Brauer Groups of fields

Olivier Haution

Ludwig-Maximilians-Universität München

Winter semester 2020/2021

Contents

Note on the literature 2

Part 1. Noncommutative Algebra 3

Chapter 1. Quaternion algebras 5
1. The norm form 5
2. Quadratic splitting fields 9
3. Biquaternion algebras 11

Chapter 2. Central simple algebras 15
1. Wedderburn's Theorem 15
2. The commutant 18

Bibliography 21

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* $N\colon Q \to k$ 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 $\mathrm{N}_{A/k}\colon A \to k$ 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

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

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. □

PROPOSITION 1.1.20. *Let Q,Q' be quaternion algebras, with respective 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 $Q' \simeq (a,b)$. □

The norm map $N\colon Q \to k$ is in fact a quadratic form. The next corollary is a reformulation of Proposition 1.1.20, assuming some basic quadratic form theory. It can be safely ignored, and will not be used in the sequel.

COROLLARY 1.1.21. *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 $N|_k=\langle 1\rangle$. 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 1.1.20 is automatically an isometry. The corollary follows, by Witt's cancellation Theorem (see for instance [**Lam05**, Theorem 4.2]). □

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 nonzero k-algebra is called *central* if 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 (because its source is a field, and its target is nonzero).

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 2 over L, hence dimension 4 over k, and thus 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 and D is nonzero, 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

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

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 $k(t)$. Writing $Q \simeq (a,b)$ for some $a,b \in k^\times$, this means that $ax^2 + by^2 = z^2$ has a nontrivial solution in $k(t)$, by Proposition 1.1.13. 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. Assume that a is not a square in k. 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. Let $\alpha \in k(\sqrt{a})$ be such that $\alpha^2 = a$. Then there are $p,q \in Q$ not both zero such that $N(p \otimes 1 + q \otimes \alpha) = 0$ by Proposition 1.1.13. Set $r = p\overline{q} \in Q$. In view of (1.2.a), we have

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

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. $\square$

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 in $Q \otimes_k Q'$

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

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 $q \otimes 1 \neq 1 \otimes q'$ and $q \otimes 1 \neq -1 \otimes q'$. 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 denote by $i, j \in Q'$ the standard generators. Since Q' is division, the element a is not a square in k (by Lemma 1.1.4). 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, in $Q \otimes_k Q'$

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

Assume that $q_1 q_2 = q_2 q_1$. 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 $q_1 \in k$, so we will assume that $q_1 \notin k$. Then 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. If $K \neq k$, then Proposition 1.2.9 thus implies that Q splits over K, and since (ii) does not hold, by the same proposition $K \otimes_k Q'$ must remain division. This conclusion also holds if $K = k$. Thus in any case $x \in K \otimes_k Q'$ admits a left inverse.

So we may assume that $q_1 q_2 \neq q_2 q_1$. Let $y = q_1 \otimes 1 - q_2 \otimes i - 1 \otimes j \in Q \otimes_k Q'$. Then

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

Thus yx belongs to the division subalgebra $Q \otimes_k L$. This element is also nonzero (since $q_1 q_2 \neq q_2 q_1$), hence admits a left inverse. Therefore x admits a left inverse. $\square$

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

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

There are isomorphisms of k-algebras

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

Moreover every element of A commutes with every element of A'. Therefore the k-linear map $f\colon A \otimes_k A' \to (a, b) \otimes_k (a, c)$ given by $x \otimes y \mapsto xy = yx$ is a morphism of k-algebras; its image 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. □

Proposition 1.3.4. *Let Q, Q' be quaternion algebras. Then*

$$Q \simeq Q' \quad \Longleftrightarrow \quad Q \otimes_k Q' \simeq M_4(k).$$

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 1.1.19 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. By Lemma 1.3.3, we have

$$M_4(k) \simeq Q \otimes_k Q' \simeq (a, b) \otimes_k (a, c) \simeq (a, bc) \otimes_k M_2(k) \simeq M_2(D).$$

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 $\lambda_1 \neq 0$. Let $f = \varphi(e_2)$. Then $\varphi(e_1) = -\lambda_1^{-1}\lambda_2 f$, hence $\varphi(D^{\oplus 2}) = Df$. 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. □

Remark 1.3.5. A tensor product of two quaternion algebras is called a *biquaternion algebra*. It follows from Theorem 1.3.2 and Lemma 1.3.3 that such an algebra is either division, or isomorphic to $M_2(D)$ for some division quaternion algebra D, or to $M_4(k)$.

CHAPTER 2

Central simple algebras

In this chapter, we develop the general theory of finite-dimensional central simple algebras over a field. Wedderburn's Theorem asserts that such algebras are matrix algebras over (finite-dimensional central) division algebras. This theorem plays a key role in the theory, because it permits to reduce many proofs to the case of division algebras, where the situation is often more tractable.

After extending scalars appropriately, any finite-dimensional central simple algebras becomes a matrix algebra over a field. So such algebras may be thought of as twisted forms of matrix algebras, and as such share many of their properties. This point of view will be further explored in the next chapters.

Much information on the algebra is encoded in the data of which extensions of the base field transform it into a matrix algebras; such fields are called splitting fields. We prove the existence of a separable splitting field, a crucial technical result which will allow us to use Galois theory later on. The index of the algebra is an integer expressing how far is the algebra from being split. In this chapter we gather basic information concerning the behaviour of this invariant under field extensions.

We conclude with a definition of the Brauer group, which classifies finite-dimensional central simple algebras over a given base field.

1. Wedderburn's Theorem

A module (resp. ideal) will mean a left module (resp. ideal). When R is a ring, the ring of n by n matrices will be denoted by $M_n(R)$. If M, N are R-modules, we denote the set of morphisms of R-modules $M \to N$ by $\operatorname{Hom}_R(M, N)$. If M is an R-module, the set $\operatorname{End}_R(M) = \operatorname{Hom}_R(M, M)$ is naturally an R-algebra, and we will denote by $\operatorname{Aut}_R(M) = (\operatorname{End}_R(M))^\times$ the set of automorphisms of M.

The letter k will denote a field, which is now allowed to be of arbitrary characteristic.

Definition 2.1.1. Let R be a ring. An R-module is called *simple* if it has exactly two submodules: zero and itself.

Lemma 2.1.2 (Schur). *Let R be a ring and M a simple R-module. Then* $\operatorname{End}_R(M)$ *is a division ring.*

Proof. Let $\varphi \in \operatorname{End}_R(M)$ be nonzero. The kernel of φ is a submodule of M unequal to M. Since M is simple, this submodule must be zero. Similarly the image of φ is a nonzero submodule of M, hence must coincide with M. Thus φ is bijective, and it follows that φ is invertible in $\operatorname{End}_R(M)$. □

Definition 2.1.3. Let R be a ring. The *opposite ring* R^{op} is the ring equal to R as an abelian group, where multiplication is defined by mapping (x, y) to yx (instead of

xy for the multiplication in R). Note that if R is a k-algebra, then R^{op} is naturally a k-algebra.

Observe that:

(i) $R = (R^{\mathrm{op}})^{\mathrm{op}}$.
(ii) Every isomorphism $R \simeq S$ induces an isomorphism $R^{\mathrm{op}} \simeq S^{\mathrm{op}}$.
(iii) If R is simple, then so is R^{op}.
(iv) Transposing matrices induces an isomorphism $M_n(R)^{\mathrm{op}} \simeq M_n(R^{\mathrm{op}})$.

LEMMA 2.1.4. *Let R be a ring (resp. k-algebra) and $e \in R$ such that $e^2 = e$. Then $S = eRe$ is naturally a ring (resp. k-algebra), which is isomorphic to* $\mathrm{End}_R(Re)^{\mathrm{op}}$.

PROOF. Consider the ring morphism $\varphi\colon S \to \mathrm{End}_R(Re)^{\mathrm{op}}$ sending s to the morphism $x \mapsto xs$. Observe that $\varphi(s)(e) = s$ for any $s \in S$, hence φ is injective. If $f\colon Re \to Re$ is a morphism of R-modules, we may find $r \in R$ such that $f(e) = re$. Then for any $y \in Re$, we have $ye = y$, hence

$$f(y) = f(ye) = yf(e) = yre = yere = \varphi(ere)(y),$$

so that $f = \varphi(ere)$, proving that φ is surjective. □

DEFINITION 2.1.5. A ring is called *simple* if it has exactly two two-sided ideals: zero and itself.

REMARK 2.1.6. A division ring (Definition 1.1.10) is simple.

PROPOSITION 2.1.7. *Let R be a ring and $n \in \mathbb{N} - 0$. We view R as the subring of diagonal matrices in $M_n(R)$.*

(i) If the ring R is simple, then so is $M_n(R)$.
(ii) The rings R and $M_n(R)$ have the same center (Definition 1.2.1).
(iii) Assume that R is a division ring (resp. division k-algebra). Then $M_n(R)$ possesses a minimal nonzero ideal. If I is any such ideal, then $R \simeq \mathrm{End}_{M_n(R)}(I)^{\mathrm{op}}$.

PROOF. We will denote by $e_{i,j} \in M_n(R)$ the matrix having (i,j)-th coefficient equal to 1, and all other coefficients equal to zero. These elements commute with the subring $R \subset M_n(R)$, and generate $M_n(R)$ as an R-module. Taking the (i,j)-th coefficient yields a morphism of two-sided R-modules $\gamma_{i,j}\colon M_n(R) \to R$. For any $m \in M_n(R)$, we have

$$m = \sum_{i,j=1}^{n} \gamma_{i,j}(m) e_{i,j} = \sum_{i,j=1}^{n} e_{i,j}\gamma_{i,j}(m),$$

and

$$e_{k,i} m e_{j,l} = \gamma_{i,j}(m) e_{k,l} \quad \text{for all } i,j,k,l \in \{1,\ldots,n\}. \tag{2.1.a}$$

(i) : Let J be a two-sided ideal of $M_n(R)$. Then there is a couple (i,j) such that the two-sided ideal $\gamma_{i,j}(J)$ of R is nonzero, hence equal to R by simplicity of R. Thus there is $m \in J$ such that $\gamma_{i,j}(m) = 1$, and (2.1.a) implies that $e_{k,l} \in J$ for all k,l. We conclude that $J = M_n(R)$.

(ii) : Let $k,l \in \{1,\ldots,n\}$ and $m \in M_n(R)$. Then

$$e_{k,l} m = \sum_{i,j=1}^{n} \gamma_{i,j}(m) e_{k,l} e_{i,j} = \sum_{j=1}^{n} \gamma_{l,j}(m) e_{k,j},$$

$$me_{k,l} = \sum_{i,j=1}^{n} \gamma_{i,j}(m)e_{i,j}e_{k,l} = \sum_{i=1}^{n} \gamma_{i,k}(m)e_{i,l}.$$

Assume that m commutes with $e_{k,l}$. Then $\gamma_{k,k}(m) = \gamma_{l,l}(m)$, and $\gamma_{i,k}(m) = 0$ for $i \neq k$. It follows that the center of $M_n(R)$ is contained in R, hence in the center of R. Conversely, any element of the center of R certainly commutes with every matrix.

(iii) : Let us write $B = M_n(R)$. For $r = 1, \dots, n$, consider the ideal $I_r = Be_{r,r}$ of B. Let m be a nonzero element of I_r. There is a couple (k, i) such that $e_{k,i}m \neq 0$. As $(e_{r,r})^2 = e_{r,r}$, we have $m = me_{r,r}$. It follows from (2.1.a) that $\gamma_{i,r}(m)e_{k,r} = e_{k,i}m$. In particular $\gamma_{i,r}(m) \neq 0$, and

$$e_{r,r} = e_{r,k}e_{k,r} = e_{r,k}\gamma_{k,r}(m)^{-1}e_{k,i}m \in Bm,$$

and therefore $I_r \subset Bm$. We have proved that I_r is a simple B-module, or equivalently a minimal nonzero ideal of B. If I is any other such ideal, then there is a surjective morphism of B-modules $B \to I$ (as I must be generated by a single element). Since the natural morphism $I_1 \oplus \cdots \oplus I_n \to B$ is surjective (as $e_{i,j} = e_{i,j}e_{j,j} \in I_j$ for all i, j), the composite $I_r \to I$ must be nonzero for some r, hence an isomorphism as both I_r and I are simple (see the proof of Lemma 2.1.2). Now the map $R \to e_{r,r}Be_{r,r}$ given by $x \mapsto xe_{r,r}$ is a ring (resp. k-algebra) isomorphism (with inverse $\gamma_{r,r}$). Thus it follows from Lemma 2.1.4 that $R \simeq \operatorname{End}_B(I_r)^{\mathrm{op}} \simeq \operatorname{End}_B(I)^{\mathrm{op}}$. □

COROLLARY 2.1.8. *If D, E are division rings (resp. division k-algebras) such that $M_n(D) \simeq M_m(E)$ for some nonzero integers m, n, then $D \simeq E$.*

PROOF. By Proposition 2.1.7 (iii), here is a minimal nonzero ideal I of $M_n(D)$. The corresponding ideal J of $M_m(E)$ is also a minimal nonzero ideal, hence by Proposition 2.1.7 (iii) again

$$D \simeq \operatorname{End}_{M_n(D)}(I)^{\mathrm{op}} \simeq \operatorname{End}_{M_m(E)}(J)^{\mathrm{op}} \simeq E. \qquad \square$$

DEFINITION 2.1.9. A ring R is called *artinian* if every descending chain of ideals stabilises. This means that if I_n for $n \in \mathbb{N}$ are ideals of R such that $I_{n+1} \subset I_n$ for all n, then there exist $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.

EXAMPLE 2.1.10. Every finite-dimensional k-algebra is an artinian ring.

PROPOSITION 2.1.11. *Let A be an artinian simple ring.*

(i) There is a unique simple A-module, up to isomorphism.
(ii) Every finitely generated A-module is a finite direct sum of simple A-modules.

PROOF. Since A is artinian, it admits a minimal nonzero ideal S. Then S is a simple A-module. Moreover the two-sided ideal SA generated by S in A is nonzero, hence $SA = A$ by simplicity of A. In particular there are elements $a_1, \dots, a_p \in A$ such that $1 \in Sa_1 + \cdots + Sa_p$. We have thus a surjective morphism of A-modules $S^{\oplus p} \to A$ given by $(s_1, \dots, s_p) \mapsto s_1a_1 + \cdots + s_pa_p$.

Let now M be a finitely generated A-module. Then M is a quotient of $A^{\oplus q}$ for some integer q, hence a quotient of $S^{\oplus n}$ for some integer n (namely $n = pq$). Choose n minimal with this property, and denote by N the kernel of the surjective morphism $S^{\oplus n} \to M$. For $i = 1, \dots, n$, denote by $\pi_i \colon S^{\oplus n} \to S$ the projection onto the i-th factor. If $N \neq 0$, there is i such that $\pi_i(N) \neq 0$. Since S is simple, this implies that $\pi_i(N) = S$. Let now $m \in M$, and $s \in S^{\oplus n}$ a preimage of m. Then there is $z \in N$ such that $\pi_i(z) = \pi_i(s)$.

The element $s - z$ is mapped to m in M, and belongs to $\ker \pi_i \simeq S^{\oplus n-1}$. This yields a surjective morphism $S^{\oplus n-1} \to M$, contradicting the minimality of n. So we must have $N = 0$, and $S^{\oplus n} \simeq M$. This proves the second statement.

If M is simple, we must have $n = 1$. Now a simple module is necessarily finitely generated, so (i) follows. □

THEOREM 2.1.12 (Wedderburn). *Let A be an artinian simple ring (resp. a finite-dimensional simple k-algebra). Then A is isomorphic to $M_n(D)$ for some integer n and division ring (resp. finite-dimensional division k-algebra) D. Such a ring (resp. k-algebra) D is unique up to isomorphism, and the centers of A and D are isomorphic.*

PROOF. Recall that in any case A is artinian (Example 2.1.10). Let S be a simple A-module, which exists by Proposition 2.1.11. Then the ring $E = \mathrm{End}_A(S)$ is division by Schur's Lemma 2.1.2. By Proposition 2.1.11 there is an integer n such that $A \simeq S^{\oplus n}$ as A-modules. In view of Lemma 2.1.4 (with $R = A$ and $e = 1$), we have

$$A = \mathrm{End}_A(A)^{\mathrm{op}} \simeq \mathrm{End}_A(S^{\oplus n})^{\mathrm{op}} = M_n(\mathrm{End}_A(S))^{\mathrm{op}} = M_n(E)^{\mathrm{op}} = M_n(E^{\mathrm{op}}).$$

Thus we may take $D = E^{\mathrm{op}}$. Unicity was proved in Corollary 2.1.8, and the last statement follows from Proposition 2.1.7 (ii). □

2. The commutant

If A, B are k-algebras, their tensor product $A \otimes_k B$ is naturally a k-algebra. We will use without explicit mention the isomorphism

$$A \otimes_k B \simeq B \otimes_k A \quad ; \quad a \otimes b \mapsto b \otimes a. \tag{2.2.a}$$

DEFINITION 2.2.1. Let R be a ring and $E \subset R$ a subset. The set

$$\mathcal{Z}_R(E) = \{r \in R | er = re \text{ for all } e \in E\}$$

is a subring of R, called the *commutant* of E in R. We say that an element of R *commutes with* E if it belongs to $\mathcal{Z}_R(E)$. Recall from Definition 1.2.1 that $\mathcal{Z}(R) = \mathcal{Z}_R(R)$ is called the center of R, and that a nonzero k-algebra A is called central if $\mathcal{Z}(A) = k$.

LEMMA 2.2.2. *The center of a simple ring is a field.*

PROOF. Let R be a simple ring, and x a nonzero element of $\mathcal{Z}(R)$. Then Rx is a nonzero two-sided ideal of R (it coincides with xR), hence $Rx = R$. Thus we find $y \in R$ such that $yx = 1$. Since $X \in \mathcal{Z}(R)$, we also have $xy = 1$. For any $r \in R$, we have

$$yr = yr(xy) = y(rx)y = y(xr)y = (yx)ry = ry,$$

proving that $y \in \mathcal{Z}(R)$. □

LEMMA 2.2.3. *Let A, B be k-algebras. If $A' \subset A$ is a subalgebra and $B \neq 0$, then*

$$\mathcal{Z}_{A \otimes_k B}(A' \otimes_k k) = \mathcal{Z}_A(A') \otimes_k B.$$

PROOF. Let $C = \mathcal{Z}_{A \otimes_k B}(A' \otimes_k k)$. Certainly $\mathcal{Z}_A(A') \otimes_k B \subset C$. Any element $c \in C$ may be written as $c = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ for some $n \in \mathbb{N}$, with $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$. We may additionally assume that $b_1, \ldots, b_n$ are linearly independent over k. Let $a' \in A'$. Then c commutes with $a' \otimes 1$, hence we have in $A \otimes_k B$

$$0 = c(a' \otimes 1) - (a' \otimes 1)c = (a_1 a' - a' a_1) \otimes b_1 + \cdots + (a_n a' - a' a_n) \otimes b_n.$$

The linear independence of $b_1, \dots, b_n$ implies that the k-subspaces $A \otimes_k b_1 k, \dots, A \otimes_k b_n k$ are in direct sum in $A \otimes_k B$ (exercise), and we conclude that each a_i commutes with a'. We have proved that $C \subset \mathcal{Z}_A(A') \otimes_k B$. $\square$

Proposition 2.2.4. *Let A, B be k-algebras. Let $A' \subset A$ and $B' \subset B$ be subalgebras. Then*

$$\mathcal{Z}_{A \otimes_k B}(A' \otimes_k B') = \mathcal{Z}_A(A') \otimes_k \mathcal{Z}_B(B').$$

Proof. We may assume that A and B are nonzero. Let $C = \mathcal{Z}_{A \otimes_k B}(A' \otimes_k B')$. Then C contains $\mathcal{Z}_A(A') \otimes_k \mathcal{Z}_B(B')$. Conversely by Lemma 2.2.3 (and (2.2.a)), the subalgebra $C \subset A \otimes_k B$ is contained in

$$\mathcal{Z}_{A \otimes_k B}(A' \otimes_k k) \cap \mathcal{Z}_{A \otimes_k B}(k \otimes_k B') = (\mathcal{Z}_A(A') \otimes_k B) \cap (A \otimes_k \mathcal{Z}_B(B')),$$

which coincides with $\mathcal{Z}_A(A') \otimes_k \mathcal{Z}_B(B')$ (exercise). $\square$

Proposition 2.2.5. *Let A, B be k-algebras. If the ring $A \otimes_k B$ is simple, then so are A and B.*

Proof. Let $I \subsetneq A$ be a two-sided ideal. Then the k-algebra $C = A/I$ is nonzero. Consider the commutative diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "a \mapsto a \otimes 1"'] & C \arrow[d, "c \mapsto c \otimes 1"] \\ A \otimes_k B \arrow[r, "f \otimes \mathrm{id}_B"] & C \otimes_k B \end{tikzcd}$$

Since $A \otimes_k B \neq 0$ (being simple), we have $B \neq 0$. As $C \neq 0$, we must have $C \otimes_k B \neq 0$ (exercise). By simplicity of $A \otimes_k B$, the ring morphism $f \otimes \mathrm{id}_B$ is injective. Since the left vertical morphism in the above diagram is also injective (exercise), it follows that f is injective, or equivalently that $I = 0$. This proves that A is simple (and so is B by symmetry). $\square$

Proposition 2.2.6. *Let A be a central simple k-algebra and B a simple k-algebra. Then the k-algebra $A \otimes_k B$ is simple.*

Proof. Let $I \subset A \otimes_k B$ be a two-sided ideal. Let $i = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ be a nonzero element of I, where $n \in \mathbb{N} - 0$, with $a_1, \dots, a_n \in A$ and $b_1, \dots, b_n \in B$. We assume that n is minimal, in the sense that if $a'_1 \otimes b'_1 + \cdots + a'_m \otimes b'_m$ is a nonzero element of I, then $m \geq n$. Consider the following subset of A:

$$H = \{\alpha_1 \in A | \alpha_1 \otimes b_1 + \cdots + \alpha_n \otimes b_n \in I \text{ for some } \alpha_2, \dots, \alpha_n \in B\}.$$

The set H is a two-sided ideal of A, and it is nonzero since it contains $a_1 \neq 0$. By simplicity of A, it follows that $H = A$, and in particular $1 \in H$. We may thus assume that $a_1 = 1$. Then for any $a \in A$, we have

$$(a \otimes 1)i - i(a \otimes 1) = (aa_2 - a_2 a) \otimes b_2 + \cdots + (aa_n - a_n a) \otimes b_n \in I.$$

By minimality of n, we must have $(a \otimes 1)i = i(a \otimes 1)$. Thus, by Lemma 2.2.3 and the fact the A is central

$$i \in \mathcal{Z}_{A \otimes_k B}(A \otimes_k k) = \mathcal{Z}_A(A) \otimes_k B = k \otimes_k B.$$

Therefore i is of the form $1 \otimes b$ for some $b \in B$. The subset $J = \{b \in B | 1 \otimes b \in I\}$ is a two-sided ideal of B. It is nonzero (as it contains i), hence coincides with B by simplicity of B. Thus J contains $1 \in B$, which implies that I contains $1 \in A \otimes_k B$, hence $I = A \otimes_k B$. We have proved that the ring $A \otimes_k B$ is simple. $\square$

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.

[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`.