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. □

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

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 $N(q) \neq 0$. □

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 $Q' \simeq (a,b)$. □

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]). □

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 $y = w = 0$. □

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

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

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 $k(t)$. 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.a), 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 $q_1 q_2 = q_2 q_1$. 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 $q_1 \in k$. 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 $q_1 q_2 \neq q_2 q_1$. Let $y = q_1 \otimes 1 - q_2 \otimes i - 1 \otimes j$. Then

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

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

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

Moreover every element of A commutes with every element of A'. Now, 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 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. $\square$

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 $(a, b) \simeq (a, b^2 c) \simeq (a, c)$, 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. $\square$

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 $\mathrm{Hom}_R(M, N)$. If M is an R-module, the set $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is naturally an R-algebra, and we will denote by $\mathrm{Aut}_R(M) = (\mathrm{End}_R(M))^\times$ 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* $\mathrm{End}_R(M)$ *is a division ring.*

Proof. Let $\varphi \in \mathrm{End}_R(M)$ 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 $\mathrm{End}_R(M)$. $\square$

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) We have $M_n(R)^{\mathrm{op}} = M_n(R^{\mathrm{op}})$.

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 $n \in \mathbb{N} - 0$.*

(i) If the ring R is simple, then so is $M_n(R)$.
(ii) 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 subalgebra $R \subset M_n(R)$, 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 $m = \sum_{i,j} \varphi_{i,j}(m) e_{i,j}$, and

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

(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 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 (ii), there is a minimal nonzero ideal I of $M_n(D)$. The corresponding ideal J of $M_m(E)$ is also minimal nonzero, hence by Proposition 2.1.7 (ii)

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

Definition 2.1.9. A ring is called *artinian* if every descending chain of ideals stabilises.

Example 2.1.10. Every finite-dimensional k-algebra is artinian.

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 $1 \in Sa_1 + \dots + Sa_p$. We have thus a surjective morphism of A-modules $S^{\oplus p} \to A$ given by $(s_1, \dots, s_p) \mapsto s_1a_1 + \dots + s_pa_p$.

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.*

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 $E = \operatorname{End}_A(S)$ is division by Schur's Lemma 2.1.2. By Proposition 2.1.11 there is an integer n such that $A^{\mathrm{op}} \simeq S^{\oplus n}$ as A-modules. In view of Lemma 2.1.4 (with $R = A$ and $e = 1$), we have

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

So we may take $D = E^{\mathrm{op}}$. Unicity was proved in Corollary 2.1.8. □

2. The commutant

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. 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 $\mathcal{Z}(A) = k$.

Remark 2.2.2. If the k-algebra A in Wedderburn's Theorem 2.1.12 is central, then so is D (indeed, every element of $\mathcal{Z}(D)$ certainly commutes with every matrix in $M_n(D)$).

Lemma 2.2.3. *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 the two-sided ideal RxR of R is nonzero, hence $RxR = R$. Thus we may write $1 = a_1xa_1' + \cdots + a_nxa_n'$ with $a_1, \ldots, a_n, a_1', \ldots, a_n' \in R$. Then the element $y = a_1a_1' + \cdots + a_na_n'$ is a two-sided inverse of x in R. 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 2.2.4. *Let A, B be k-algebras, and $A' \subset A$ a subalgebra. 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 $c = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ 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 $A \otimes_k B$

$$0 = c(a' \otimes 1) - (a' \otimes 1)c = (a_1a' - a'a_1) \otimes b_1 + \cdots + (a_na' - a'a_n) \otimes b_n.$$

The linear independence of $b_1, \ldots, b_n$ implies that the k-subspaces $A \otimes_k b_1k, \ldots, A \otimes_k b_nk$ are in direct sum in $A \otimes_k B$ (exercise), and we conclude that each a_i commutes with a', proving the other inclusion. □

Proposition 2.2.5. *Let A, B be k-algebras, and $A' \subset A, B' \subset B$ subalgebras. Then*

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

Proof. 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 2.2.4, 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). □

Proposition 2.2.6. *Let A, B be k-algebras. If the ring $A \otimes_k B$ is simple, then so are A and B.*

Proof. Let I be a two-sided ideal of A such that $I \neq A$. 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 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). □

Proposition 2.2.7. *Let A be a simple k-algebra and B a central simple k-algebra. Then the k-algebra $A \otimes_k B$ is simple.*

Proof. Let $I \subsetneq A \otimes_k B$ 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 $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$. 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 B:

$$H = \{\beta_1 \in B | a_1 \otimes \beta_1 + \cdots + a_n \otimes \beta_n \in I \text{ for some } \beta_2, \ldots, \beta_n \in B\}.$$

The set H is a two-sided ideal of B, and it is nonzero since it contains $b_1 \neq 0$. By simplicity of B, it follows that $H = B$, hence H contains 1. We may thus assume that $b_1 = 1$. Then for any $b \in B$, we have

$$(1 \otimes b)i - i(1 \otimes b) = a_2 \otimes (bb_2 - b_2 b) + \cdots + a_n \otimes (bb_n - b_n b) \in I.$$

By minimality of n, we must have $(1 \otimes b)i = i(1 \otimes b)$. Thus, by Proposition 2.2.5

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

Therefore i is of the form $a \otimes 1$ for some $a \in A$. The subset $\{a \in A | a \otimes 1 \in I\} \subset A$ is a two-sided ideal of A. It is distinct from A (for otherwise $1 \in I$), hence is zero by simplicity of A. Thus $i = 0$, a contradiction. □

Corollary 2.2.8. *Let A, B be k-algebras. Then the k-algebra $A \otimes_k B$ is central simple if and only if A and B are central simple.*

Proof. Combine Proposition 2.2.7, Proposition 2.2.5 and Proposition 2.2.6. □

Proposition 2.2.9. *Let A be a finite-dimensional central simple k-algebra. Then the morphism $\varphi \colon A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ mapping $a \otimes b$ to $x \mapsto axb$ is an isomorphism.*

Proof. This morphism is visibly nonzero. Its kernel is a two-sided ideal in the ring $A \otimes_k A^{\mathrm{op}}$, which is simple by Proposition 2.2.7. Thus φ is injective, and bijective for dimensional reasons. □

Lemma 2.2.10. *Let A be a finite-dimensional central simple k-algebra and $B \subset A$ a subalgebra. Then there is a natural isomorphism*

$$\mathcal{Z}_A(B) \otimes_k A^{\mathrm{op}} \simeq \mathrm{End}_B(A).$$

Proof. Consider the isomorphism $\varphi \colon A \otimes_k A^{\mathrm{op}} \simeq \mathrm{End}_k(A)$ of Proposition 2.2.9, and let $C = \varphi(B \otimes_k k)$. A morphism $f \in \mathrm{End}_k(A)$ commutes with C if and only if it is B-linear (for the left action on A). Thus

$$\mathcal{Z}_{A \otimes_k A^{\mathrm{op}}}(B \otimes_k k) \simeq \mathcal{Z}_{\mathrm{End}_k(A)}(C) = \mathrm{End}_B(A).$$

To conclude, note that $\mathcal{Z}_{A \otimes_k A^{\mathrm{op}}}(B \otimes_k k) = \mathcal{Z}_A(B) \otimes_k A^{\mathrm{op}}$ by Lemma 2.2.4. □

Proposition 2.2.11. *Let A be a finite-dimensional central simple k-algebra and B a simple subalgebra of A.*

(i) *The ring $\mathcal{Z}_A(B)$ is simple.*
(ii) *There exists a division k-algebra D, and integers n, r such that*

$$\mathcal{Z}_A(B) \otimes_k A^{\mathrm{op}} \simeq M_n(D^{\mathrm{op}}) \quad ; \quad B \simeq M_r(D).$$

(iii) $(\dim_k B)(\dim_k \mathcal{Z}_A(B)) = \dim_k A$.
(iv) $\mathcal{Z}_A(\mathcal{Z}_A(B)) = B$.
(v) *The centers of B and $\mathcal{Z}_A(B)$ coincide, as subsets of A.*

Proof. Let $C = \mathcal{Z}_A(B)$.

(ii): By Proposition 2.1.11, there exist a simple B-module S, and integers r, n such that $B \simeq S^{\oplus r}$ and $A \simeq S^{\oplus n}$ as B-modules. The k-algebra $D = \mathrm{End}_B(S)^{\mathrm{op}}$ is division by Schur's Lemma 2.1.2. We have, by Lemma 2.2.10

$$C \otimes_k A^{\mathrm{op}} \simeq \mathrm{End}_B(A) \simeq \mathrm{End}_B(S^{\oplus n}) = M_n(\mathrm{End}_B(S)) = M_n(D^{\mathrm{op}}).$$

Now, by Lemma 2.1.4 (with $R = B$ and $e = 1$)

$$B = \mathrm{End}_B(B)^{\mathrm{op}} \simeq \mathrm{End}_B(S^{\oplus r})^{\mathrm{op}} = M_r(\mathrm{End}_B(S))^{\mathrm{op}} = M_r(\mathrm{End}_B(S)^{\mathrm{op}}) = M_r(D).$$

(i): Since $M_n(D^{\mathrm{op}})$ is simple by Remark 2.1.6 and Proposition 2.1.7 (i), it follows from Proposition 2.2.6 that $\mathcal{Z}_A(B)$ is simple.

(iii): Let $a = \dim_k A, b = \dim_k B, c = \dim_k C, d = \dim_k D, s = \dim_k S$. Taking the dimensions in (i) yields $ac = n^2 d$ and $b = r^2 d$. Since $B \simeq S^{\oplus r}$ and $A \simeq S^{\oplus n}$, we have $b = rs$ and $a = ns$, and therefore $ar = bn$. Thus

$$a^2 b = a^2 r^2 d = b^2 n^2 d = b^2 ac,$$

hence $a = bc$.

(iv): Clearly $B \subset \mathcal{Z}_A(C)$. The equality follows by dimensional reasons. Indeed, let $z = \dim_k \mathcal{Z}_A(B)$ and $z' = \dim_k \mathcal{Z}_A(\mathcal{Z}_A(B)), a = \dim_k A, b = \dim_k B$. Then by(i) and (iii), we have $bz = a = zz'$, so that $b = z'$.

(v): Let R be a subring of A, and $S = \mathcal{Z}_A(R)$. Then $R \subset \mathcal{Z}_A(S)$, hence

$$\mathcal{Z}(R) = R \cap \mathcal{Z}_A(R) = R \cap S \subset \mathcal{Z}_A(S) \cap S = \mathcal{Z}(S). \tag{2.2.a}$$

Taking $R = B$ in (2.2.a) yields $\mathcal{Z}(B) \subset \mathcal{Z}(C)$. Since $B = \mathcal{Z}_A(C)$ by (iv), taking $R = C$ in (2.2.a) yields $\mathcal{Z}(C) \subset \mathcal{Z}(B)$. □

3. Skolem–Noether's Theorem

Lemma 2.3.1. *Let A be a simple k-algebra. Then two A-modules of finite dimension over k are isomorphic if and only if they have the same dimension over k.*

Proof. This follows from Proposition 2.1.11. Indeed let S be a simple A-module. Then every A-module M of finite dimension over k (which is necessarily finitely generated) is isomorphic to $S^{\oplus n}$ for some integer n, which is determined by $\dim_k M$. □

Theorem 2.3.2 (Skolem–Noether). *Let B be a simple k-algebra and A a finite-dimensional central simple k-algebra. If $f, g \colon B \to A$ are morphisms of k-algebras, there is an element $u \in A^\times$ such that $f(b) = u^{-1} g(b) u$ for all $b \in B$.*

Proof. Let $h \colon B \to A$ be a morphism of k-algebras. Consider the k-algebra $C = B \otimes_k A^{\mathrm{op}}$. It is simple by Proposition 2.2.7. We define a C-module A_h, by setting $A_h = A$ as a k-vector space, with the C-module structure given by letting $b \otimes_k a \in C$ act on A_h by

$x \mapsto h(b)xa$. As $\dim_k A_f = \dim_k A = \dim_k A_g$, by Lemma 2.3.1 there is an isomorphism of C-modules $\varphi\colon A_f \to A_g$. Set $u = \varphi(1) \in A$. For any $b \in B$, we have

$$\varphi(f(b)) = \varphi((b \otimes 1)1) = (b \otimes 1)\varphi(1) = g(b)u,$$

$$\varphi(f(b)) = \varphi((1 \otimes f(b))1) = (1 \otimes f(b))\varphi(1) = uf(b).$$

To conclude, we prove that $v = \varphi^{-1}(1) \in A$ is a two-sided inverse of u. We have

$$\varphi(uv) = \varphi((1 \otimes u)v) = (1 \otimes u)\varphi(v) = u = \varphi(1),$$

so that $uv = 1$, since φ is injective. We conclude using Remark 1.1.11, or alternatively computing

$$vu = (1 \otimes v)\varphi(1) = \varphi((1 \otimes v)1) = \varphi(v) = 1. \qquad \square$$

COROLLARY 2.3.3. *Every automorphism of a finite-dimensional central simple k-algebra A is inner, i.e. of the form $x \mapsto a^{-1}xa$ for some $a \in A^\times$.*

4. The index

When L/k is a field extension and A a k-algebra, we will denote by A_L the L-algebra $A \otimes_k L$.

LEMMA 2.4.1. *Let A be a k-algebra and L/k a field extension. Then A is a finite-dimensional central simple k-algebra if and only if A_L is a finite-dimensional central simple L-algebra.*

PROOF. Since $\dim_k A = \dim_L A_L$ and $\mathcal{Z}(A_L) = \mathcal{Z}(A) \otimes_k L$ by Proposition 2.2.5, the k-algebra A is finite-dimensional (resp. central) if and only if the L-algebra A_L is so. Observe that the ring L is simple (Remark 2.1.6). Thus the equivalence follows from Proposition 2.2.6 and Proposition 2.2.7. $\square$

LEMMA 2.4.2. *Every subalgebra of a finite-dimensional division k-algebra is division.*

PROOF. Let D be a finite-dimensional division k-algebra, and B a subalgebra. Let b be a nonzero element of B. The k-linear map $B \to B$ given by left multiplication by b is injective, because if $x \in B$ is such that $bx = 0$, then $0 = b^{-1}bx = x$ in A, hence $x = 0$ in B. By dimensional reasons, this map is surjective. Thus the element $1 \in B$ lies in its image, so there is $b' \in B$ such that $bb' = 1$. Multiplying by b^{-1} on the left, we deduce that $b^{-1} = b' \in B$. $\square$

PROPOSITION 2.4.3. *If k is algebraically closed, the only finite-dimensional division k-algebra is k.*

PROOF. Let D be a finite-dimensional division k-algebra. Pick an element $x \in D$. The k-subalgebra of D generated by x is commutative, hence a field by Lemma 2.4.2. It has finite degree over k, and is thus an algebraic extension of k. By assumption it must equal k, hence $x \in k$, and finally $D = k$. $\square$

COROLLARY 2.4.4. *If k is algebraically closed, then every finite-dimensional simple k-algebra is isomorphic to $M_n(k)$ for some integer n.*

PROOF. This follows from Wedderburn's Theorem 2.1.12 and Proposition 2.4.3. $\square$

COROLLARY 2.4.5. *If A is a finite-dimensional central simple k-algebra, the integer $\dim_k A$ is a square.*

PROOF. Let $\overline{k}$ be an algebraic closure of k. The $\overline{k}$-algebra $A_{\overline{k}}$ is finite-dimensional simple by Lemma 2.4.1, hence isomorphic to $M_n(\overline{k})$ for some integer n by Corollary 2.4.4. Then $\dim_k A = \dim_{\overline{k}} A_{\overline{k}} = n^2$. □

DEFINITION 2.4.6. When A is a finite-dimensional central simple k-algebra, the integer $d \in \mathbb{N}$ such that $d^2 = \dim_k A$ is called the *degree* of A and denoted $\deg(A)$. By Wedderburn's Theorem 2.1.12 (and Remark 2.2.2) there is a finite-dimensional central division k-algebra D such that $A \simeq M_n(D)$ for some integer n, and D is unique up to isomorphism. The *index* of A, denoted $\operatorname{ind}(A)$, is defined as the degree of D.

Observe that $\operatorname{ind}(A)$ divides $\deg(A)$, and that if $A \simeq M_r(B)$ for some integer $r \geq 1$ and finite-dimensional central simple k-algebra B, then $\operatorname{ind}(A) = \operatorname{ind}(B)$ (recall that $M_r(M_n(D)) \simeq M_{rn}(D)$).

LEMMA 2.4.7. *Let A be a finite-dimensional central simple k-algebra, and L/k a field extension. Then*

$$\operatorname{ind}(A_L) \mid \operatorname{ind}(A).$$

PROOF. Let D be a central division k-algebra such that $A \simeq M_n(D)$ for some integer n. Then $A_L \simeq M_n(D_L)$, hence

$$\operatorname{ind}(A_L) = \operatorname{ind}(D_L) \mid \deg(D_L) = \deg(D) = \operatorname{ind}(A).$$ □

5. Splitting fields

DEFINITION 2.5.1. A finite-dimensional central simple k-algebra is called *split* if it is isomorphic to the matrix algebra $M_n(k)$ for some integer n. A field extension L/k is called a *splitting field* of A if the L-algebra $A_L = A \otimes_k L$ is split.

PROPOSITION 2.5.2. *Let A be a finite-dimensional central simple k-algebra, and L/k be a field extension of finite degree splitting A. Then*

$$\operatorname{ind}(A) \mid [L:k].$$

PROOF. Let $d = \operatorname{ind}(A)$ and $n = [L:k]$. Let D be a central division k-algebra such that $A \simeq M_t(D)$ for some integer t. We view L as a k-subalgebra of $\operatorname{End}_k(L) \simeq M_n(k)$ by mapping $\lambda \in L$ the endomorphism $x \mapsto \lambda x$ of L. Then we have inclusions

$$M_d(k) \subset M_d(L) \simeq D \otimes_k L \subset D \otimes_k M_n(k) = M_n(D).$$

Thus we may view $M_d(k)$ as a subalgebra of $M_n(D)$. It is a simple subalgebra by Proposition 2.1.7 (i), hence so is $B = \mathcal{Z}_{M_n(D)}(M_d(k))$ by Proposition 2.2.11 (i). Then $\mathcal{Z}_{M_n(D)}(B) = M_d(k)$ by Proposition 2.2.11 (iv). By Proposition 2.2.11 (ii) there exists a division k-algebra E and integers r, s such that $B \simeq M_r(E)$ and $M_d(k) \otimes_k M_n(D)^{\mathrm{op}} \simeq M_s(E^{\mathrm{op}})$. Then $M_{dn}(D) \simeq M_s(E)$, so that $E \simeq D$ by Corollary 2.1.8. It follows that $B \simeq M_r(D)$. Setting $b = \dim_k B$, we have thus $b = r^2 d^2$. By Proposition 2.2.11 (iii) we have $bd^2 = n^2 d^2$. Thus $n^2 = r^2 d^2$, and $d \mid n$. □

PROPOSITION 2.5.3. *Let D be a finite-dimensional central division k-algebra, and $L \subset D$ a commutative subalgebra. Then L is a field, and the following are equivalent:*

(i) $L = \mathcal{Z}_D(L)$
(ii) *L is maximal among the commutative k-subalgebras of D.*
(iii) $[L:k] = \operatorname{ind}(D)$.
(iv) *L splits D.*

Proof. The first assertion follows from Lemma 2.4.2. Since L is commutative, we have $L \subset \mathcal{Z}_D(L)$. The ring L being simple (Remark 2.1.6), by Proposition 2.2.11 (iii) we have

$$\operatorname{ind}(D)^2 = [L:k] \cdot \dim_k \mathcal{Z}_D(L) = [L:k]^2 \cdot \dim_L \mathcal{Z}_D(L).$$

It follows that $[L:k] \mid \operatorname{ind}(D)$, with equality if and only if $L = \mathcal{Z}_D(L)$. This implies the equivalence of (i) and (iii).

(iv) $\Longrightarrow$ (iii) : This follows from Proposition 2.5.2 (as observed above $[L:k]$ always divides $\operatorname{ind}(D)$).

(i) $\Longrightarrow$ (ii) : Any commutative k-subalgebra of D containing L must be contained in $\mathcal{Z}_D(L)$.

(ii) $\Longrightarrow$ (i) : Let $x \in \mathcal{Z}_D(L)$. The k-subalgebra of D generated by L and x is commutative, hence equals L. Thus $x \in L$.

(i) $\Longrightarrow$ (iv) : If $L = \mathcal{Z}_D(L)$, then $(D^{\mathrm{op}})_L \simeq \operatorname{End}_L(D)$ by Lemma 2.2.10. Thus L splits D^{op}, hence also D. □

Definition 2.5.4. A subalgebra L satisfying the equivalent conditions of Proposition 2.5.3 is called a *maximal subfield*.

In view of the characterisation (ii) in Proposition 2.5.3, maximal subfields always exist in finite-dimensional central division k-algebras (by dimensional reasons).

Corollary 2.5.5. *Let A be a finite-dimensional central simple k-algebra. Then A is split by a field extension of k of degree* $\operatorname{ind}(A)$.

Proof. We may assume that A is division, and use the observation just above. □

Proposition 2.5.6. *Let A be a finite-dimensional central simple k-algebra, and L/k a field extension of finite degree. Then*

$$\operatorname{ind}(A_L) \mid \operatorname{ind}(A) \mid [L:k] \operatorname{ind}(A_L).$$

Proof. The first divisibility was established in Lemma 2.4.7. By Corollary 2.5.5, there exists a field extension E/L splitting the L-algebra A_L and such that $[E:L] = \operatorname{ind}(A_L)$. Then E is a splitting field for the k-algebra A, and it follows from Proposition 2.5.2 that

$$\operatorname{ind}(A) \mid [E:k] = [L:k][E:L] = [L:k] \operatorname{ind}(A_L). \qquad \square$$

Corollary 2.5.7. *If D is a finite-dimensional central division k-algebra and L/k a field extension of finite degree coprime to the degree of D, then D_L is division.*

Proof. Proposition 2.5.6 yields

$$\operatorname{ind}(D_L) = \operatorname{ind}(D) = \deg(D) = \deg(D_L),$$

which implies that D_L is division. □

Proposition 2.5.8. *Let A, B be finite-dimensional central simple k-algebras. Then*

$$\operatorname{ind}(A \otimes_k B) \mid \operatorname{ind}(A) \operatorname{ind}(B) \mid \operatorname{ind}(A \otimes_k B) \gcd(\operatorname{ind}(A)^2, \operatorname{ind}(B)^2).$$

Proof. Let L/k be a splitting field for A such that $[L:k] = \operatorname{ind}(A)$. Then $(A \otimes_k B)_L \simeq M_d(B_L)$, where $d = \deg(A)$, hence $\operatorname{ind}((A \otimes_k B)_L) = \operatorname{ind}(B_L)$. Applying Proposition 2.5.6 to the algebra $A \otimes_k B$, and Lemma 2.4.7 to the algebra B yields

$$\operatorname{ind}(A \otimes_k B) \mid [L:k] \operatorname{ind}((A \otimes_k B)_L) = \operatorname{ind}(A) \operatorname{ind}(B_L) \mid \operatorname{ind}(A) \operatorname{ind}(B),$$

proving the first divisibility. Applying Proposition 2.5.6 to the algebra B, and Proposition 2.5.6 to the algebra $A \otimes_k B$ yields

$$\operatorname{ind}(B) \mid [L:k] \operatorname{ind}(B_L) = \operatorname{ind}(A) \operatorname{ind}((A \otimes_k B)_L) \mid \operatorname{ind}(A) \operatorname{ind}(A \otimes_k B).$$

Similarly $\operatorname{ind}(A) \mid \operatorname{ind}(B) \operatorname{ind}(A \otimes_k B)$, and the second divisibility follows. □

Corollary 2.5.9. *If D, D' are finite-dimensional central division k-algebras of coprime degrees, then $D \otimes_k D'$ is division.*

Proof. Proposition 2.5.8 yields

$$\operatorname{ind}(D \otimes_k D') = \operatorname{ind}(D) \operatorname{ind}(D') = \deg(D) \deg(D') = \deg(D \otimes_k D'),$$

which implies that $D \otimes_k D'$ is division. □

Proposition 2.5.10. *Let D be a finite-dimensional division k-algebra. If D is not commutative, then D contains a nontrivial separable field extension of k.*

Proof. By Lemma 2.4.2, the k-subalgebra generated by any element of $D - k$ is a field (being commutative). Assume for a contradiction that $D - k$ contains no element separable over k. Let $d \in D$. Since D is finite-dimensional over k, 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. The field k has characteristic $p > 0$, and we may find a power q of p such that $P(X) = Q(X^q)$, where $Q \in k[Y]$ and $Q \notin k[Y^p]$. The polynomial Q is irreducible (because P is so), hence separable (as it does not lie in $k[Y^p]$). Since $Q(d^q) = 0$, we must have $d^q \in k$, by our assumption.

Let now $a \in D$ be such that $a \notin \mathcal{Z}(D)$. Consider the k-algebra automorphism $\sigma\colon D \to D$ given by $x \mapsto axa^{-1}$. As we have just seen, there is a power q of p such that $a^q \in k$, so that $\sigma^q = \mathrm{id}$. We thus have $(\sigma - \mathrm{id})^q = \sigma^q - \mathrm{id} = 0$, since k has characteristic p. Let f be the largest integer such that $(\sigma - \mathrm{id})^f \neq 0$, and let $c \in D$ be such that $(\sigma - \mathrm{id})^f(c) \neq 0$. Since $a \notin \mathcal{Z}(D)$, we have $\sigma \neq \mathrm{id}$, and thus $f \geq 1$. Let $x = (\sigma - \mathrm{id})^{f-1}(c)$ and $y = (\sigma - \mathrm{id})^f(c) = \sigma(x) - x$. Since $(\sigma - \mathrm{id})^{f+1} = 0$, we have $\sigma(y) = y$. Set $z = y^{-1}x$. Then

$$\sigma(z) = \sigma(y)^{-1}\sigma(x) = y^{-1}(y + x) = 1 + z.$$

As we have seen above, there is a power r of p such that $z^r \in k$. Then

$$z^r = \sigma(z^r) = \sigma(z)^r = (1 + z)^r = 1 + z^r$$

(as k has characteristic p), a contradiction. □

Corollary 2.5.11. *Assume that k is separably closed (i.e. admits no nontrivial separable extension). Then every finite-dimensional division k-algebra is commutative. In particular, every finite-dimensional central simple k-algebra splits.*

Proof. The first statement follows from Proposition 2.5.10. In particular k is the only finite-dimensional central division k-algebra, which implies the second statement by Wedderburn's Theorem 2.1.12 (and Remark 2.2.2). □

Theorem 2.5.12 (Köthe). *Every finite-dimensional central division k-algebra contains a maximal subfield which is separable over k.*

Proof. Recall that every commutative subalgebra of D is a field by Lemma 2.4.2. Let L be a commutative subalgebra of D, which is maximal among those which are separable as a field extension of k. As L is commutative, we have $L \subset \mathcal{Z}_D(L)$. The L-algebra $\mathcal{Z}_D(L)$ is division by Lemma 2.4.2, and central by Proposition 2.2.11 (v). If $L \subsetneq \mathcal{Z}_D(L)$, then we find a separable extension $L \subsetneq L' \subset \mathcal{Z}_D(L)$ by Proposition 2.5.10, contradicting the maximality of L. Thus $L = \mathcal{Z}_D(L)$, and L is a maximal subfield. □

Corollary 2.5.13. *Let A be a finite-dimensional central simple k-algebra. Then A is split by a separable field extension of k of degree* $\operatorname{ind}(A)$.

Proof. We may assume that A is division, in which case the statement follows from Theorem 2.5.12 (in view of Proposition 2.5.3). □

We conclude this section with two classical results concerning division algebras over specific fields.

Theorem 2.5.14 (Wedderburn, 1905). *Every division ring of finite cardinality is a field.*

Proof. Let k be the center D; it is a field by Lemma 2.2.3. Then D is a finite-dimensional central division k-algebra; let n be its degree. Let q be the cardinality of k. Let L be a maximal subfield of D. Then L/k is a field extension of degree n by Proposition 2.5.3 (iii), and such an extension is isomorphic to the splitting field of the polynomial $X^{q^n} - X \in k[X]$ by the theory of finite fields. Therefore if L' is another maximal subfield of D, there exists an isomorphism of k-algebras $\sigma\colon L \to L'$. Applying Skolem–Noether's Theorem 2.3.2 to the pair of morphisms $L \subset D$ and $L \xrightarrow{\sigma} L' \subset D$ shows that there is $d \in D^\times$ such that $L' = \sigma(L) = dLd^{-1} \subset D$. Thus the group $D^\times$ act transitively on the set of maximal subfields, by conjugation. The set $N = \{d \in D^\times | dLd^{-1} = L\}$ is a subgroup of $D^\times$, and the number of maximal subfields is $[D^\times : N]$. Since any element of D is contained in a maximal subfield (by Proposition 2.5.3 (ii)), the set D is the union of the maximal subfields. Thus

$$[D^\times : N] \cdot |L| = |D| = 1 + |D^\times| = 1 + [D^\times : N] \cdot |N|,$$

which implies that $[D^\times : N] = 1$ and $|L| = |N| + 1$. We deduce that $D = L$, hence D is commutative. □

Theorem 2.5.15 (Frobenius, 1877). *Every finite-dimensional division $\mathbb{R}$-algebra is isomorphic to $\mathbb{R}$, or to $\mathbb{C}$, or to the quaternion $\mathbb{R}$-algebra* $(-1,-1)$.

Proof. Let D be a finite-dimensional division $\mathbb{R}$-algebra, and k its center. Then k is a finite extension of $\mathbb{R}$, hence $k = \mathbb{R}$ or $k \simeq \mathbb{C}$. In the latter case, we have $D \simeq \mathbb{C}$ by Proposition 2.4.3. So we may assume that $k = \mathbb{R}$. Then D splits over the degree two extension $\mathbb{C}$ of $\mathbb{R}$ (by Corollary 2.4.4) hence $\operatorname{ind}(D) \in \{1,2\}$ by Proposition 2.5.2. If $\operatorname{ind}(D) = 1$, then $D = \mathbb{R}$. Otherwise D is a quaternion $\mathbb{R}$-algebra by Corollary 1.2.6; such an algebra is division if and only if it is isomorphic to $(-1,-1)$ by Example 1.1.17. □

6. The Brauer group

Definition 2.6.1. Two finite-dimensional central simple k-algebras A, B are called *Brauer equivalent* if there are integers m, n and an isomorphism of k-algebras $M_n(A) \simeq M_m(B)$.

This defines an equivalence relation on the set of isomorphism classes of finite-dimensional central simple k-algebras (recall that $M_n(M_m(R)) \simeq M_{nm}(R)$ for any ring R). Let us denote by $[A]$ the Brauer-equivalence class of a finite-dimensional central simple k-algebra A. In view of Proposition 2.2.9, the operation $([A],[B]) \mapsto A \otimes_k B$ endows the set of equivalence classes with the structure of an abelian group, where

$$0 = [k] \quad , \quad [A]+[B] = [A \otimes_k B] \quad , \quad -[A] = [A^{\mathrm{op}}].$$

DEFINITION 2.6.2. The group of Brauer-equivalence classes is called the *Brauer group* of k, and is denoted by $\mathrm{Br}(k)$.

By Wedderburn's Theorem 2.1.12 (and Remark 2.2.2), each element of $\mathrm{Br}(k)$ is represented by a finite-dimensional central division k-algebra, which is unique up to isomorphism.

EXAMPLE 2.6.3. It follows respectively from Corollary 2.5.11, Theorem 2.5.14 and Theorem 2.5.15 that:
(i) $\mathrm{Br}(k) = 0$ when k is separably closed.
(ii) $\mathrm{Br}(k) = 0$ when k is finite.
(iii) $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2$.

PROPOSITION 2.6.4. *Let A, B be finite-dimensional central simple k-algebras such that $[B]$ belongs to the subgroup generated by $[A]$ in $\mathrm{Br}(k)$. Then $\mathrm{ind}(B) \mid \mathrm{ind}(A)$.*

PROOF. There is an integer i such that $A^{\otimes i}$ is Brauer-equivalent to B, which implies that $\mathrm{ind}(A^{\otimes i}) = \mathrm{ind}(B)$, by the definition of the index. By Corollary 2.5.5, we may find an extension L/k of degree $\mathrm{ind}(A)$ splitting A. Then L splits $A^{\otimes i}$, hence by Lemma 2.4.7

$$\mathrm{ind}(B) = \mathrm{ind}(A^{\otimes i}) \mid [L:k] = \mathrm{ind}(A). \qquad \square$$

COROLLARY 2.6.5. *The index of a finite-dimensional central simple k-algebra A depends only on the subgroup of $\mathrm{Br}(k)$ generated by $[A]$.*

DEFINITION 2.6.6. If L/k is a field extension, we denote by $\mathrm{Br}(L/k)$ the subgroup of $\mathrm{Br}(k)$ consisting of those classes of algebras split by L.

Observe that, if L/k is a field extension, then the map $\mathrm{Br}(k) \to \mathrm{Br}(L)$ given by $[A] \mapsto [A \otimes_k L]$ is a group morphism, whose kernel is $\mathrm{Br}(L/k)$.

We will use the following observation:

REMARK 2.6.7. Let $A \neq k$ be a split finite-dimensional central simple algebra. Then A contains an element $x \neq 0$ such that $x^2 = 0$. Indeed we may assume that $A = M_r(k)$ for some $r > 1$, and then take for x the matrix whose only nontrivial entry is 1 in the upper right corner.

LEMMA 2.6.8. *Let L/k be a field extension. Then*

$$\mathrm{Br}(L/k) = \bigcup_K \mathrm{Br}(K/k) \subset \mathrm{Br}(k),$$

where K runs over the finitely generated field extensions of k contained in L.

PROOF. We show that every finite-dimensional central division k-algebra D splitting over L splits over a finitely generated subextension of L, proceeding by induction on the degree of D (for all fields k simultaneously). We may assume that $D \neq k$. Then

$D \otimes_k L$ contains an element $x \neq 0$ such that $x^2 = 0$ (Remark 2.6.7). Writing $x = d_1 \otimes \lambda_1 + \cdots + d_n \otimes \lambda_n$, where $d_1, \ldots, d_n \in D$ and $\lambda_1, \ldots, \lambda_n \in L$, we see that x belongs to $D \otimes_k K'$, where K' is the subextension of L generated by $\lambda_1, \ldots, \lambda_n$. Then $D \otimes_k K'$ is not division (as it contains the nonzero noninvertible element x), hence is Brauer equivalent to a central division algebra of strictly smaller degree, by Wedderburn's Theorem 2.1.12 (in view of Remark 2.2.2). So by induction it splits over a finitely generated extension K of K'. Then K is a finitely generated extension of k splitting D. □

Proposition 2.6.9. *If L is a purely transcendental extension of k, then* $\operatorname{Br}(L/k) = 0$.

Proof. By Lemma 2.6.8, we may assume that $L = k(t_1, \ldots, t_n)$, and using induction we reduce to the case $n = 1$, that is $L = k(t)$. Let $D \neq k$ be a finite-dimensional central division k-algebra which splits over $k(t)$. Then $D \otimes_k k(t)$ contains an element $x \neq 0$ such that $x^2 = 0$ (Remark 2.6.7). We may write

$$x = \sum_{i=1}^{n} d_i \otimes (f_i/g_i)$$

where $d_i \in D$ and $f_i, g_i \in k(t)$ for all i. Choosing such a decomposition with n minimal, we see that the elements $d_i \in D$ must be linearly independent over k. Multiplying x with an appropriate element of $k[t]$, we may assume that $g_1 = \cdots = g_n = 1$, and that there is $j \in \{1, \ldots, n\}$ such that f_j is not divisible by t. In particular $x \in D \otimes_k k[t]$. Consider the k-linear map $e \colon D \otimes_k k[t] \to D$ given by $d \otimes f \mapsto df(0)$. Then

$$e(x) = \sum_{i=1}^{n} d_i f_i(0) \in D$$

is nonzero (as the elements d_i are linearly independent over k and $f_j(0) \neq 0$). As e is a ring morphism, we have $e(x)^2 = e(x^2) = 0$. Thus $e(x)$ is a nonzero noninvertible element of the division algebra D, a contradiction. □

Part 2

Torsors

CHAPTER 3

Galois descent

In this chapter, we develop the tools permitting to work with the absolute Galois group, which is almost always infinite. It is however profinite, and such groups carry a nontrivial topology. Compared with finite Galois theory, the key point is that one must systematically keep track of this topology, and in particular restrict one's attention to continuous actions of the Galois group. Although most arguments involving the absolute Galois group can ultimately be reduced to finite Galois theory, this point of view is extremely useful, and permits a very convenient formulation of many results and proofs.

The chapter concludes with a basic treatment of Galois descent, a technique that will be ubiquitous in the sequel. The general philosophy is that extending scalars to a separable closure is a reversible operation, as long as one keeps track of the action of the absolute Galois group.

1. Profinite sets

Definition 3.1.1. An *inverse system* of sets consists of:

— a partially ordered set $(A, \leq)$,
— for each $\alpha \in A$ a set E_α,
— for each $\alpha \leq \beta$ in A a map $f_{\beta\alpha} \colon E_\beta \to E_\alpha$ (called *transition map*).

These data must satisfy the following conditions:

(i) For each $\alpha, \beta \in A$, there is $\gamma \in A$ such that $\alpha \leq \gamma$ and $\beta \leq \gamma$.
(ii) For each $\alpha \in A$, we have $f_{\alpha\alpha} = \mathrm{id}_{E_\alpha}$.
(iii) For each $\alpha \leq \beta \leq \gamma$, we have $f_{\beta\alpha} \circ f_{\gamma\beta} = f_{\gamma\alpha}$.

Definition 3.1.2. The *inverse limit* of an inverse system $(E_\alpha, f_{\beta\alpha})$ is defined as

$$E = \varprojlim E_\alpha = \Big\{ (e_\alpha) \in \prod_{\alpha \in A} E_\alpha \text{ such that } f_{\beta\alpha}(e_\beta) = e_\alpha \text{ for all } \alpha \leq \beta \text{ in } A \Big\}.$$

It is equipped with projections maps $\pi_\alpha \colon E \to E_\alpha$ for every $\alpha \in A$, such that $f_{\beta\alpha} \circ \pi_\beta = \pi_\alpha$ for all $\alpha \leq \beta$. It satisfies the following universal property: if $s_\alpha \colon S \to E_\alpha$ is a collection of maps satisfying $f_{\beta\alpha} \circ s_\beta = s_\alpha$ for all $\alpha \leq \beta$, then there is a unique map $s \colon S \to E$ such that $s_\alpha = \pi_\alpha \circ s$ for all $\alpha \in A$.

Observe that (E'_α) is another inverse system indexed by the same set A and $E'_\alpha \to E_\alpha$ are maps compatible with the transition maps, there is a unique morphism $\varprojlim E'_\alpha \to \varprojlim E_\alpha$ compatible with the projection maps.

Definition 3.1.3. A *profinite set* E is an inverse limit of finite sets E_α. It is endowed with the *profinite topology*, which is generated by open subsets of the form $\pi_\alpha^{-1}\{x\}$ for $\alpha \in A$ and $x \in E_\alpha$, where $\pi_\alpha \colon E \to E_\alpha$ is the projection map.

Let us fix an inverse system of finite sets E_α for $\alpha \in A$, with transition maps $f_{\alpha\beta}$, inverse limit E, and projection maps $\pi_\alpha \colon E \to E_\alpha$.

Lemma 3.1.4. *Every open subset of E is a union of subsets of the form $\pi_\alpha^{-1}\{x\}$ where $\alpha \in A$ and $x \in E_\alpha$.*

Proof. Let $U \subset E$ be an open subset, and $u \in U$. By definition of the topology, there are $\alpha_1, \ldots, \alpha_n \in A$ and $x_i \in E_{\alpha_i}$ for $i = 1, \ldots, n$ such that $\pi_{\alpha_1}^{-1}\{x_1\} \cap \cdots \cap \pi_{\alpha_n}^{-1}\{x_n\}$ is contained in U and contains u. Let us choose $\alpha \in A$ such that $\alpha_i \leq \alpha$ for all $i \in \{1, \ldots, n\}$. Set $x = \pi_\alpha(u)$. Then $u \subset \pi_\alpha^{-1}\{x\}$. On the other hand $\pi_\alpha^{-1}\{x\} \subset \pi_{\alpha_i}^{-1}\{x_i\}$ for all i, hence $\pi_\alpha^{-1}\{x\} \subset U$. $\square$

Lemma 3.1.5. *The inverse limit of an inverse system of nonempty finite sets is nonempty.*

Proof. Assume that each E_α is nonempty. Let us define a subsystem as a collection of subsets $T_\alpha \subset E_\alpha$ for each $\alpha \in A$ such that $f_{\beta\alpha}(T_\beta) \subset T_\alpha$ for each $\alpha \leq \beta$. Consider the set $\mathcal{T}$ of all subsystems (T_α) such that each T_α is nonempty. We may order such subsystems by inclusion. Consider a totally ordered family of subsystems $(T_\alpha)_i \in \mathcal{T}$, for $i \in I$. For a fixed $\alpha \in A$, let us set $S_\alpha = \bigcap_{i \in I}(T_\alpha)_i$. Since each $(T_\alpha)_i$ is nonempty, so is S_α (here we use the finiteness of E_α), and therefore $S_\alpha \in \mathcal{T}$. Thus by Zorn's lemma, there is a (possibly nonunique) minimal element of $(T_\alpha) \in \mathcal{T}$.

Consider the subsystem (T'_α) defined by $T'_\alpha = \bigcap_{\alpha \leq \beta} f_{\beta\alpha}(T_\beta)$. Let $\alpha \in A$. Since T_α is finite, we may write $T'_\alpha = f_{\beta_1\alpha}(T_{\beta_1}) \cap \cdots \cap f_{\beta_n\alpha}(T_{\beta_n})$ where $\alpha \leq \beta_i$ for $i = 1, \ldots, n$. Choose $\beta \in A$ such that $\beta_i \leq \beta$ for all $i = 1, \ldots, n$. Then T'_α contains the set $f_{\beta\alpha}(T_\beta)$ which is nonempty, since T_β is nonempty. We have proved that $(T'_\alpha) \in \mathcal{T}$. By minimality of (T_α), we deduce that $(T'_\alpha) = (T_\alpha)$; in other words the maps $T_\beta \to T_\alpha$ for $\alpha \leq \beta$ are surjective.

Now let us fix $\gamma \in A$ and $x \in T_\gamma$. For $\alpha \in A$, we set

$$S_\alpha = \begin{cases} \text{preimage of } \{x\} \text{ under } T_\alpha \to T_\gamma & \text{if } \gamma \leq \alpha, \\ T_\alpha & \text{otherwise.} \end{cases}$$

Then (S_α) is a subsystem contained in (T_α). By surjectivity of the maps $T_\alpha \to T_\gamma$ when $\gamma \leq \alpha$, it follows that $(S_\alpha) \in \mathcal{T}$. By minimality of (T_α), we deduce that $(S_\alpha) = (T_\alpha)$. We have $S_\gamma = \{x\}$, and thus $T_\gamma = \{x\}$. We have proved that each T_α is a singleton, say $T_\alpha = \{x_\alpha\}$. The elements $x_\alpha \in E_\alpha$ then define an element of $\varprojlim E_\alpha$. $\square$

Proposition 3.1.6. *Every profinite set is compact.*

Proof. Let U_i for $i \in I$ be a family of open subsets covering E. We need to find a finite subset $J \subset I$ such that the subsets U_i for $i \in J$ cover E. While doing so, by Lemma 3.1.4 we may assume that each U_i is of the form $\pi_{\alpha_i}^{-1}\{x_i\}$, where $\alpha_i \in A$ and $x_i \in E_\alpha$.

For each $\alpha \in A$, let $F_\alpha \subset E_\alpha$ be the subset consisting of those elements x such that $f_{\alpha\alpha_i}(x) \neq x_i$ for every $i \in I$ such that $\alpha_i \leq \alpha$. Then for any $\alpha \leq \beta$, we have $f_{\beta\alpha}(F_\beta) \subset F_\alpha$, hence the sets F_α for $\alpha \in A$ form an inverse system, whose transition maps are the restrictions of the maps $f_{\beta\alpha}$.

Assume that $F_\alpha = \varnothing$ for some $\alpha \in A$. Then E_α is covered by subsets of the form $V_i = f_{\alpha\alpha_i}^{-1}\{x_i\}$. As E_α is finite, it is covered by finitely many such subsets, and thus

$E = \pi_\alpha^{-1} E_\alpha$ is covered by finitely many subsets of the form $\pi_\alpha^{-1} V_i = U_i$. Thus we are done in this case.

Therefore we may assume that $F_\alpha \neq \varnothing$ for each $\alpha \in A$. Then $\varprojlim F_\alpha$ contains an element by Lemma 3.1.5. Its image in $y \in E$ satisfies $\pi_\alpha(y) \in F_\alpha \subset E_\alpha$ for all $\alpha \in A$, and in particular y belongs to no U_i. This contradicts the fact the the subsets U_i for $i \in I$ cover E. $\square$

LEMMA 3.1.7. *Assume that each E_α is finite, and that the transition maps $E_\beta \to E_\alpha$ for $\alpha \leq \beta$ are surjective. Then the projection maps $\pi_\alpha \colon E \to E_\alpha$ are surjective.*

PROOF. Fix $\gamma \in A$ and $x \in E_\gamma$. Define an inverse system by

$$F_\alpha = \begin{cases} \text{preimage of } \{x\} \text{ under } E_\alpha \to E_\gamma & \text{if } \gamma \leq \alpha \ , \\ E_\alpha & \text{otherwise.} \end{cases}$$

Then each F_α is nonempty and finite, hence $\varprojlim F_\alpha$ contains an element by Lemma 3.1.5. Its image in $y \in E$ satisfies $\pi_\gamma(y) = x$. $\square$

2. Profinite groups

DEFINITION 3.2.1. When each E_α appearing in Definition 3.1.1 is a group and the transition maps $f_{\beta\alpha}$ are group morphisms, we say that E_α is an *inverse system of groups*. Its inverse limit is naturally a group, and the projections maps π_α are group morphisms. Such an inverse limit is called a *profinite group* when each E_α is finite.

EXAMPLE 3.2.2. Every finite group is a profinite group, whose topology is discrete (take for A a singleton).

EXAMPLE 3.2.3. Let p be a prime number. The groups $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$, together with the maps $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for $m \leq n$ given by $(1 \mod p^n) \mapsto (1 \mod p^m)$ yield an inverse system of groups, whose limit is the profinite group denoted by $\mathbb{Z}_p$.

EXAMPLE 3.2.4. The groups $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$, together with the maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$ given by $(1 \mod n) \mapsto (1 \mod m)$ yield an inverse system of groups, whose limit is the profinite group denoted by $\widehat{\mathbb{Z}}$.

We fix an inverse system of groups Γ_α for $\alpha \in A$, with transition morphisms $f_{\beta\alpha} \colon \Gamma_\beta \to \Gamma_\alpha$ when $\alpha \leq \beta$, set $\Gamma = \varprojlim \Gamma_\alpha$, and denote by $\pi_\alpha \colon \Gamma \to \Gamma_\alpha$ the projections. We also define the subgroups $U_\alpha = \ker \pi_\alpha$.

LEMMA 3.2.5. *(i) Let $U \subset \Gamma$ be an open subset and $u \in U$. Then there is an index α such that $uU_\alpha \subset U$.*
(ii) A subgroup of Γ is open if and only if it is closed and of finite index.
(iii) If a subgroup of Γ contains an open subgroup, it is open.

PROOF. (i) : By Lemma 3.1.4 there are $\alpha \in A$ and $x \in E_\alpha$ such that $\pi_\alpha^{-1}\{x\}$ is contained in U and contains u. Then $uU_\alpha \subset \pi_\alpha^{-1}\{x\}$.

(ii) : Let $U \subset \Gamma$ be an open subgroup, and S its complement in Γ. Then S is the union of the subsets γU for $\gamma \in S$. Such subsets are homeomorphic to U, hence open, so that S is open, proving that U is closed. By (i) (with $u = 1$) the subgroup U contains U_α for some $\alpha \in A$. Certainly U_α has finite index in Γ (since $\Gamma/U_\alpha \simeq \Gamma_\alpha$), so that U has finite index in Γ.

Let now $H \subset \Gamma$ be a closed subgroup of finite index. Its complement is the union of subsets γH where γ runs over a finite subset of Γ (a set of representatives of Γ/H), hence is closed. Thus H is open.

(iii) : Let $H \subset \Gamma$ be a subgroup containing an open subgroup U. Then $H = HU = \bigcup_{h \in H} hU$ is open, since each hU is open, being homeomorphic to U. $\square$

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`.