a left inverse. □

LEMMA 1.3.3. *For any $a, b, c \in k^\times$, we have*

$$(a, b) \otimes_k (a, c) \simeq (a, bc) \otimes_k M_2(k).$$

PROOF. Let i, j, resp. i', j', be the standard generators of (a, b), resp. (a, c). Consider the k-subspace A of $(a, b) \otimes_k (a, c)$ generated by

$$1 \otimes 1, \quad i \otimes 1, \quad j \otimes j', \quad ij \otimes j'.$$

Then A is stable under multiplication. So is the k-subspace A' generated by

$$1 \otimes 1, \quad 1 \otimes j', \quad i \otimes i', \quad i \otimes j'i'.$$

Moreover there are isomorphisms of k-algebras

$$A \simeq (a, bc) \quad ; \quad A' \simeq (c, a^2) \simeq (c, 1) \simeq M_2(k).$$

The image of the morphism of k-algebras $f \colon A \otimes_k A' \to (a, b) \otimes_k (a, c)$ given by $x \otimes y \mapsto xy$ visibly contains the elements

$$i \otimes 1, \quad 1 \otimes i', \quad j \otimes 1, \quad 1 \otimes j'.$$

Since these elements generate the k-algebra $(a, b) \otimes_k (a, c)$, we conclude that f is surjective, hence an isomorphism by dimensional reasons. □

REMARK 1.3.4. A tensor product of two quaternion algebras is called a *biquaternion algebra*. By Theorem 1.3.2 and Lemma 1.3.3, such an algebra is either division, or isomorphic to $M_2(D)$ for some division quaternion algebra D, or to $M_4(k)$.

PROPOSITION 1.3.5. *Let Q, Q' be quaternion algebras. Then*

$$Q \simeq Q' \iff Q \otimes_k Q' \simeq M_4(k).$$

PROOF. If $Q \simeq Q' \simeq (a, b)$ for some $a, b \in k^\times$, then $Q \otimes_k Q' \simeq (a, b^2) \otimes_k M_2(k)$ by Lemma 1.3.3, and $(a, b^2) \simeq (a, 1) \simeq M_2(k)$. Now $M_2(k) \otimes_k M_2(k) \simeq M_4(k)$ (exercise).

Assume now that $Q \otimes_k Q' \simeq M_4(k)$. Since $M_4(k)$ is not division, by Albert's Theorem 1.3.2, there are $a, b, c \in k^\times$ such that $Q \simeq (a, b)$ and $Q' \simeq (a, c)$. If (a, bc) splits, then Proposition 1.1.18 implies that $(a, b) \simeq (a, b^2c) \simeq (a, c)$, as required. So we assume that $D = (a, bc)$ is division, and come to a contradiction. We have $M_2(D) = D \otimes_k M_2(k) \simeq M_4(k)$ by Lemma 1.3.3. The element of $M_2(D)$ corresponding to the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in M_4(k)$$

is an endomorphism φ of the left D-module $D^{\oplus 2} = De_1 \oplus De_2$ such that $\varphi^3 \neq 0$ and $\varphi^4 = 0$. Since φ is not injective (as φ^4 is not injective), the kernel of φ contains an element $\lambda_1 e_1 + \lambda_2 e_2$, where $\lambda_1, \lambda_2 \in D$ are not both zero. Upon exchanging the roles of e_1 and e_2, we may assume that $\lambda_1 \neq 0$. Then $\varphi(e_1) = -\lambda_1^{-1}\lambda_2\varphi(e_2) \in D\varphi(e_2)$, hence letting $f = \varphi(e_2)$, we have $\varphi(D^{\oplus 2}) = Df$. Thus $\varphi(f) = \mu f$ for some $\mu \in D$, and

$$0 = \varphi^4(e_2) = \varphi^3(f) = \mu^3 f.$$

If $\mu \neq 0$, then $f = \mu^{-3}\mu^3 f = 0$, which implies that $\varphi = 0$, a contradiction. Thus $\mu = 0$, and $\varphi^2 = 0$, another contradiction. $\square$

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. Second edition of [MR2266528].

[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, english edition, 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`.