Brauer Groups of fields

Olivier Haution

Ludwig-Maximilians-Universität München

Winter semester 2020/2021

Contents

Note on the literature

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

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

Part 1

Noncommutative Algebra

CHAPTER 1

Quaternion algebras

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

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

1. The norm form

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

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

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

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

Definition 1.1.1. Let $a, b \in k^\times$. We define a k-algebra (a, b) as follows. A basis of (a, b) as k-vector space is given by $1, i, j, ij$. It is easy to verify that (a, b) admits a unique k-algebra structure such that

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

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

Let us first formalise an argument that will be used repeatedly, in order to prove that a given algebra is isomorphic to a certain 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 $1, i$. □

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 $j = \beta^{-1}j''$. □

The algebra $M_2(k)$ of 2 by 2 matrices with coefficients in k is an example of quaternion algebra:

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. We will focus on "intrinsic" properties of Q, i.e. those that do not depend on the choice of a particular isomorphism $Q \simeq (a, b)$ for some $a, b \in k^\times$. Of course, the proofs may involve choosing such a representation.

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 $u = u(av) = (ua)v = v$.

Of course, 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 below. □

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 $a, b \in k^\times$).

Note that Proposition 1.1.13 (v) provides an effective of checking whether a quaternion algebra is split, by looking at the solutions of a quadratic equation.

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 illustrates the strong connections between the theories of quaternion algebras and quadratic forms. 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 $y = w = 0$. □

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 $D \simeq (a, b)$. □

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 $\dim_k L = 2$. □

We thus obtain an intrinsic characterisation of quaternion division algebras (recall that a quaternion algebra is either split or division, by Proposition 1.1.13):

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. □

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) ⇒ (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) ⇒ (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) ⇒ (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 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 $q_1q_2 \neq q_2q_1$. Let $y = q_1 \otimes 1 - q_2 \otimes i - 1 \otimes j \in Q \otimes_k Q'$. Then

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

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

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

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

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

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

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

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

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*

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

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 1.1.19 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

Simple algebras

In this chapter, we develop the general theory of finite-dimensional 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.

The tensor product of simple algebras need not be simple. We prove that this is however the case when one factor is additionally central. The notion of commutant (also called centraliser) generalises that of center of an algebra. Applied to a subalgebra, this yields another subalgebra, which in some respects behaves as a dual to the original subalgebra. Our analysis of the commutant will be used in the next chapter to investigate the so-called "maximal subfields" of division algebras.

We conclude this chapter with Skolem–Noether's Theorem, which essentially describes the automorphism group of finite-dimensional central simple algebras, by asserting that all such automorphisms are inner (that is, given by the conjugation by some invertible element).

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 $\mathrm{End}_R(M)$. □

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.

We now collect a few facts concerning matrix algebras, that are proved using explicit manipulations of the matrix coefficients.

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

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

(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 $k,l \in \{1,\dots,n\}$ 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 $R \simeq \mathrm{End}_B(I_r)^{\mathrm{op}} \simeq \mathrm{End}_B(I)^{\mathrm{op}}$. □

The main interest of Proposition 2.1.7 (iii) is that it permits to recover R from $M_n(R)$ when R is division. We deduce that following "unicity" result:

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

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

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.

Remark 2.1.11. In the literature, the artinian property is sometimes included in the definition of simple rings. So what we call "artinian simple rings" are simply refered to as "simple rings".

Proposition 2.1.12. *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 2.1.13 (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 2.1.12. Then the ring $E = \mathrm{End}_A(S)$ is division by Schur's Lemma 2.1.2. By Proposition 2.1.12 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

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

In this section, we consider the problem of determining whether a tensor product of simple algebras is simple.

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 $y \in \mathcal{Z}(R)$. □

Let us investigate the interactions between the tensor product and commutant.

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 $A \otimes_k B$

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

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'. We have proved that $C \subset \mathcal{Z}_A(A') \otimes_k B$. □

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). □

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

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & C \\ {\scriptstyle a\mapsto a\otimes 1}\downarrow & & \downarrow{\scriptstyle c\mapsto c\otimes 1} \\ A \otimes_k B & \xrightarrow{f\otimes \mathrm{id}_B} & C \otimes_k B \end{array}$$

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). □

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 $a_1, \ldots, a_n \in A$ 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 A:

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

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

$$(a \otimes 1)i - i(a \otimes 1) = (aa_2 - a_2a) \otimes b_2 + \cdots + (aa_n - a_na) \otimes b_n \in I.$$

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. □

Remark 2.2.7. The assumption that one factor is central is necessary in Proposition 2.2.6 (take $A = B = L$, where L/k is, say, a quadratic field extension).

We can now summarise our results as follows:

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 2.2.6, Proposition 2.2.4 and Proposition 2.2.5. □

In order to proceed further, let us restrict ourselves to finite-dimensional algebras.

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. The map φ is a nonzero morphism of k-algebras (because $\mathrm{End}_k(A) \neq 0$, as A is simple), and its kernel is a two-sided ideal in the ring $A \otimes_k A^{\mathrm{op}}$, which is simple by Proposition 2.2.6. 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 $\varphi\colon A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ of Proposition 2.2.9, and let $C = \varphi(B \otimes_k k)$ (recall that A is nonzero, being simple). A morphism in $\mathrm{End}_k(A)$ commutes with C if and only if it is B-linear (for the left action on A induced by multiplication). 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 2.2.3. □

We collect in the next statement useful facts concerning the commutant. Part (iii) is sometimes referred to as the *double centraliser theorem*.

Proposition 2.2.11. *Let A be a finite-dimensional central simple k-algebra and B a simple subalgebra of A. Let $C = \mathcal{Z}_A(B)$.*

(i) The ring C is simple.
(ii) $\dim_k B \cdot \dim_k C = \dim_k A$.
(iii) $\mathcal{Z}_A(C) = B$.
(iv) The centers of B and C coincide, as subsets of A.

Proof. By Proposition 2.1.12, 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

$$C \otimes_k A^{\mathrm{op}} \simeq \mathrm{End}_B(A) \simeq \mathrm{End}_B(S^{\oplus n}) = M_n(\mathrm{End}_B(S)) = M_n(D^{\mathrm{op}}). \tag{2.2.b}$$

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

$$B = \mathrm{End}_B(B)^{\mathrm{op}} \simeq \mathrm{End}_B(S^{\oplus r})^{\mathrm{op}} = M_r(\mathrm{End}_B(S))^{\mathrm{op}} = M_r(D). \tag{2.2.c}$$

(i): Since $M_n(D^{\mathrm{op}})$ is simple by Remark 2.1.6 and Proposition 2.1.7 (i), it follows from Proposition 2.2.5 and (2.2.b) that C is simple.

(ii): 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 (2.2.b) and (2.2.c) 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 $a = bc$.

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

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

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

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

Corollary 2.2.12. *Let A be a finite-dimensional central simple k-algebra and B a central simple subalgebra of A. Then the k-algebra $\mathcal{Z}_A(B)$ is central simple, and*

$$B \otimes_k \mathcal{Z}_A(B) \simeq A.$$

Proof. Let $C = \mathcal{Z}_A(B)$. The k-algebra C is central and simple by Proposition 2.2.11 (iv) and (i). The k-linear map $B \otimes_k C \to A$ given by $b \otimes c \mapsto bc$ is a morphism of k-algebras (because B commutes with C). Its kernel is a two-sided ideal in the ring $B \otimes_k C$, which is simple by Proposition 2.2.6. As $A \neq 0$, the morphism is injective, and bijective for dimensional reasons, in view of Proposition 2.2.11 (ii). □

3. Skolem–Noether's Theorem

A theorem in linear algebra asserts that every automorphism of the matrix algebra $M_n(k)$ is given by conjugation by some matrix. This is a special case of the Skolem–Noether's theorem, which applies to any finite-dimensional central simple algebra. Before proving this theorem, let us make a couple of observations.

Lemma 2.3.1. *Let A be a finite-dimensional 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 2.1.12. 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 $n \in \mathbb{N}$. Then $\dim_k M = n \dim_k S$, hence the integer n is determined by $\dim_k M$. □

We will need the following notation. Let $h\colon B \to A$ be a morphism of k-algebras. We define a $B \otimes_k A^{\mathrm{op}}$-module A^h, by setting $A^h = A$ as a k-vector space, with the module structure given by letting $b \otimes a$, where $b \in B$ and $a \in A^{\mathrm{op}}$, act on A^h by $x \mapsto h(b)xa$.

Lemma 2.3.2. *Let $f, g\colon B \to A$ be morphisms of k-algebras such that $A^f \simeq A^g$ as $B \otimes_k A^{\mathrm{op}}$-modules. Then there exists an element $u \in A^\times$ such that $f(b) = u^{-1}g(b)u$ for all $b \in B$.*

Proof. Let $\varphi\colon A^f \to A^g$ be an isomorphism of $B \otimes_k A^{\mathrm{op}}$-modules. 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

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

so that $vu = 1$, since φ is injective. On the other hand

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

Theorem 2.3.3 (Skolem–Noether). *Let A, B be finite-dimensional simple k-algebras. Assume that A or B is central. If $f, g\colon B \to A$ are morphisms of k-algebras, there exists an element $u \in A^\times$ such that $f(b) = u^{-1}g(b)u$ for all $b \in B$.*

Proof. The k-algebra $B \otimes_k A^{\mathrm{op}}$ is simple by Proposition 2.2.6. As $\dim_k A^f = \dim_k A = \dim_k A^g$, by Lemma 2.3.1 the $B \otimes_k A^{\mathrm{op}}$-modules A^f and A^g are isomorphic, and the statement follows from Lemma 2.3.2. $\square$

Corollary 2.3.4. *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 $a \in A^\times$.*

Proof. Take $B = A$ and $g = \mathrm{id}_A$ in Theorem 2.3.3. $\square$

We later need the following variant of Skolem–Noether's Theorem 2.3.3. In this statement, the B-module structure on A induced by a morphism of k-algebras $h\colon B \to A$ is given by letting $b \in A$ act by $x \mapsto h(b)x$.

Proposition 2.3.5. *Let A be a finite-dimensional central simple k-algebra, and $B_1, \dots, B_n$ be finite-dimensional simple k-algebras. Set $B = B_1 \times \cdots \times B_n$. If $f, g\colon B \to A$ are morphisms of k-algebras inducing isomorphic structures of B-modules on A, then there exists $u \in A$ such that $f(b) = u^{-1}g(b)u$ for all $b \in B$.*

Proof. We will use the following observation (left as an exercise). Let $R_1, \dots, R_n$ be rings, and $R = R_1 \times \cdots \times R_n$. Then every R-module M is of the form $M_1 \times \cdots \times M_n$, where M_i are uniquely determined R_i-modules. Moreover two R-modules M, N are isomorphic if and only if the R_i-modules M_i, N_i are isomorphic for each $i = 1, \dots, n$.

Let $C = B \otimes_k A^{\mathrm{op}}$, and view A^f and A^g as C-modules. We have $C = C_1 \times \cdots \times C_n$ as k-algebras, where $C_i = B_i \otimes_k A^{\mathrm{op}}$. Then for each $i = 1, \dots, n$, the B_i-modules $(A^f)_i$ and $(A^g)_i$ are isomorphic by the assumption, and in particular have the same finite dimension over k. Since each k-algebra C_i is simple by Proposition 2.2.6, it follows from Lemma 2.3.1 that $(A^f)_i$ and $(A^g)_i$ are isomorphic as C_i-modules. We deduce that $A^f \simeq A^g$ as C-modules, and the statement follows from Lemma 2.3.2. $\square$

CHAPTER 3

Central simple algebras and scalars extensions

After extending scalars appropriately, any finite-dimensional central simple algebra 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, and how it relates to the degrees of splitting fields.

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

1. 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 3.1.1. *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 2.2.4, 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 2.2.5 and Proposition 2.2.6. □

LEMMA 3.1.2. *Every finite-dimensional subalgebra of a division k-algebra is division.*

PROOF. Let D be a division k-algebra, and B a finite-dimensional 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 D, 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 $b^{-1} = b' \in B$. □

PROPOSITION 3.1.3. *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 3.1.2. It

has finite dimension over k, and is thus an algebraic extension of k. By assumption it must equal k, hence $x \in k$, and finally $D = k$. □

Corollary 3.1.4. *If k is algebraically closed, every finite-dimensional simple k-algebra is isomorphic to $M_n(k)$ for some integer n.*

Proof. This follows from Wedderburn's Theorem 2.1.13 and Proposition 3.1.3. □

Corollary 3.1.5. *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 central simple by Lemma 3.1.1, hence isomorphic to $M_n(\overline{k})$ for some integer n by Corollary 3.1.4. Then $\dim_k A = \dim_{\overline{k}} A_{\overline{k}} = n^2$. □

Definition 3.1.6. 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 $\deg(A)$.

Observe that $\deg(A_L) = \deg(A)$ for any field extension L/k.

Definition 3.1.7. Two finite-dimensional central simple k-algebras A, B are called *Brauer-equivalent* if there exist 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 $M_n(M_m(A)) \simeq M_{nm}(A)$ for any k-algebra A). Wedderburn's Theorem 2.1.13 implies that each Brauer-equivalence class contains exactly one isomorphism class of division algebras.

Definition 3.1.8. When A is a finite-dimensional central simple k-algebra, the degree of a division algebra Brauer-equivalent to A is called the *index* of A and denoted $\mathrm{ind}(A)$.

Observe that $\mathrm{ind}(A)$ divides $\deg(A)$, and that $\mathrm{ind}(A)$ depends only on the Brauer-equivalence class of A.

Lemma 3.1.9. *Let A be a finite-dimensional central simple k-algebra, and L/k a field extension. Then*

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

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

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

2. Splitting fields

Definition 3.2.1. 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 (which must then coincides with $\deg(A)$). A field extension L/k is called a *splitting field* of A if the L-algebra $A_L = A \otimes_k L$ is split.

In this section, we obtain certain bounds on the degree of finite splitting fields, and prove the existence of such fields having the minimal possible degree.

Proposition 3.2.2. *Let A be a finite-dimensional central simple k-algebra, and L/k an extension of finite degree n splitting A. Then the algebra A is Brauer-equivalent (Definition 3.1.8) to a finite-dimensional central simple k-algebra of degree n containing L as a subalgebra.*

Proof. Let $d = \deg(A)$ and $V = L^{\oplus d}$. We view L as a subalgebra of $\mathrm{End}_L(V)$ by mapping $l \in L$ to the endomorphism $x \mapsto lx$. The isomorphisms of L-algebras $A^{\mathrm{op}} \otimes_k L \simeq M_d(L)^{\mathrm{op}} \simeq M_d(L) \simeq \mathrm{End}_L(V)$ allow us to view A^{op} as a k-subalgebra of $\mathrm{End}_L(V)$; in the algebra $\mathrm{End}_L(V)$, every element of L commutes with A^{op}. Let us view $\mathrm{End}_L(V)$ as a subalgebra of $\mathrm{End}_k(V)$, and set $B = \mathcal{Z}_{\mathrm{End}_k(V)}(A^{\mathrm{op}})$. Then $L \subset B$. It follows from Proposition 2.2.11 (i) and (iv) that B is a central simple k-algebra. By Proposition 2.2.11 (ii) we have $\dim_k A^{\mathrm{op}} \cdot \dim_k B = \dim_k \mathrm{End}_k(V)$. Since $\dim_k A^{\mathrm{op}} = d^2$ and $\dim_k V = dn$, we deduce that $\deg(B) = n$. Finally, by Proposition 2.2.9 and Corollary 2.2.12 we have

$$M_{d^2}(B) \simeq B \otimes_k \mathrm{End}_k(A^{\mathrm{op}}) \simeq B \otimes_k A^{\mathrm{op}} \otimes_k A \simeq \mathrm{End}_k(V) \otimes_k A \simeq M_{dn}(A),$$

so that B is Brauer-equivalent to A. □

Corollary 3.2.3. *Let A be a finite-dimensional central simple k-algebra, and L/k be a field extension of finite degree splitting A. Then*

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

Proof. By the Proposition 3.2.2, we may assume that $\deg(A) = [L : k]$. Then $\mathrm{ind}(A)$ divides $\deg(A) = [L : k]$. □

Lemma 3.2.4. *Let A be a finite-dimensional central simple k-algebra, and $L \subset A$ a subalgebra. Assume that L is a field. Then $[L : k] \mid \deg(A)$, with equality if and only if $L = \mathcal{Z}_A(L)$.*

Proof. Since L is commutative, we have $L \subset \mathcal{Z}_A(L)$. The ring L being simple (Remark 2.1.6), by Proposition 2.2.11 (ii) we have

$$\deg(A)^2 = [L : k] \cdot \dim_k \mathcal{Z}_A(L) = [L : k]^2 \cdot \dim_L \mathcal{Z}_A(L),$$

from which the statement follows. □

Proposition 3.2.5. *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 subalgebras of D.*
(iii) $[L : k] = \mathrm{ind}(D)$.
(iv) *L splits D.*

Proof. The first assertion follows from Lemma 3.1.2.

(i) ⇔ (iii) : This has been proved in Lemma 3.2.4.

(iv) ⇒ (iii) : Since $[L : k] \mid \mathrm{ind}(D)$ by Lemma 3.2.4, this follows from Corollary 3.2.3.

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

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

Definition 3.2.6. A subalgebra L satisfying the equivalent conditions of Proposition 3.2.5 is called a *maximal subfield*.

In view of the characterisation (ii) in Proposition 3.2.5, maximal subfields always exist in finite-dimensional central division k-algebras (by dimensional reasons).

Corollary 3.2.7. *Let A be a finite-dimensional central simple k-algebra. Then A is split by a field extension of k of degree* $\mathrm{ind}(A)$.

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

Proposition 3.2.8. *Let A be a finite-dimensional central simple k-algebra, and L/k a field extension of finite degree. Then*

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

Proof. The first divisibility was established in Lemma 3.1.9. By Corollary 3.2.7, there exists a field extension E/L splitting the L-algebra A_L and such that $[E:L] = \mathrm{ind}(A_L)$. Then E is a splitting field for the k-algebra A, and it follows from Corollary 3.2.3 that

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

Corollary 3.2.9. *If D is a finite-dimensional central division k-algebra and L/k a field extension of finite degree coprime to* $\deg(D)$*, then D_L is division.*

Proof. Proposition 3.2.8 yields

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

which implies that D_L is division. □

Proposition 3.2.10. *Let A, B be finite-dimensional central simple k-algebras. Then*

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

Proof. By Corollary 3.2.7, there exists an extension L/k splitting the k-algebra A and such that $[L:k] = \mathrm{ind}(A)$. Then $(A \otimes_k B)_L \simeq M_d(B_L)$, where $d = \deg(A)$, hence $\mathrm{ind}((A \otimes_k B)_L) = \mathrm{ind}(B_L)$. Applying Proposition 3.2.8 to the k-algebra $A \otimes_k B$, and Lemma 3.1.9 to the k-algebra B yields

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

proving the first divisibility. Applying Proposition 3.2.8 to the algebra B, and Proposition 3.2.8 to the algebra $A \otimes_k B$ yields

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

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

Corollary 3.2.11. *If D, D' are finite-dimensional central division k-algebras of coprime degrees, then $D \otimes_k D'$ is division.*

Proof. Proposition 3.2.10 yields

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

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

3. Separable splitting fields

We have seen that every finite-dimensional central simple k-algebra splits over a finite extension of k (Corollary 3.2.7). In this section, we prove that this extension may additionally be chosen to be *separable*.

Recall that an irreducible polynomial $P \in k[X]$ is called separable if it has no multiple root in every field extension of k. Equivalently P is separable if and only if it is prime to its derivative $P' \in k[X]$. A field extension L/k is called separable if every element of L is the root of an irreducible separable polynomial with coefficients in k (in particular separable will always be algebraic).

Proposition 3.3.1. *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 3.1.2, the k-subalgebra generated by any element of D is a field (being commutative). Assume for a contradiction that no such field is a nontrivial separable extension of k. Since algebraic extensions of fields of characteristic zero are separable, we may assume that k has characteristic $p > 0$. 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. 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 3.3.2. *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 3.3.1. In particular k is the only finite-dimensional central division k-algebra, which implies the second statement by Wedderburn's Theorem 2.1.13. □

Theorem 3.3.3 (Köthe). *Every finite-dimensional central division k-algebra contains a maximal subfield which is separable over k.*

Proof. Let D be a finite-dimensional central division k-algebra. Recall that every commutative subalgebra of D is a field by Lemma 3.1.2. Let L be a commutative subalgebra of D, which is maximal among those which are separable as a field extension of k. Let $E = \mathcal{Z}_D(L)$. As L is commutative, we have $L \subset E$. The L-algebra E is division

by Lemma 3.1.2. If E is not commutative, using Proposition 3.3.1 we find a separable extension L'/L such that $L \subsetneq L' \subset E$. The field extension L'/k is then separable (being a composite of separable extensions), contradicting the maximality of L. Thus E is commutative. Therefore $E \subset \mathcal{Z}_D(E) = L$ by Proposition 2.2.11 (iii). We have proved that $L = E = \mathcal{Z}_D(L)$, so that L is a maximal subfield. □

Corollary 3.3.4. *Let A be a finite-dimensional central simple k-algebra. Then A is split by a separable field extension of k of degree* $\mathrm{ind}(A)$.

Proof. We may assume that A is division, in which case the statement follows from Theorem 3.3.3 (in view of Proposition 3.2.5). □

4. Finite division rings, real division algebras

We are now in position to prove two classical results concerning division algebras over specific fields. Although these results may seem quite different in nature, both proofs crucially rely on the precise understanding of the finite extensions of the respective base field (namely $\mathbb{F}_q$ and $\mathbb{R}$).

Theorem 3.4.1 (Wedderburn, 1905). *Every division ring of finite cardinality is a field.*

Proof. Let D be a division ring of finite cardinality. Its center k is a field by Lemma 2.2.2, and denote by q the cardinality of k. Then D is a finite-dimensional central division k-algebra; let n be its degree. Let L be a maximal subfield of D. Then $[L : k] = n$ by Proposition 3.2.5 (iii).

For $d \in D^\times$, the subset $K = d^{-1}Ld \subset D$ is a k-subalgebra. Moreover the map $L \to K$ given by $x \mapsto d^{-1}xd$ is an isomorphism of k-algebras. In particular K is a field and $[K : k] = [L : k] = n$. It follows from Proposition 3.2.5 (iii) that K is a maximal subfield of D. We have thus defined an action of the group $D^\times$ on the set of maximal subfields of D.

By the theory of finite fields, the extension L/k is isomorphic to the splitting field of the polynomial $X^{q^n} - X \in k[X]$. 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 2.3.3 to the pair of morphisms $L \subset D$ and $L \xrightarrow{\sigma} L' \subset D$ (recall that L is a simple ring, being a field) shows that there exists $e \in D^\times$ such that $L' = \sigma(L) = e^{-1}Le \subset D$. This proves that the above action is transitive.

The set $N = \{d \in D^\times | d^{-1}Ld = L\}$ is a subgroup of $D^\times$, and the number of maximal subfields of D is $[D^\times : N]$. Since any element of D is contained in a maximal subfield (by Proposition 3.2.5 (ii)), the set $D^\times - \{1\}$ is the union of the sets $K^\times - \{1\}$, where K runs over the maximal subfields of D. Thus

$$[D^\times : N] \cdot (|L^\times| - 1) \geq |D^\times| - 1 = [D^\times : N] \cdot |N| - 1.$$

Since N contains $L^\times$, we must have $[D^\times : N] = 1$ and $L^\times = N$. We deduce that $D = L$, hence D is commutative. □

Theorem 3.4.2 (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 3.1.3. So we may assume that $k = \mathbb{R}$. Then D splits over the degree two extension $\mathbb{C}/\mathbb{R}$ (by Corollary 3.1.4) hence $\mathrm{ind}(D) \in \{1, 2\}$ by Corollary 3.2.3. If $\mathrm{ind}(D) = 1$, 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 1.1.18. □

5. The Brauer group, I

Let us denote by $[A]$ the Brauer-equivalence class (Definition 3.1.8) 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 3.5.1. The group of Brauer-equivalence classes is called the *Brauer group* of k, and is denoted by $\mathrm{Br}(k)$.

Remark 3.5.2. When A, B are finite-dimensional central simple k-algebras with $B \subset A$, the Brauer-class of the commutant $\mathcal{Z}_A(B)$ can be expressed using Corollary 2.2.12:

$$[\mathcal{Z}_A(B)] = [A] - [B] \in \mathrm{Br}(k).$$

Example 3.5.3. It follows respectively from Corollary 3.3.2, Theorem 3.4.1 and Theorem 3.4.2 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 3.5.4. *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 $A^{\otimes i} = A \otimes_k \cdots \otimes_k A$ is Brauer-equivalent to B, which implies that $\mathrm{ind}(A^{\otimes i}) = \mathrm{ind}(B)$. By Corollary 3.2.7, we may find an extension L/k of degree $\mathrm{ind}(A)$ splitting A. Then the L-algebra $(A^{\otimes i})_L$ is isomorphic to $A_L \otimes_L \cdots \otimes_L A_L$, hence splits because each A_L splits. Thus by Lemma 3.1.9

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

Corollary 3.5.5. *The index of a finite-dimensional central simple k-algebra A depends only on the subgroup of $\mathrm{Br}(k)$ generated by $[A]$.*

Definition 3.5.6. 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 $\mathrm{Br}(L/k)$.

Example 3.5.7. Assume that k has characteristic $\neq 2$, and let $L = k(\sqrt{a})$ for some $a \in k^\times$. Then

$$\mathrm{Br}(L/k) = \{[(a, b)], b \in k^\times\}.$$

Indeed any element of $\mathrm{Br}(k)$ is of the form $[D]$, where D is a finite-dimensional central division k-algebra. If $[D] \in \mathrm{Br}(L/k)$, then $\mathrm{ind}(D) \in \{1, 2\}$ by Corollary 3.2.3. In any case $[D]$ is the class of a quaternion algebra (possibly split), and we conclude using Proposition 1.2.9.

Let us observe that split nontrivial finite-dimensional central simple algebras contain nilpotent elements, which distinguishes them from division algebras:

Remark 3.5.8. 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 3.5.9. *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 3.5.8). 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 2.1.13. 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 3.5.10. *If L is a purely transcendental extension of k, then*

$$\mathrm{Br}(L/k) = 0.$$

Proof. If $L = k(t_i, i \in I)$, then every element of L belongs to a subextension of L/k generated by finitely many t_i's (such element is a quotient of two polynomials, and a given polynomial involves only finitely many variables). Therefore every finitely generated subextension K/k is contained in a subextension of L/k generated by finitely many t_i's. In view of Lemma 3.5.9, we may thus assume that I is finite. Using induction we reduce to the case $|I| = 1$, 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 3.5.8). 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 4

Infinite Galois theory

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

We begin this chapter with basic facts and definitions concerning profinite sets, which will allow us to manipulate infinite Galois groups later on.

DEFINITION 4.1.1. A *directed set* is a nonempty set $\mathcal{A}$, equipped with a partial order $\leq$, such that for any $\alpha, \beta \in \mathcal{A}$, there exists $\gamma \in \mathcal{A}$ such that $\alpha \leq \gamma$ and $\beta \leq \gamma$.

DEFINITION 4.1.2. Let $(\mathcal{A}, \leq)$ be a directed set. An *inverse system* of sets (indexed by $\mathcal{A}$) consists of:

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

These data must satisfy the following conditions:

(i) For each $\alpha \in \mathcal{A}$, we have $f_{\alpha\alpha} = \mathrm{id}_{E_\alpha}$.
(ii) For each $\alpha \leq \beta \leq \gamma$, we have $f_{\beta\alpha} \circ f_{\gamma\beta} = f_{\gamma\alpha}$.

DEFINITION 4.1.3. The *inverse limit* of an inverse system $(E_\alpha, f_{\beta\alpha})$ is defined as

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

It is equipped with projections maps $\pi_\alpha \colon E \to E_\alpha$ for every $\alpha \in \mathcal{A}$, such that $f_{\beta\alpha} \circ \pi_\beta = \pi_\alpha$ for all $\alpha \leq \beta$. It enjoys 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 $\alpha \in \mathcal{A}$.

Observe that $(E_\alpha), (E'_\alpha)$ are inverse systems indexed by the same directed set $\mathcal{A}$ 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 4.1.4. Let $\mathcal{A}$ be directed set, and E the inverse limit of finite sets E_α for $\alpha \in \mathcal{A}$. The *profinite topology* on the set E, is the topology generated by open subsets of the form $\pi_\alpha^{-1}\{x\}$ for $\alpha \in \mathcal{A}$ and $x \in E_\alpha$, where $\pi_\alpha \colon E \to E_\alpha$ is the projection map.

Definition 4.1.5. A topological space E is called a *profinite set* if it is an inverse limit of finite sets E_α for $\alpha \in \mathcal{A}$, for some directed set $\mathcal{A}$, the topology of E being the profinite topology.

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

Lemma 4.1.6. *Every open subset of E is a union of subsets of the form $\pi_\alpha^{-1}\{x\}$ where $\alpha \in \mathcal{A}$ and $x \in E_\alpha$.*

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

Lemma 4.1.7. *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 $\alpha \in \mathcal{A}$ 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 $\alpha \in \mathcal{A}$, 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 $\alpha \in \mathcal{A}$. Since T_α is finite, we may write $T'_\alpha = f_{\beta_1\alpha}(T_{\beta_1}) \cap \dots \cap f_{\beta_n\alpha}(T_{\beta_n})$ where $\alpha \leq \beta_i$ for $i = 1, \dots, n$. Choose $\beta \in \mathcal{A}$ such that $\beta_i \leq \beta$ for all $i = 1, \dots, n$. 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 $\gamma \in \mathcal{A}$ and $x \in T_\gamma$. For $\alpha \in \mathcal{A}$, 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 $\varprojlim E_\alpha$. □

Proposition 4.1.8. *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 4.1.6 we may assume that each U_i is of the form $\pi_{\alpha_i}^{-1}\{x_i\}$, where $\alpha_i \in \mathcal{A}$ and $x_i \in E_\alpha$.

For each $\alpha \in \mathcal{A}$, 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 $\alpha \in \mathcal{A}$ form an inverse system, whose transition maps are the restrictions of the maps $f_{\beta\alpha}$.

Assume that $F_\alpha = \varnothing$ for some $\alpha \in \mathcal{A}$. 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 $\alpha \in \mathcal{A}$. Then $\varprojlim F_\alpha$ contains an element by Lemma 4.1.7. Its image in $y \in E$ satisfies $\pi_\alpha(y) \in F_\alpha \subset E_\alpha$ for all $\alpha \in \mathcal{A}$, and in particular y belongs to no U_i. This contradicts the fact that the subsets U_i for $i \in I$ cover E. □

Remark 4.1.9. Proposition 4.1.8 and Lemma 4.1.7 may also be viewed as consequences of Tikhonov's Theorem, asserting that a product of compact topological spaces is compact.

Remark 4.1.10. The sets $F_\alpha = \operatorname{im}\pi_\alpha \subset E_\alpha$ for an inverse system. Let F be its inverse limit. The natural map $F \to E$ is continuous, open, and bijective, and is therefore a homeomorphism. Thus (replacing E_α with F_α) we can always represent a profinite set as an inverse limit of finite sets in such a way that the projection maps are surjective. Note that this implies that the transition maps are also surjective.

Conversely:

Lemma 4.1.11. *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 $\gamma \in \mathcal{A}$ 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 4.1.7. Its image in $y \in E$ satisfies $\pi_\gamma(y) = x$. □

2. Profinite groups

We now specialise to the case of profinite groups, and gather the general results that will be applied to Galois groups.

Definition 4.2.1. When each E_α appearing in Definition 4.1.2 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. When each E_α is finite, the topological group E is called a *profinite group*.

Example 4.2.2. Every finite group is a profinite group, whose topology is discrete (take for $\mathcal{A}$ a singleton).

Example 4.2.3. 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 4.2.4. 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 $\widehat{\mathbb{Z}}$.

Let us fix a profinite group Γ. We choose a directed set $\mathcal{A}$ and an inverse system of finite groups Γ_α for $\alpha \in \mathcal{A}$ such that $\Gamma = \varprojlim \Gamma_\alpha$, and denote by $\pi_\alpha \colon \Gamma \to \Gamma_\alpha$ the projections. We also define the subgroups $U_\alpha = \ker \pi_\alpha$. By Remark 4.1.10, we can assume that each projection morphism π_α is surjective, and thus identify each Γ_α with Γ/U_α.

Lemma 4.2.5. *(i) Let $U \subset \Gamma$ be an open subset and $u \in U$. Then there exists $\alpha \in \mathcal{A}$ such that $uU_\alpha \subset U$.*
(ii) A subgroup of Γ is open if and only if it is closed and has finite index.
(iii) If a subgroup of Γ contains an open subgroup, it is open.

Proof. (i) : By Lemma 4.1.6 there exist $\alpha \in \mathcal{A}$ 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 images of U under a self-homeomorphism of Γ (namely, left multiplication by γ), hence are open, so that S is open, proving that U is closed. By (i) (with $u = 1$) the subgroup U contains U_α for some $\alpha \in \mathcal{A}$. Certainly U_α has finite index in Γ (as $\Gamma/U_\alpha \simeq \Gamma_\alpha$), 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 $H = HU$ is the union of the subsets hU for $h \in H$. Such subsets are images of U under a self-homeomorphism of Γ, hence are open, so that H is open. □

Remark 4.2.6. Let $\mathcal{U}$ be the set of open normal subgroups of Γ, ordered by letting $U \leq V$ when $V \subset U$. Then $\mathcal{U}$ is a directed set, and the groups Γ/U for $U \in \mathcal{U}$ form an inverse system of finite groups, whose inverse limit is isomorphic to Γ, as a topological group (exercise). Thus every profinite group admits a canonical representation as an inverse limit.

Definition 4.2.7. Let p be a prime number. Recall that a p-group is a finite group whose order is a power of p. A *pro-p-group* is an inverse limit of p-groups. A subgroup P of Γ is called a *pro-p-Sylow subgroup* if all the following conditions are satisfied:

(i) P is a closed subgroup of Γ,
(ii) P is a pro-p-group,
(iii) for every open normal subgroup U of Γ, the image of P in Γ/U has index prime to p.

Observe that if P is a pro-p-Sylow subgroup of Γ, then the image of P in Γ/U is a Sylow p-group, for every open normal subgroup U of Γ.

Proposition 4.2.8. *The profinite group Γ admits a pro-p-Sylow subgroup.*

Proof. For each $\alpha \in \mathcal{A}$, let S_α be the set of p-Sylow subgroups of $\Gamma_\alpha = \Gamma/U_\alpha$, which is finite and nonempty by Sylow's Theorem. If $\alpha \leq \beta$ in $\mathcal{A}$, the map $\Gamma_\beta \to \Gamma_\alpha$ sends elements of S_β to elements of S_α, because the image of a p-Sylow subgroup under

a surjective morphism of finite groups is a p-Sylow subgroup (exercise). Thus the sets S_α form an inverse system indexed by $\mathcal{A}$, whose inverse limit S is nonempty by Lemma 4.1.7. Any element of S is represented by a collection of p-Sylow subgroups $P_\alpha \subset \Gamma_\alpha$ for $\alpha \in \mathcal{A}$, such that for any $\alpha \leq \beta$ in $\mathcal{A}$ the morphism $\Gamma_\beta \to \Gamma_\alpha$ maps P_β onto P_α. The group $P = \varprojlim P_\alpha$ is naturally a subgroup of Γ, and is a pro-p-group. The subset $P \subset \Gamma$ is closed, being the intersection of the preimages of $P_\alpha \subset \Gamma_\alpha$ for $\alpha \in \mathcal{A}$ (by construction of the inverse limit). It follows from Lemma 4.1.11 (applied to the system P_α for $\alpha \in \mathcal{A}$) that for each $\alpha \in \mathcal{A}$ the image of P in Γ_α is the p-Sylow subgroup P_α. Now any an open subgroup U of Γ contains U_α for some $\alpha \in \mathcal{A}$, and the image of P in Γ/U coincides with the image of P_α under the surjective morphism $\Gamma_\alpha = \Gamma/U_\alpha \to \Gamma/U$, and in particular has index prime to p (exercise). □

Lemma 4.2.9. *Let X be a set with an action of the profinite group Γ. The following conditions are equivalent:*

(i) The action map $\Gamma \times X \to X$ is continuous, for the discrete topology on X.
(ii) Every element of X is fixed by some open subgroup of Γ.

Proof. (i) ⇒ (ii) : Let $x \in X$. The map $\Gamma \to X$ given by $g \mapsto g \cdot x$ factors as $\Gamma = \Gamma \times \{x\} \subset \Gamma \times X \to X$ (where the last map is the action map), and is thus continuous by (i). Therefore the preimage of $x \in X$ is an open subset of Γ, which by construction fixes x. This proves (ii).

(ii) ⇒ (i) : For $x, y \in X$, we denote by $U_{x,y}$ the subset of Γ consisting of those elements γ such that $\gamma x = y$. The set $U_{x,y}$ is either empty, or equal to $\gamma U_{x,x}$ for some (in fact, any) $\gamma \in U_{x,y}$. The subgroup $U_{x,x} \subset \Gamma$ contains an open subgroup by (ii), hence is open by Lemma 4.2.5 (iii). Thus $U_{x,y}$ is open, being either empty or the image of $U_{x,x}$ under a self-homeomorphism of Γ. Now the preimage of any $y \in X$ under the action morphism $\Gamma \times X \to X$ is the union of the subsets $U_{x,y} \times \{x\}$ where x runs over X, which are open since X has the discrete topology. This proves (i). □

Definition 4.2.10. When the conditions of Lemma 4.2.9 are fulfilled, we say that Γ acts *continuously* on X, or that X is a *discrete Γ-set*. A discrete Γ-set equipped with a Γ-equivariant group structure will be called a discrete Γ-*group*. A discrete Γ-group whose underlying group is abelian will be called a discrete Γ-*module*. We define a morphism of discrete Γ-groups, resp. Γ-modules, as a Γ-equivariant group morphism.

Lemma 4.2.11. *Let X be a discrete Γ-set, and F a finite subset of X. Then there exists an open subgroup of Γ fixing each element of F.*

Proof. By assumption, each $f \in F$ is fixed by some open subgroup U_f of Γ. Then the open subgroup $\bigcap_{f \in F} U_f$ of Γ fixes each element of F. □

We conclude this section with a statement that will be needed later. When a group acts on a set X, we denote by X^G the set of elements of X fixed by every element of G.

Lemma 4.2.12. *Let X be a discrete Γ-set and n an integer. Then every continuous map $\Gamma^n \to X$ factors through a map $(\Gamma/U)^n \to X^U$ for some open normal subgroup U of Γ. Conversely, any map $\Gamma^n \to X$ factoring through $(\Gamma/U)^n \to X$ for some open normal subgroup U of Γ is continuous.*

Proof. If $\Gamma^n \to X$ factors through a map $(\Gamma/U)^n \to X$ for some open normal subgroup U of Γ, it is continuous, since both maps $\Gamma^n \to (\Gamma/U)^n$ and $(\Gamma/U)^n \to X$ are continuous (for the discrete topology on $(\Gamma/U)^n$).

Let now $f\colon \Gamma^n \to X$ be a continuous map, and $Y \subset X$ its image. Since Γ^n is profinite set (the limit of the inverse system $(\Gamma_\alpha)^n$), it is compact by Proposition 4.1.8. Therefore Y is compact. Being also discrete, the set Y is finite. Since X is a discrete Γ-set, there is an open subgroup U' in Γ fixing all the elements of Y (Lemma 4.2.11). Shrinking U', we may assume that it is normal in Γ (by Lemma 4.2.5 (i) with $u = 1$). We have achieved $f(\Gamma^n) \subset X^{U'}$.

For each $x \in X$, the preimage $f^{-1}\{x\}$ is an open subset of Γ^n. For any $g \in f^{-1}\{x\}$, we may find open subsets $W_1, \dots, W_n$ of Γ such that $g \in W_1 \times \cdots \times W_n \subset f^{-1}\{x\}$. Write $g = (g_1, \dots, g_n) \in \Gamma^n$ with $g_1, \dots, g_n \in \Gamma$. By Lemma 4.2.5 (i), for each $i \in \{1, \dots, n\}$ we may find an open normal subgroup $V_{g,i}$ of Γ such that $g_i V_{g,i} \subset W_i$. Set $V_g = V_{g,1} \cap \cdots \cap V_{g,n}$. Then $g(V_g)^n$ is an open subset of $f^{-1}\{x\}$. Therefore the set $f^{-1}\{x\}$ is covered by the open subsets $g(V_g)^n$ for $g \in f^{-1}\{x\}$. As $f^{-1}\{x\}$ is compact (being closed in the compact space Γ^n), it is covered by the subsets $g(V_g)^n$, where g runs over some finite subset F_x of $f^{-1}\{x\}$. The subgroup $U''_x = \bigcap_{g \in F_x} V_g$ is open and normal in Γ, and so is $U'' = \bigcap_{x \in Y} U''_x$ (recall that Y is finite). Then the right action of $(U'')^n$ on Γ^n stabilises the subset $f^{-1}\{x\}$ for each $x \in X$, which means that f factors through $\Gamma^n \to \Gamma^n/(U'')^n = (\Gamma/U'')^n$. Setting $U = U' \cap U''$ concludes the proof. □

3. Infinite Galois extensions

In this chapter, we review some aspects of Galois theory, and show that the Galois group is an example of a profinite group. The only nontrivial fact that we will use without proof is the existence of algebraic closures.

When A, B are k-algebras, we will denote by $\mathrm{Hom}_{k-\mathrm{alg}}(A, B)$ the set morphisms of k-algebras $A \to B$. The group of automorphisms of a k-algebra A will be denoted by $\mathrm{Aut}_{k-\mathrm{alg}}(A)$.

Lemma 4.3.1. *Let L/k and F/k be field extensions.*

(i) If L/k is algebraic, and F is algebraically closed, then $\mathrm{Hom}_{k-\mathrm{alg}}(L, F) \neq \varnothing$.
(ii) If L/k is finite, then $|\mathrm{Hom}_{k-\mathrm{alg}}(L, F)| \leq [L : k]$.
(iii) If L/k is finite separable, and F is algebraically closed, then $|\mathrm{Hom}_{k-\mathrm{alg}}(L, F)| = [L : k]$.

Proof. (i) : Consider the set of pairs (K, σ) where K/k is a subextension of L/k, and $\sigma\colon K \to F$ a k-algebra morphism. It is partially ordered by letting $(K, \sigma) \leq (K', \sigma')$ when $K \subset K'$ and $\sigma'|_K = \sigma$. It is easy to see that every totally ordered subset admits an upper bound. By Zorn's lemma, we find a maximal element (K, σ). Let $x \in L$, and $P \in K[X]$ be the minimal polynomial of x over K. Then P has a root y in the algebraically closed field F. The subextension E of L/K generated by x is isomorphic to $K[X]/P$, and mapping x to y induces a k-algebra morphism $E \to F$ extending σ. By maximality of (K, σ), we must have $K = E$, hence $x \in K$, and finally $L = K$.

(ii) and (iii) : We proceed by induction on $[L : k]$. Let $x \in L - k$, and $P \in k[X]$ the minimal polynomial of x over k. The subextension K of L/k generated by x is isomorphic to $k[X]/P$, and morphisms of k-algebras $K \to F$ correspond to roots of P in F. There are at most (resp. exactly, if L/k is separable and F is algebraically closed) $\deg P = [K : k]$

such roots. By induction each morphism of k-algebras $K \to F$ admits at most (resp. exactly) $[L : K]$ extensions to a morphism $L \to F$. There are thus at most (resp. exactly) $[L : K][K : k] = [L : k]$ morphisms of k-algebras $L \to F$. □

Recall that when a group G acts on a set X, we denote by X^G the set of elements of X fixed by every element of G.

Proposition 4.3.2. *Let L/k be a finite field extension. Let G be a subgroup of $\mathrm{Aut}_{k-\mathrm{alg}}(L)$ such that $L^G = k$. Then $G = \mathrm{Aut}_{k-\mathrm{alg}}(L)$ and $|G| = [L : k]$.*

Proof. We have $[L : k] \geq |\mathrm{Aut}_{k-\mathrm{alg}}(L)|$ by Lemma 4.3.1 (iii). In particular G is finite, and it will suffice to prove that $|G| \geq [L : k]$. Let M be the set of maps $G \to L$, viewed as an k-vector space via pointwise operations. Consider the k-linear map $\varphi\colon L \otimes_k L \to M$ sending $x \otimes y$ to the map $g \mapsto xg(y)$. Assume that the kernel of φ contains a nonzero element $v = x_1 \otimes y_1 + \cdots + x_r \otimes y_r$, where $x_1, \ldots, x_r, y_1, \ldots, y_r \in L$. Choose r minimal with this property. Then $x_1, \ldots, x_r$ are linearly independent over k. Replacing v with $(1 \otimes y_1^{-1})v$, we may assume that $y_1 = 1$. Since the elements $x_1, \ldots, x_r$ are linearly independent over k and $0 = \varphi(v)(\mathrm{id}_L) = x_1y_1 + \cdots + x_ry_r$, there exists $j \in \{2, \ldots, r\}$ such that y_j does not lie in k. As $k = L^G$, we may find $g \in G$ such that $g(y_j) \neq y_j$. The element $v' = x_1 \otimes g(y_1) + \cdots + x_r \otimes g(y_r)$ also lies in the kernel of φ, hence so does

$$v - v' = \sum_{i=1}^{r} x_i \otimes y_i - \sum_{i=1}^{r} x_i \otimes g(y_i) = \sum_{i=2}^{r} x_i \otimes (y_i - g(y_i)).$$

This element is nonzero, because $x_2, \ldots, x_r$ are linearly independent over k and $y_j - g(y_j) \neq 0$. We have obtained a contradiction with the minimality of r. This proves that φ is injective, so that

$$[L : k]^2 = \dim_k L \otimes_k L \leq \dim_k M = |G| \cdot [L : k],$$

and thus $|G| \geq [L : k]$, as required. □

Recall that an algebraic extension L/k is called *normal* if the minimal polynomial over k of every element of L splits into a product of linear factors over L.

Lemma 4.3.3. *Let L/k be a normal field extension and F/k a field extension. Then all morphisms of k-algebras $L \to F$ have the same image.*

Proof. Let $\mathcal{P} \subset k[X]$ be the set of minimal polynomials over k of elements of L, and E be the set of roots in F of the elements of $\mathcal{P}$. We prove that E is the common image. Let $\sigma\colon L \to F$ be a k-algebra morphism. If $x \in L$, then $\sigma(x) \in F$ is a root of the minimal polynomial of x over k, proving that $\sigma(L) \subset E$. Conversely, let $y \in E$, and pick $P \in \mathcal{P}$ such that $P(y) = 0$. As L/k is normal, we may find $x_1, \ldots, x_n \in L$ such that $P = (X - x_1) \cdots (X - x_n)$ in $L[X]$, hence

$$0 = \sigma(P(y)) = (\sigma(P))(y) = (y - \sigma(x_1)) \cdots (y - \sigma(x_n)) \in F,$$

so that $y = \sigma(x_i)$ for some $i \in \{1, \ldots, n\}$. Thus $E \subset \sigma(L)$. □

Proposition 4.3.4. *Let F/k be an algebraic field extension. The following are equivalent:*

(i) The extension F/k is separable and normal,
(ii) $F^{\mathrm{Aut}_{k-\mathrm{alg}}(F)} = k$.

Proof. (i) $\Rightarrow$ (ii) : Let $x \in F - k$, and P the minimal polynomial of x over k. The polynomial P splits into a product of linear factors over F (as F/k is normal), and has no multiple root (as F/k separable). Since P has degree at least two, we find $y \in F$ such that $y \neq x$ and $P(y) = 0$. Let K be the subfield of F generated by x over k, and $\overline{F}$ be an algebraic closure of F. The morphism of k-algebras $k[X]/P \to K$ given by $X \mapsto x$ is an isomorphism, hence we can define a morphism of k-algebras $K \to \overline{F}$ by $x \mapsto y$. That morphism extends to a morphism $F \to \overline{F}$ by Lemma 4.3.1 (i), whose image equals F by Lemma 4.3.3. We have thus found $\sigma \in \mathrm{Aut}_{k-\mathrm{alg}}(F)$ such that $\sigma(x) = y \neq x$, proving (ii).

(ii) $\Rightarrow$ (i) : Let $x \in F$. Let S be the set of those $\sigma(x) \in F$, where σ runs over $\mathrm{Aut}_{k-\mathrm{alg}}(F)$. The elements of S are among the roots of the minimal polynomial of x over k, and in particular S is finite. Consider the polynomial

$$P = \prod_{s \in S} (X - s) \in F[X].$$

Every $\sigma \in \mathrm{Aut}_{k-\mathrm{alg}}(F)$ permutes the elements of S, so that

$$\sigma(P) = \prod_{s \in S} (X - \sigma(s)) = \prod_{s \in S} (X - s) = P.$$

Thus $P = (F[X])^{\mathrm{Aut}_{k-\mathrm{alg}}(F)} = (F^{\mathrm{Aut}_{k-\mathrm{alg}}(F)})[X] = k[X]$. The minimal polynomial of x over k divides P, hence also splits into a product of pairwise distinct monic linear factors over F. □

Definition 4.3.5. An algebraic field extension F/k is called *Galois* if it satisfies the conditions of Proposition 4.3.4. Its *Galois group* $\mathrm{Gal}(F/k)$ is defined as the group $\mathrm{Aut}_{k-\mathrm{alg}}(F)$.

Lemma 4.3.6. *If F/k is a Galois extension and E a subextension of F/k, then the extension F/E is Galois.*

Proof. Let $x \in F$, and $P \in k[X]$, resp. $Q \in E[X]$, be the minimal polynomial of x over k, resp. E. Then Q divides P in $F[X]$, hence also splits into a product of pairwise distinct monic linear factors over F. □

Lemma 4.3.7. *Let F/k be a Galois extension, and E/k a Galois subextension of F/k. Then every element of* $\mathrm{Gal}(F/k)$ *restricts to an element of* $\mathrm{Gal}(E/k)$*, and the induced morphism* $\mathrm{Gal}(F/k) \to \mathrm{Gal}(E/k)$ *is surjective.*

Proof. Let $\sigma \in \mathrm{Gal}(F/k)$. Then $\sigma(E) = E$ by Lemma 4.3.3, proving the first statement. Let now $\tau \in \mathrm{Gal}(E/k)$. Let $\overline{F}$ be an algebraic closure of F. Then the morphism $E \xrightarrow{\tau} E \subset \overline{F}$ extends to a morphism of k-algebras $F \to \overline{F}$ by Lemma 4.3.1 (i), whose image equals F by Lemma 4.3.3. We have thus extended τ to an element of $\mathrm{Gal}(F/k)$. □

Lemma 4.3.8. *Let F/k be a Galois extension. Then every finite subset of F is contained in a finite Galois subextension of F/k.*

Proof. For any $x \in F$, the elements $\sigma(x) \in F$ for $\sigma \in \mathrm{Gal}(F/k)$ are roots of the minimal polynomial of x over k, hence are in finite number. Thus, if S is a finite subset of F, the subextension L/k of F/k generated by the elements $\sigma(x)$, for $x \in S$ and $\sigma \in \mathrm{Gal}(F/k)$, is finite. Since the extension F/k is Galois, for every $y \in L - k$ we may find $\sigma \in \mathrm{Gal}(F/k)$ such that $\sigma(y) \neq y$ (Proposition 4.3.4). But $\sigma(L) = L$ by construction

of L, hence σ restricts to an element of $\mathrm{Aut}_{k-\mathrm{alg}}(L)$. This proves that the extension L/k is Galois (Proposition 4.3.4). □

Proposition 4.3.9. *Let F/k be a Galois extension. The groups $\mathrm{Gal}(L/k)$, where L/k runs over the finite Galois subextensions of F/k (ordered by inclusion) form an inverse system of groups, whose inverse limit is isomorphic to $\mathrm{Gal}(F/k)$.*

Proof. Let $\mathcal{F}$ be the set of finite Galois subextensions of F/k. If $L, L' \in \mathcal{F}$, then we may find $L'' \in \mathcal{F}$ such that $L \subset L''$ and $L' \subset L''$ by Lemma 4.3.8. The morphisms $\mathrm{Gal}(L'/k) \to \mathrm{Gal}(L/k)$ for $L, L' \in \mathcal{F}$ with $L \subset L'$ are given by restricting automorphisms (see Lemma 4.3.7).

By Lemma 4.3.8 the field F is the union of the fields $L \in \mathcal{F}$. Therefore an automorphism of F is the identity if and only if it restricts to the identity on each $L \in \mathcal{F}$. This implies the injectivity of the natural morphism (see Lemma 4.3.7)

$$\mathrm{Gal}(F/k) \to \varprojlim \mathrm{Gal}(L/k) \subset \prod_{L \in \mathcal{F}} \mathrm{Gal}(L/k).$$

Let now $\sigma^L \in \mathrm{Gal}(L/k)$ be a family of elements representing an element of $\varprojlim \mathrm{Gal}(L/k)$. Let $x \in F$. By Lemma 4.3.8, there exists $L \in \mathcal{F}$ such that $x \in L$. Moreover, if another extension $L' \in \mathcal{F}$ contains x, then there exists an extension $L'' \in \mathcal{F}$ containing L and L', so that $\sigma^L(x) = \sigma^{L''}(x) = \sigma^{L'}(x)$. Therefore $\sigma^L(x) \in F$ does not depend on the choice of the extension $L \in \mathcal{F}$ containing x. We have thus defined a map $\sigma \colon F \to F$ restricting to σ^L for each finite Galois subextension L/k of F/k. It is easy to verify that σ is indeed an automorphism of the k-algebra F. □

Definition 4.3.10. Let F/k be a Galois extension. By Proposition 4.3.9 the group $\mathrm{Gal}(F/k)$ is profinite. The corresponding topology is called the *Krull topology.*

Theorem 4.3.11 (Krull). *The associations*

$$E \mapsto \mathrm{Gal}(F/E) \quad ; \quad H \mapsto F^H$$

yield inclusion-reversing, mutually inverse bijections between subextensions E of F/k and closed subgroups H of $\mathrm{Gal}(F/k)$. If E is a subextension of F/k, then

(i) the subgroup $\mathrm{Gal}(F/E)$ is open if and only if E/k is finite,
(ii) the subgroup $\mathrm{Gal}(F/E)$ is normal if and only if E/k is Galois.

Proof. Let E be a subextension of F/k. By Lemma 4.3.6 we have $F^{\mathrm{Gal}(F/E)} = E$. If E/k is finite, it is contained in a finite Galois subextension E' of F/k by Lemma 4.3.8. The subgroup $\mathrm{Gal}(F/E)$ is then open in $\mathrm{Gal}(F/k)$, hence also closed, because it is the preimage of $\mathrm{Gal}(E'/E)$ under the projection $\mathrm{Gal}(F/k) \to \mathrm{Gal}(E'/k)$ (by definition of the topology). When the subextension E is arbitrary (not necessarily finite), it is the union of its finite subextensions, so that $\mathrm{Gal}(F/E)$ is an intersection of closed subgroups in $\mathrm{Gal}(F/k)$, hence is closed.

Conversely, let $H \subset \mathrm{Gal}(F/k)$ be a closed subgroup. Let $E = F^H$. Then $H \subset \mathrm{Gal}(F/E)$. Assume $\sigma \in \mathrm{Gal}(F/E)$ does not belong to H. By Lemma 4.2.5 (i), the open complement of H in $\mathrm{Gal}(F/k)$ contains a subset of the $\sigma\,\mathrm{Gal}(F/L)$, where L is a finite Galois subextension of F/k. Let H' be the image of H under the morphism $\mathrm{Gal}(F/k) \to \mathrm{Gal}(L/k)$, and set $E' = L^{H'} = E \cap L$. The extension L/E' is Galois and $H' = \mathrm{Gal}(L/E')$ by Proposition 4.3.2. In particular we may find $h \in H$ such that

$h|_L = \sigma|_L \in \mathrm{Gal}(L/E')$. But then $h \in H \cap \sigma\,\mathrm{Gal}(F/L)$, contradicting the choice of L. We have proved that $H = \mathrm{Gal}(F/E)$.

Now assume that H is an open subgroup of $\mathrm{Gal}(F/k)$. By Lemma 4.2.5 (i), there exists a finite Galois subextension L of F/k such that $\mathrm{Gal}(F/L) \subset H$. Then F^H is contained in $F^{\mathrm{Gal}(F/L)} = L$, hence is finite.

If E is a Galois subextension of F/k, the subgroup $\mathrm{Gal}(F/E)$ is normal, being the kernel of the morphism $\mathrm{Gal}(F/k) \to \mathrm{Gal}(E/k)$. Conversely let H be a normal subgroup of $\mathrm{Gal}(F/k)$, and $E = F^H$. Let $x \in E$. Then for any $\sigma \in \mathrm{Gal}(F/k)$ and $h \in H$, the automorphism $\sigma^{-1} \circ h \circ \sigma \in \mathrm{Gal}(F/k)$ belongs to H, hence fixes x. Therefore

$$h \circ \sigma(x) = \sigma \circ \sigma^{-1} \circ h \circ \sigma(x) = \sigma(x),$$

proving that $\sigma(x) \in E$. Thus the subfield $E \subset F$ is stable under the action of $\mathrm{Gal}(F/k)$, so that $E^{\mathrm{Aut}_{k-\mathrm{alg}}(E)} \subset F^{\mathrm{Gal}(F/k)} = k$. It follows that the extension E/k is Galois (Proposition 4.3.4). □

In the sequel, the most important example of an infinite Galois extension will be the separable closure, which we discuss now. Recall that a field is called separably closed if it admits no nontrivial separable extension. An extension F/k is called a *separable closure* if it is separable and if F is separably closed. Such an extension always exists: we may take for F the set of separable elements in a given algebraic closure of k.

Lemma 4.3.12. *Let L/k and F/k be field extensions.*

(i) Assume that L is separable over k and that F is separably closed. Then there exists a morphism of k-algebras $L \to F$.

(ii) Assume that L is separably closed and that F is separable over k. Then any morphism of k-algebras $L \to F$ is an isomorphism.

Proof. (i) : Let $\overline{F}$ be an algebraic closure of F. By Lemma 4.3.1, we find a morphism of k-algebras $\sigma\colon L \to \overline{F}$. Let $x \in L$. Then x is a root of an irreducible separable polynomial in $k[X]$, and $\sigma(x) \in \overline{F}$ is a root of same polynomial. In particular $\sigma(x)$ is separable over k, hence belongs to F. Therefore $\sigma(L) \subset F$, proving (i).

(ii) : Since every element of F is separable over k, any morphism of k-algebras $L \to F$ is a separable extension, hence an isomorphism since L is separably closed. □

Proposition 4.3.13. *Every separable closure of k is a Galois extension.*

Proof. Let F be a separable closure of k, and $x \in F - k$. The minimal polynomial $P \in k[X]$ of x over k is separable of degree at least two. Its image in $F[X]$ thus possesses an irreducible factor Q such that $Q(x) \neq 0$. The field $F[X]/Q$ is a separable extension of F, hence equals F. It follows that $Q = X - y$ for some $y \in F$ distinct from x. Let K be the subextension of F/k generated by x. Then $X \mapsto x$ induces an isomorphism of k-algebras $k[X]/P \simeq K$, and we may thus define a morphism of k-algebras $K \to F$ mapping x to y. As F is separable over K, this morphism extends to a morphism of k-algebras $\sigma\colon F \to F$ by Lemma 4.3.12 (i), which is an isomorphism by Lemma 4.3.12 (ii). We have thus constructed $\sigma \in \mathrm{Aut}_{k-\mathrm{alg}}(F)$ such that $\sigma(x) \neq x$, proving that F is Galois (Proposition 4.3.4). □

Remark 4.3.14. By Lemma 4.3.12, a separable closure of k is unique up to an isomorphism of k-algebras. But by Proposition 4.3.13 and Proposition 4.3.4, such an

isomorphism is nonunique, unless k is separably closed. For this reason, we will usually fix a separable closure k_s of k.

Example 4.3.15. Let k be a finite field, and k_s a separable closure of k. Then k has positive characteristic p, and its cardinality q is a power of p. For each $n \in \mathbb{N} - \{0\}$, there is a unique subextension F_n of k_s/k having degree n, namely the set of roots of the polynomial $X^{q^n} - X \in k[X]$. This polynomial splits into distinct linear factors over F_n, hence F_n/k is Galois. The group $\mathrm{Gal}(F_n/k)$ is cyclic of order n, generated by the automorphism $x \mapsto x^q$. We deduce that (see Example 4.2.4)

$$\mathrm{Gal}(k_s/k) = \widehat{\mathbb{Z}}.$$

Bibliography

[Dra83] Peter 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] Tsi-Yuen 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`.