

# Galois cohomology

Olivier Haution

Ludwig-Maximilians-Universität München

Summer semester 2020

## Contents

Note on the literature	2
<b>Part 1. Noncommutative Algebra</b>	<b>3</b>
Chapter 1. Quaternion algebras	5
1. The norm form	5
2. Quadratic splitting fields	9
3. Biquaternion algebras	11
Chapter 2. Central simple algebras	15
1. Wedderburn's Theorem	15
2. The commutant	18
3. Skolem–Noether's Theorem	20
4. The index	21
5. Splitting fields	22
6. The Brauer group	25
<b>Part 2. Torsors</b>	<b>29</b>
Chapter 3. Galois descent	31
1. Profinite sets	31
2. Profinite groups	33
3. Infinite Galois extensions	36
4. Galois descent	40
Chapter 4. Étale and Galois algebras	43
1. Categories	43
2. Étale algebras	44
Bibliography	49

### Note on the literature

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

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

## Part 1

# Noncommutative Algebra



## CHAPTER 1

## Quaternion algebras

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

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

## 1. The norm form

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

We fix a base field  $k$ . A  $k$ -algebra is a (unital associative) ring  $A$  equipped with a structure of  $k$ -vector space such that the multiplication map  $A \times A \rightarrow A$  is  $k$ -bilinear. A morphism of  $k$ -algebras is a ring morphism which is  $k$ -linear. If  $A \neq 0$ , the map  $k \rightarrow A$  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  $a \in A$

$$(1.1.a) \quad \lambda a = (\lambda a)1 = a(\lambda 1) = a\lambda.$$

In this chapter on quaternion algebras, we will assume that the characteristic of  $k$  is not equal to two.

DEFINITION 1.1.1. Let  $a, b \in k^\times$ . We define a  $k$ -algebra  $(a, b)$  as follows. A basis of  $(a, b)$  as  $k$ -vector space is given by  $1, i, j, ij$ . The multiplication is determined by the rules

$$(1.1.b) \quad i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

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

LEMMA 1.1.2. Let  $A$  be a 4-dimensional  $k$ -algebra. If  $i, j \in A$  satisfy the relations (1.1.b) for some  $a, b \in k^\times$ , then  $A \simeq (a, b)$ .

PROOF. It will suffice to prove that the elements  $1, i, j, ij$  are linearly independent over  $k$ . Since  $i$  anticommutes with  $j$ , the elements  $1, i, j$  must be linearly independent. Now assume that  $ij = u + vi + wj$ , with  $u, v, w \in k$ . Then

$$0 = i(ij + ji) = i(ij) + (ij)i = i(u + vi + wj) + (u + vi + wj)i = 2ui + 2av,$$

hence  $u = v = 0$ . So  $ij = wj$ , hence  $ij^2 = wj^2$  and thus  $bi = bw$ , a contradiction.  $\square$

The following observations will be used without explicit mention.

LEMMA 1.1.3. *Let  $a, b \in k^\times$ . Then*

- (i)  $(a, b) \simeq (b, a)$ ,
- (ii)  $(a, b) \simeq (a\alpha^2, b\beta^2)$  for any  $\alpha, \beta \in k^\times$ .

PROOF. (i) : The isomorphism is given by exchanging  $i$  and  $j$ .

(ii) : The isomorphism is given by  $i \mapsto \alpha i$  and  $j \mapsto \beta j$ .  $\square$

LEMMA 1.1.4. *For any  $b \in k^\times$ , the  $k$ -algebra  $(1, b)$  is isomorphic to the algebra  $M_2(k)$  of 2 by 2 matrices with coefficients in  $k$ .*

PROOF. The matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, J = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \in M_2(k)$$

satisfy  $I^2 = 1, J^2 = b, IJ = -JI$ . Thus the statement follows from Lemma 1.1.2.  $\square$

From now on, the letter  $Q$  will denote a quaternion algebra over  $k$ .

DEFINITION 1.1.5. An element  $q \in Q$  such that  $q^2 \in k$  and  $q \notin k^\times$  will be called a *pure quaternion*.

LEMMA 1.1.6. *Let  $a, b \in k^\times$  and  $x, y, z, w \in k$ . The element  $x + yi + zj + wij$  in the quaternion algebra  $(a, b)$  is a pure quaternion if and only if  $x = 0$ .*

PROOF. This follows from the computation

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

LEMMA 1.1.7. *The subset  $Q_0 \subset Q$  of pure quaternions is a  $k$ -subspace, and we have  $Q = k \oplus Q_0$  as  $k$ -vector spaces.*

PROOF. Letting  $a, b \in k^\times$  be such that  $Q \simeq (a, b)$ , this follows from Lemma 1.1.6.  $\square$

It follows from Lemma 1.1.7 that every  $q \in Q$  may be written uniquely as  $q = q_1 + q_2$ , where  $q_1 \in k$  and  $q_2$  is a pure quaternion. We define the *conjugate of  $q$*  as  $\bar{q} = q_1 - q_2$ . The following properties are easily verified:

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

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

For all  $p, q \in Q$ , we have  $N(pq) = N(p)N(q)$  for all  $p, q \in Q$ . If  $a, b \in k^\times$  are such that  $Q = (a, b)$  and  $q = x + yi + zj + wij$  with  $x, y, z, w \in k$ , then

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

LEMMA 1.1.9. *An element  $q \in Q$  admits a two-sided inverse if and only if  $N(q) \neq 0$ .*

PROOF. If  $N(q) \neq 0$ , then  $q$  is a left inverse of  $N(q)^{-1}\bar{q}$ , hence a two-sided inverse by Remark 1.1.11. Conversely, if  $pq = 1$ , then  $N(p)N(q) = 1$ , hence  $N(q) \neq 0$ .  $\square$

We will give below a list of criteria for a quaternion algebra to be isomorphic to  $M_2(k)$ . In order to do so, we need some definitions.

DEFINITION 1.1.10. A ring (resp. a  $k$ -algebra)  $D$  is called *division* if it is nonzero and every nonzero element of  $D$  admits a two-sided inverse. Such rings are also called skew-fields in the literature.

REMARK 1.1.11. Let  $A$  be a finite-dimensional  $k$ -algebra and  $a \in A$ . We claim that a left inverse of  $a$  is automatically a two-sided inverse. Indeed, assume that  $u \in A$  satisfies  $ua = 1$ . Then the  $k$ -linear morphism  $A \rightarrow A$  given by  $x \mapsto ax$  is injective (as  $ax = 0$  implies  $x = uax = 0$ ), hence surjective by reasons of dimensions. In particular 1 lies in its image, hence there is  $v \in A$  such that  $av = 1$ . Then  $u = u(av) = (ua)v = v$ .

DEFINITION 1.1.12. Let  $A$  be a commutative finite-dimensional  $k$ -algebra. The (algebra) norm map  $N_{A/k}: A \rightarrow k$  is defined by mapping  $a \in A$  to the determinant of the  $k$ -linear map  $A \rightarrow A$  given by  $x \mapsto ax$ .

It follows from the multiplicativity of the determinant that  $N_{A/k}(ab) = N_{A/k}(a)N_{A/k}(b)$  for every  $a, b \in A$ .

When  $a \in k$ , we consider the field extension

$$k(\sqrt{a}) = \begin{cases} k & \text{if } a \text{ is a square in } k, \\ k[X]/(X^2 - a) & \text{if } a \text{ is not a square in } k. \end{cases}$$

In the second case, we will denote by  $\sqrt{a} \in k(\sqrt{a})$  the element corresponding to  $X$  (this element is determined only up to sign by the field extension  $k(\sqrt{a})/k$ ). Every element of  $k(\sqrt{a})$  is represented as  $x + y\sqrt{a}$  for uniquely determined  $x, y \in k$ , and

$$N_{k(\sqrt{a})/k}(x + y\sqrt{a}) = x^2 - ay^2.$$

PROPOSITION 1.1.13. Let  $a, b \in k^\times$ . The following are equivalent.

- (i)  $(a, b) \simeq M_2(k)$ .
- (ii)  $(a, b)$  is not a division ring.
- (iii) The quaternion norm map  $(a, b) \rightarrow k$  has a nontrivial zero.
- (iv) We have  $b \in N_{k(\sqrt{a})/k}(k(\sqrt{a}))$ .
- (v) There are  $x, y \in k$  such that  $ax^2 + by^2 = 1$ .
- (vi) There are  $x, y, z \in k$ , not all zero, such that  $ax^2 + by^2 = z^2$ .

PROOF. (i)  $\Rightarrow$  (ii) : The nonzero matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(k)$$

is not invertible.

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

(iii)  $\Rightarrow$  (iv) : We may assume that  $a$  is not a square in  $k$ . Let  $q = x + yi + zj + wij$  be a nontrivial zero of the norm map, where  $x, y, z, w \in k$ . Then by the formula (1.1.c)

$$0 = x^2 - ay^2 - bz^2 + abw^2,$$



hence  $x^2 - ay^2 = b(z^2 - aw^2)$ . Assume that  $z^2 - aw^2 = 0$ . Then  $z = w = 0$ , because  $a$  is not a square. Thus  $x^2 - ay^2 = 0$ , and for the same reason  $x = y = 0$ . Thus  $q = 0$ , a contradiction. Therefore  $z^2 - aw^2 \neq 0$ , and

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

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

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

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

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

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

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

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

DEFINITION 1.1.14. A quaternion algebra satisfying the conditions of Proposition 1.1.13 will be called *split* (observe that this does not depend on the choice of  $a, b \in k^\times$ ).

EXAMPLE 1.1.15. Assume that every element of  $k$  is a square. Then for every  $a, b \in k^\times$ , we have  $(a, b) \simeq (1, b) \simeq M_2(k)$  by Lemma 1.1.4. Therefore every quaternion  $k$ -algebra splits.

EXAMPLE 1.1.16. Assume that the field  $k$  is finite, with  $q$  elements. As the group  $k^\times$  is cyclic of order  $q - 1$ , there are exactly  $1 + (q - 1)/2$  squares in  $k$ . Thus the sets  $\{ax^2 | x \in k\}$  and  $\{1 - by^2 | y \in k\}$  both consist of  $1 + (q - 1)/2$  elements; as subsets of the set  $k$  having  $q$  elements, they must intersect. It follows from the criterion (v) in Proposition 1.1.13 that  $(a, b)$  splits. Therefore *every quaternion algebra over a finite field is split*.

EXAMPLE 1.1.17. Let  $k = \mathbb{R}$ . The quaternion algebra  $(-1, -1)$  is not split, by Proposition 1.1.13 (v). Since  $k^\times/k^{\times 2} = \{1, -1\}$ , and taking into account Lemma 1.1.4, we see that there are exactly two isomorphism classes of  $k$ -algebras, namely  $M_2(k)$  and  $(-1, -1)$ .

Let us record another useful consequence of the argument used to prove the implication (vi)  $\Rightarrow$  (i) in Proposition 1.1.13:

PROPOSITION 1.1.18. *Let  $a, b, c \in k^\times$ . If  $(a, c)$  is split, then  $(a, bc) \simeq (a, b)$ .*

PROOF. Since  $(a, c)$  is split, by Proposition 1.1.13 (iv) there are  $\alpha, \beta \in k$  such that  $c = \alpha^2 - a\beta^2$ . Let  $Q = (a, bc)$  with its standard generators  $i', j'$ . Set

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

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

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

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

PROPOSITION 1.1.19. *Let  $Q, Q'$  be quaternion algebras, with pure quaternion subspaces  $Q_0, Q'_0$ . Then  $Q \simeq Q'$  if and only if there is a  $k$ -linear map  $\varphi: Q_0 \rightarrow Q'_0$  such that  $\varphi(q)^2 = q^2 \in k$  for all  $q \in Q_0$ .*

PROOF. Let  $\psi: Q \rightarrow Q'$  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  $\varphi$  the restriction of  $\psi$ .

Conversely, let  $\varphi: Q_0 \rightarrow Q'_0$  be a  $k$ -linear map such that  $\varphi(q)^2 = q^2 \in k$  for all  $q \in Q_0$ . We may assume that  $Q = (a, b)$  with its standard generators  $i, j$ . We have  $\varphi(i)^2 = i^2 = a$  and  $\varphi(j)^2 = j^2 = b$ , and

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

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

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

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

PROOF. Let  $Q$  be a quaternion algebra and  $N: Q \rightarrow k$  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  $N|_k = \text{id}_k$ . So we have a decomposition  $N \simeq \langle 1 \rangle \perp (N|_{Q_0})$ . This quadratic form is nondegenerate (e.g. by (1.1.c)), hence a morphism  $\varphi$  as in Proposition 1.1.19 is automatically an isometry. The corollary follows, by Witt's cancellation Theorem (see for instance [Lam05, Theorem 4.2]).  $\square$

## 2. Quadratic splitting fields

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

LEMMA 1.2.2. *Every quaternion algebra is central.*

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

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

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

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

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

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

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

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

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

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

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

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

PROPOSITION 1.2.9. *Let  $a \in k^\times$  and  $Q$  be a quaternion algebra. Assume that  $a$  is not a square in  $k$ . Then the following are equivalent:*

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

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

(ii)  $\Rightarrow$  (iii) : If  $Q$  is split, then  $Q \simeq (1, a) \simeq (a, 1)$  by Lemma 1.1.4, and (iii) was observed in Remark 1.2.3. Thus we assume that  $Q$  is division. Then there are  $p, q \in Q$

not both zero such that  $N(p \otimes 1 + q \otimes \sqrt{a}) = 0$  by Proposition 1.1.13. Set  $r = p\bar{q} \in Q$ . In view of (1.2.a), we have

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

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

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

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  $k[X]/(X^2 - a) \rightarrow Q$ , and (iii) follows.

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

### 3. Biquaternion algebras

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

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

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

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

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

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

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

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

(i)  $\Rightarrow$  (ii) : We assume that (ii) does not hold, and show that  $Q \otimes_k Q'$  is division. In view of Lemma 1.1.4 none of the algebras  $Q, Q'$  is isomorphic to  $M_2(k)$ , so  $Q$  and  $Q'$  are division by Proposition 1.1.13. We may assume that  $Q' = (a, b)$  for some  $a, b \in k^\times$ , and consider the standard generators  $i, j \in Q'$ . 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

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

Assume that  $q_1 q_2 = q_2 q_1$ . Let  $K$  be the  $k$ -subalgebra of  $Q$  generated by  $q_1, q_2$ . We claim that if  $K \neq k$ , then  $K$  is a quadratic field extension of  $k$ . Indeed, this is true by Lemma 1.2.5 if  $q_1 \in k$ . Otherwise the  $k$ -subalgebra  $K_1$  of  $Q$  generated by  $q_1$  is a quadratic field extension of  $k$ , by the same lemma. If  $q_2 \notin K_1$ , then  $1, q_2$  is a  $K_1$ -basis of  $Q$ , so that  $K = Q$ . This is not possible since  $q_1$  and  $q_2$  commute (as  $Q$  is central). Thus  $q_2 \in K_1$ , and  $K = K_1$  is as required, proving the claim. 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  $x \in K \otimes_k Q'$  admits a left inverse.

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

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

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

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

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

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

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

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

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

Moreover every element of  $A$  commutes with every element of  $A'$ . Now, there are isomorphisms of  $k$ -algebras

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

The  $k$ -linear map  $f: A \otimes_k A' \rightarrow (a, b) \otimes_k (a, c)$  given by  $x \otimes y \mapsto xy = yx$  is a morphism of  $k$ -algebras; its image visibly contains the elements

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

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

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

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

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

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

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

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

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

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

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



## CHAPTER 2

## Central simple algebras

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

After extending scalars appropriately, any finite-dimensional central simple 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 algebra; such fields are called splitting fields. We prove the existence of a separable splitting field, a crucial technical result which will allow us to use Galois theory later on. The index of the algebra is an integer expressing how far is the algebra from being split. In this chapter we gather basic information concerning the behaviour of this invariant under field extensions.

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

## 1. Wedderburn's Theorem

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

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

**DEFINITION 2.1.3.** Let  $R$  be a ring. The *opposite ring*  $R^{\text{op}}$  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  $R^{\text{op}}$  is naturally a  $k$ -algebra.

Observe that:

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

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  $\text{End}_R(Re)^{\text{op}}$ .*

PROOF. Consider the ring morphism  $\varphi: S \rightarrow \text{End}_R(Re)^{\text{op}}$  sending  $s$  to the morphism  $x \mapsto xs$ . Observe that  $\varphi(s)(e) = s$  for any  $s \in S$ , hence  $\varphi$  is injective. If  $f: Re \rightarrow Re$  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  $\varphi$  is surjective.  $\square$

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

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

PROPOSITION 2.1.7. *Let  $R$  be a ring and  $n \in \mathbb{N} - 0$ .*

- (i) *If the ring  $R$  is simple, then so is  $M_n(R)$ .*
- (ii) *Assume that  $R$  is a division ring (resp. division  $k$ -algebra). Then  $M_n(R)$  possesses a minimal nonzero ideal. If  $I$  is any such ideal, then  $R \simeq \text{End}_{M_n(R)}(I)^{\text{op}}$ .*

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

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

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

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

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

and therefore  $I_r \subset Bm$ . We have proved that  $I_r$  is a simple  $B$ -module, or equivalently a minimal nonzero ideal of  $B$ . If  $I$  is any other such ideal, then there is a surjective morphism of  $B$ -modules  $B \rightarrow I$  (as  $I$  must be generated by a single element). Since the natural morphism  $I_1 \oplus \dots \oplus I_n \rightarrow B$  is surjective (as  $e_{i,j} = e_{i,j}e_{j,j} \in I_j$  for all  $i, j$ ),

the composite  $I_r \rightarrow I$  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  $R \rightarrow e_{r,r}Be_{r,r}$  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  $R \simeq \text{End}_B(I_r)^{\text{op}} \simeq \text{End}_B(I)^{\text{op}}$ .  $\square$

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

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

$$D \simeq \text{End}_{M_n(D)}(I)^{\text{op}} \simeq \text{End}_{M_m(E)}(J)^{\text{op}} \simeq E. \quad \square$$

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

**EXAMPLE 2.1.10.** Every finite-dimensional  $k$ -algebra is artinian.

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

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

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

Let now  $M$  be a finitely generated  $A$ -module. Then  $M$  is a quotient of  $A^{\oplus q}$  for some integer  $q$ , hence a quotient of  $S^{\oplus n}$  for some integer  $n$  (namely  $n = pq$ ). Choose  $n$  minimal with this property, and denote by  $N$  the kernel of the surjective morphism  $S^{\oplus n} \rightarrow M$ . For  $i = 1, \dots, n$ , denote by  $\pi_i: S^{\oplus n} \rightarrow S$  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  $S^{\oplus n-1} \rightarrow M$ , 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.  $\square$

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

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

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

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

## 2. The commutant

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

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

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

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

LEMMA 2.2.3. *The center of a simple ring is a field.*

PROOF. Let  $R$  be a simple ring, and  $x$  a nonzero element of  $\mathcal{Z}(R)$ . Then the two-sided ideal  $RxR$  of  $R$  is nonzero, hence  $RxR = R$ . Thus we may write  $1 = a_1xa'_1 + \cdots + a_nxa'_n$  with  $a_1, \dots, a_n, a'_1, \dots, a'_n \in R$ . Then the element  $y = a_1a'_1 + \cdots + a_na'_n$  is a two-sided inverse of  $x$  in  $R$ . For any  $r \in R$ , we have

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

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

LEMMA 2.2.4. *Let  $A, B$  be  $k$ -algebras, and  $A' \subset A$  a subalgebra. Then*

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

PROOF. Let  $C = \mathcal{Z}_{A \otimes_k B}(A' \otimes_k k)$ . Certainly  $\mathcal{Z}_A(A') \otimes_k B \subset C$ . Any element  $c \in C$  may be written as  $c = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$  with  $a_1, \dots, a_n \in A$  and  $b_1, \dots, b_n \in B$ . We may additionally assume that  $b_1, \dots, b_n$  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  $b_1, \dots, b_n$  implies that the  $k$ -subspaces  $A \otimes_k b_1k, \dots, A \otimes_k b_nk$  are in direct sum in  $A \otimes_k B$  (exercise), and we conclude that each  $a_i$  commutes with  $a'$ , proving the other inclusion.  $\square$

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

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

PROOF. Let  $C = \mathcal{Z}_{A \otimes_k B}(A' \otimes_k B')$ . Then  $C$  contains  $\mathcal{Z}_A(A') \otimes_k \mathcal{Z}_B(B')$ . Conversely by Lemma 2.2.4, the subalgebra  $C \subset A \otimes_k B$  is contained in

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

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

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

PROOF. Let  $I$  be a two-sided ideal of  $A$  such that  $I \neq A$ . Then the  $k$ -algebra  $C = A/I$  is nonzero. Consider the commutative diagram

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

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 morphism  $f \otimes \text{id}_B$  is injective. Since the left vertical morphism in the above diagram is also injective (exercise), it follows that  $f$  is injective, or equivalently that  $I = 0$ . This proves that  $A$  is simple (and so is  $B$  by symmetry).  $\square$

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

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

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

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

$$(1 \otimes b)i - i(1 \otimes b) = a_2 \otimes (bb_2 - b_2b) + \cdots + a_n \otimes (bb_n - b_nb) \in I.$$

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

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

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

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

**PROOF.** Combine Proposition 2.2.7, Proposition 2.2.5 and Proposition 2.2.6.  $\square$

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

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

**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*

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

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

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

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

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

- (i) The ring  $\mathcal{Z}_A(B)$  is simple.
- (ii) There exists a division  $k$ -algebra  $D$ , and integers  $n, r$  such that
$$\mathcal{Z}_A(B) \otimes_k A^{\text{op}} \simeq M_n(D^{\text{op}}) \quad ; \quad B \simeq M_r(D).$$
- (iii)  $(\dim_k B)(\dim_k \mathcal{Z}_A(B)) = \dim_k A$ .
- (iv)  $\mathcal{Z}_A(\mathcal{Z}_A(B)) = B$ .
- (v) The centers of  $B$  and  $\mathcal{Z}_A(B)$  coincide, as subsets of  $A$ .

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

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

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

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

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

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

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

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

hence  $a = bc$ .

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

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

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

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

### 3. Skolem–Noether's Theorem

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

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

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

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

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

$$\begin{aligned}\varphi(f(b)) &= \varphi((b \otimes 1)1) = (b \otimes 1)\varphi(1) = g(b)u, \\ \varphi(f(b)) &= \varphi((1 \otimes f(b))1) = (1 \otimes f(b))\varphi(1) = uf(b).\end{aligned}$$

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  $\varphi$  is injective. We conclude using Remark 1.1.11, or alternatively computing

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

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

#### 4. The index

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

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

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

**LEMMA 2.4.2.** *Every 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  $B \rightarrow B$  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  $b^{-1} = b' \in B$ .  $\square$

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

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

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

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

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

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

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

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

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

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

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

$$\text{ind}(A_L) = \text{ind}(D_L) \mid \deg(D_L) = \deg(D) = \text{ind}(A). \quad \square$$

## 5. Splitting fields

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PROOF. We may assume that  $A$  is division, and use the observation just above.  $\square$

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

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

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

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

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

PROOF. Proposition 2.5.6 yields

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

which implies that  $D_L$  is division.  $\square$

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

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

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

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



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

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

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

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

**PROOF.** Proposition 2.5.8 yields

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

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

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

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

Let now  $a \in D$  be such that  $a \notin \mathcal{Z}(D)$ . Consider the  $k$ -algebra automorphism  $\sigma: D \rightarrow D$  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  $\sigma^q = \text{id}$ . We thus have  $(\sigma - \text{id})^q = \sigma^q - \text{id} = 0$ , since  $k$  has characteristic  $p$ . Let  $f$  be the largest integer such that  $(\sigma - \text{id})^f \neq 0$ , and let  $c \in D$  be such that  $(\sigma - \text{id})^f(c) \neq 0$ . Since  $a \notin \mathcal{Z}(D)$ , we have  $\sigma \neq \text{id}$ , and thus  $f \geq 1$ . Let  $x = (\sigma - \text{id})^{f-1}(c)$  and  $y = (\sigma - \text{id})^f(c) = \sigma(x) - x$ . Since  $(\sigma - \text{id})^{f+1} = 0$ , 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.  $\square$

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

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

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

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

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

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

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

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

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

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

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

## 6. The Brauer group

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

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

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

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

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

EXAMPLE 2.6.3. It follows respectively from Corollary 2.5.11, Theorem 2.5.14 and Theorem 2.5.15 that:

- (i)  $\text{Br}(k) = 0$  when  $k$  is separably closed.
- (ii)  $\text{Br}(k) = 0$  when  $k$  is finite.
- (iii)  $\text{Br}(\mathbb{R}) = \mathbb{Z}/2$ .

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

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

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

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

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

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

We will use the following observation:

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

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

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

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

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

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

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

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

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

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



## **Part 2**

# **Torsors**



## CHAPTER 3

## Galois descent

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

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

## 1. Profinite sets

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

- a partially ordered set  $(A, \leq)$ ,
- for each  $\alpha \in A$  a set  $E_\alpha$ ,
- for each  $\alpha \leq \beta$  in  $A$  a map  $f_{\beta\alpha}: E_\beta \rightarrow E_\alpha$  (called *transition map*).

These data must satisfy the following conditions:

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

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

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

It is equipped with projections maps  $\pi_\alpha: E \rightarrow E_\alpha$  for every  $\alpha \in A$ , such that  $f_{\beta\alpha} \circ \pi_\beta = \pi_\alpha$  for all  $\alpha \leq \beta$ . It satisfies the following universal property: if  $s_\alpha: S \rightarrow E_\alpha$  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  $s: S \rightarrow E$  such that  $s_\alpha = \pi_\alpha \circ s$  for all  $\alpha \in A$ .

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

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



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

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

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

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

PROOF. Assume that each  $E_\alpha$  is nonempty. Let us define a subsystem as a collection of subsets  $T_\alpha \subset E_\alpha$  for each  $\alpha \in A$  such that  $f_{\beta\alpha}(T_\beta) \subset T_\alpha$  for each  $\alpha \leq \beta$ . Consider the set  $\mathcal{T}$  of all subsystems  $(T_\alpha)$  such that each  $T_\alpha$  is nonempty. We may order such subsystems by inclusion. Consider a totally ordered family of subsystems  $(T_\alpha)_i \in \mathcal{T}$ , for  $i \in I$ . For a fixed  $\alpha \in A$ , let us set  $S_\alpha = \bigcap_{i \in I} (T_\alpha)_i$ . Since each  $(T_\alpha)_i$  is nonempty, so is  $S_\alpha$  (here we use the finiteness of  $E_\alpha$ ), 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  $(T'_\alpha)$  defined by  $T'_\alpha = \bigcap_{\alpha \leq \beta} f_{\beta\alpha}(T_\beta)$ . Let  $\alpha \in A$ . Since  $T_\alpha$  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  $\beta \in A$  such that  $\beta_i \leq \beta$  for all  $i = 1, \dots, n$ . Then  $T'_\alpha$  contains the set  $f_{\beta\alpha}(T_\beta)$  which is nonempty, since  $T_\beta$  is nonempty. We have proved that  $(T'_\alpha) \in \mathcal{T}$ . By minimality of  $(T_\alpha)$ , we deduce that  $(T'_\alpha) = (T_\alpha)$ ; in other words the maps  $T_\beta \rightarrow T_\alpha$  for  $\alpha \leq \beta$  are surjective.

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

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

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

PROPOSITION 3.1.6. *Every profinite set is compact.*

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

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

Assume that  $F_\alpha = \emptyset$  for some  $\alpha \in A$ . Then  $E_\alpha$  is covered by subsets of the form  $V_i = f_{\alpha\alpha_i}^{-1}\{x_i\}$ . As  $E_\alpha$  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  $F_\alpha \neq \emptyset$  for each  $\alpha \in A$ . Then  $\varprojlim F_\alpha$  contains an element by Lemma 3.1.5. Its image in  $y \in E$  satisfies  $\pi_\alpha(y) \in F_\alpha \subset E_\alpha$  for all  $\alpha \in A$ , and in particular  $y$  belongs to no  $U_i$ . This contradicts the fact the the subsets  $U_i$  for  $i \in I$  cover  $E$ .  $\square$

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

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

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

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

## 2. Profinite groups

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

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

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

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

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

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

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

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

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

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

The next lemma shows that any profinite group admits a canonical representation as an inverse limit. We let  $\mathcal{U}$  be the set of open normal subgroups of  $\Gamma$ , ordered by letting  $U \leq V$  when  $V \subset U$ .

LEMMA 3.2.6. *The groups  $\Gamma/U$  for  $U \in \mathcal{U}$  form an inverse system of finite groups, whose inverse limit is isomorphic to  $\Gamma$ , as a topological group.*

PROOF. The finiteness of the groups  $\Gamma/U$  for  $U \in \mathcal{U}$  was observed in Lemma 3.2.5 (ii). Any pair of elements  $U, U' \in \mathcal{U}$  contain the common element  $U \cap U' \in \mathcal{U}$ . It follows that the groups  $\Gamma/U$  for  $U \in \mathcal{U}$  form an inverse system. Let  $\Gamma'$  be their inverse limit, and  $\pi_U: \Gamma' \rightarrow \Gamma/U$  the projection maps. The quotient morphisms  $q_U: \Gamma \rightarrow \Gamma/U$  induce a morphism  $\rho: \Gamma \rightarrow \Gamma'$  such that  $\pi_U \circ \rho = q_U$  for all  $U \in \mathcal{U}$ . For any such  $U$  and  $x \in U$ , the subset  $\rho^{-1}\pi_U^{-1}\{x\} = q_U^{-1}\{x\}$  is homeomorphic to  $U$ , hence open in  $\Gamma$ , showing that  $\rho$  is continuous. Conversely, there is a unique group morphism  $\theta: \Gamma' \rightarrow \Gamma$  such that  $\pi_\alpha \circ \theta = \pi_{U_\alpha}$  for all  $\alpha \in A$ . For all  $\alpha \in A$  and  $x \in \Gamma_\alpha$ , the subset  $\theta^{-1}\pi_\alpha^{-1}\{x\} = \pi_{U_\alpha}^{-1}\{x\}$  is open in  $\Gamma'$ , showing that  $\theta$  is continuous. Note that  $U \in \mathcal{U}$  contains the subgroup  $U_\alpha$  for some  $\alpha \in A$  (by Lemma 3.2.5 (i) with  $u = 1$ ), and that, letting  $p: \Gamma_\alpha \rightarrow \Gamma/U$  be the quotient map,

$$q_U \circ \theta = p \circ \pi_\alpha \circ \theta = p \circ \pi_{U_\alpha} = \pi_U.$$

Therefore  $\pi_U \circ \rho \circ \theta = \pi_U$  for all  $U \in \mathcal{U}$ , and  $\pi_\alpha \circ \theta \circ \rho = \pi_\alpha$  for all  $\alpha \in A$ . The universal property of the inverse limit then implies that  $\rho \circ \theta = \text{id}_{\Gamma'}$ , and  $\theta \circ \rho = \text{id}_\Gamma$ .  $\square$

DEFINITION 3.2.7. Let  $p$  be a prime. A  $p$ -group is finite group whose order is a power of  $p$ . A *pro- $p$ -group* is an inverse limit of  $p$ -groups. A subgroup  $P$  of  $\Gamma$  is called a *pro- $p$ -Sylow subgroup* if all the following conditions are satisfied:

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

Observe that a finite quotient of pro- $p$ -group is a  $p$ -group. Therefore if  $P$  is a pro- $p$ -Sylow subgroup of  $\Gamma$ , then the image of  $P$  in  $\Gamma/U$  is a  $p$ -group, for every open normal subgroup  $U$  of  $\Gamma$ .

PROPOSITION 3.2.8. *The profinite group  $\Gamma$  admits a pro- $p$ -Sylow subgroup.*

PROOF. By Lemma 3.2.6, we may identify  $\Gamma$  with  $\varprojlim (\Gamma/U)$  for  $U \in \mathcal{U}$ . For each  $U \in \mathcal{U}$  of  $\Gamma$ , let  $S_U$  be the set of  $p$ -Sylow subgroups of  $\Gamma/U$ , which is finite and nonempty by Sylow's Theorem. If  $U \leq V$  in  $\mathcal{U}$ , the map  $\Gamma/V \rightarrow \Gamma/U$  sends elements of  $S_V$  to elements of  $S_U$ , because the image of a  $p$ -Sylow subgroup under a surjective morphism is a  $p$ -Sylow subgroup (exercise). Thus the sets  $S_U$  form an inverse system, whose inverse limit  $S$  is nonempty by Lemma 3.1.5. Any element of  $S$  is represented by a collection of  $p$ -Sylow subgroups  $P_U \subset \Gamma/U$  for  $U \in \mathcal{U}$ , such that for any  $U \leq V$  in  $\mathcal{U}$  the morphism  $\Gamma/V \rightarrow \Gamma/U$  maps  $P_V$  onto  $P_U$ . The group  $P = \varprojlim P_U$  is naturally a subgroup of  $\Gamma$ ,

and is a pro- $p$ -group. Since  $P$  is the intersection in  $\Gamma$  of the preimages of  $P_U \subset \Gamma/U$  for  $U \in \mathcal{U}$  (by construction of the inverse limit), it is closed in  $\Gamma$ . It follows from Lemma 3.1.7 (applied to the system  $P_U$  for  $U \in \mathcal{U}$ ) that for each  $U \in \mathcal{U}$  the image of  $P$  in  $\Gamma/U$  is the  $p$ -Sylow subgroup  $P_U$ , and in particular has index prime to  $p$ .  $\square$

LEMMA 3.2.9. *Let  $X$  be a set with an action of the profinite group  $\Gamma$ . The following conditions are equivalent:*

- (i) *The action morphism  $\Gamma \times X \rightarrow X$  is continuous, for the discrete topology on  $X$ .*
- (ii) *Every element of  $X$  is fixed by an open subgroup of  $\Gamma$ .*
- (iii) *Every finite subset of  $X$  is elementwise fixed by an open subgroup of  $\Gamma$ .*

PROOF. (i)  $\Rightarrow$  (ii): Let  $x \in X$ , and  $U$  be the preimage of  $x$  under the map  $\Gamma \rightarrow E$  given by  $g \mapsto g \cdot x$ , which is continuous by (i). Then  $U$  is an open subgroup in  $\Gamma$ , hence has finite index by Lemma 3.2.5 (iii).

(ii)  $\Rightarrow$  (i): For  $x, y \in X$ , we denote by  $U_{x,y}$  the subset of  $\Gamma$  consisting of those elements  $\gamma$  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 3.2.5. Thus  $U_{x,y}$  is open, being either empty or homeomorphic to  $U_{x,x}$ . Now the preimage of any  $y \in X$  under the action morphism  $\Gamma \times X \rightarrow X$  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).

(ii)  $\Rightarrow$  (iii): Let  $F \subset X$  be a finite subset. Each  $f \in F$  is fixed by some open subgroup  $U_f$  of  $\Gamma$ . Then the open subgroup  $\bigcap_{f \in F} U_f$  of  $\Gamma$  fixes each element of  $F$ .

(iii)  $\Rightarrow$  (ii): Clear.  $\square$

DEFINITION 3.2.10. When the conditions of Lemma 3.2.9 are fulfilled, we say that  $\Gamma$  acts *continuously* on  $X$ , or that  $X$  is a  $\Gamma$ -set. A  $\Gamma$ -set equipped with a  $\Gamma$ -equivariant group structure will be called a  $\Gamma$ -group. A  $\Gamma$ -group whose underlying group is abelian will be called a  $\Gamma$ -module. A morphism of  $\Gamma$ -groups, resp.  $\Gamma$ -modules, is just a  $\Gamma$ -equivariant group morphism.

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 3.2.11. *Let  $X$  be a  $\Gamma$ -set and  $n$  an integer. Then every continuous map  $\Gamma^n \rightarrow X$  factors through a map  $(\Gamma/U)^n \rightarrow X^U$  for some open normal subgroup  $U$  of  $\Gamma$ .*

PROOF. Let  $f: \Gamma^n \rightarrow X$  be a continuous map, and  $Y \subset X$  its image. Since  $\Gamma^n$  is profinite set (the limit of the inverse system  $(\Gamma_\alpha)^n$ ), it is compact by Proposition 3.1.6. Therefore  $Y$  is compact. Being also discrete, the set  $Y$  is finite. Since  $X$  is a  $\Gamma$ -set, there is an open subgroup  $U'$  in  $\Gamma$  fixing all the elements of  $Y$ . Shrinking  $U'$ , we may assume that it is normal in  $\Gamma$  (by Lemma 3.2.5 (i) with  $u = 1$ ).

For each  $y \in Y$ , the preimage  $f^{-1}\{y\}$  is a nonempty open subset of  $\Gamma^n$ . Therefore there exists a nonempty open subset  $V_y$  of  $\Gamma$  such that  $(V_y)^n \subset f^{-1}\{y\}$ . By Lemma 3.2.5 (i), the subset  $V_y$  contains a subset of the form  $gU_y$ , where  $f(g) = y$  and  $U_y$  is an open normal subgroup of  $\Gamma$ . Then  $U'' = \bigcap_{y \in Y} U_y$  is an open normal subgroup of  $\Gamma$ . Setting  $U = U' \cap U''$  does the job.  $\square$

### 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.

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

LEMMA 3.3.1. *Let  $L/k$  and  $F/k$  be field extensions.*

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

PROOF. (i) : Consider the set of pairs  $(K, \sigma)$  where  $K/k$  is a subextension of  $L/k$ , and  $\sigma : K \rightarrow F$  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 a maximal element. By Zorn's lemma, we find a maximal element  $(K, \sigma)$ . Let  $x \in L$  and  $P$  be its minimal polynomial over  $k$ . Then  $P$  has a root  $y$  in  $F$ . 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  $E \rightarrow F$  extending  $\sigma$ . By maximality of  $(K, \sigma)$ , 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  $P$  its minimal polynomial. The subextension  $K$  of  $L/k$  generated by  $x$  is isomorphic to  $k[X]/P$ , and morphisms of  $k$ -algebras  $K \rightarrow F$  correspond to roots of  $P$  in  $F$ . There are at most (resp. exactly, if  $L/k$  is separable and  $F$  is algebraically closed)  $\deg P = [L : k]$  such roots. By induction each morphism of  $k$ -algebras  $K \rightarrow F$  admits at most (resp. exactly)  $[L : K]$  extensions to a morphism  $L \rightarrow F$ . There are thus at most (resp. exactly)  $[L : K][K : k] = [L : k]$  morphisms of  $k$ -algebras  $L \rightarrow F$ .  $\square$

PROPOSITION 3.3.2. *Let  $L/k$  be a finite field extension. Let  $G$  be a subgroup of  $\text{Aut}_{k\text{-alg}}(L)$  such that  $L^G = k$ . Then  $G = \text{Aut}_{k\text{-alg}}(L)$  and  $|G| = [L : k]$ .*

PROOF. We have  $[L : k] \geq |\text{Aut}_{k\text{-alg}}(L)|$  by Lemma 3.3.1 (ii). In particular  $G$  is finite, and it will suffice to prove that  $|G| \geq [L : k]$ . Let  $M$  be the set of maps  $G \rightarrow L$ , viewed as an  $k$ -vector space via pointwise operations. Consider the  $k$ -linear map  $\varphi : L \otimes_k L \rightarrow M$  sending  $x \otimes y$  to the map  $g \mapsto xg(y)$ . Assume that the kernel of  $\varphi$  contains a nonzero element  $v = x_1 \otimes y_1 + \cdots + x_r \otimes y_r$ , where  $x_1, \dots, x_r, y_1, \dots, y_r \in L$ . Choose  $r$  minimal with this property. Then  $x_1, \dots, x_r$  are linearly independent over  $k$ . Replacing  $v$  with  $(1 \otimes y_1^{-1})v$ , we may assume that  $y_1 = 1$ . Since  $0 = \varphi(v)(\text{id}_L) = x_1 y_1 + \cdots + x_r y_r$  and the elements  $x_1, \dots, x_r$  are linearly independent over  $k$ , there is  $j \in \{2, \dots, r\}$  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  $\varphi$ , 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  $x_2, \dots, x_r$  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

$\varphi$  is injective, so that

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

and  $|G| \geq [L : k]$ .  $\square$

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

LEMMA 3.3.3. *Let  $L/k$  be a normal field extension and  $F/k$  a field extension. Then all morphisms of  $k$ -algebras  $L \rightarrow F$  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  $\mathcal{P}$ . Let  $\sigma : L \rightarrow F$  be a  $k$ -algebra morphism. If  $x \in L$ , then  $\sigma(x) \in F$  is a root of the minimal polynomial of  $x$ , 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  $x_1, \dots, x_n \in L$  such that  $P = (X - x_1) \cdots (X - x_n)$  in  $L[X]$ , hence

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

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

PROPOSITION 3.3.4. *Let  $F/k$  be an algebraic field extension. The following are equivalent:*

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

PROOF. (i)  $\implies$  (ii) : Let  $P$  be the minimal polynomial of an element  $x \in F - k$ . The polynomial  $P$  splits into 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  $K \rightarrow \overline{F}$  given by  $x \mapsto y$  extends to a morphism  $F \rightarrow \overline{F}$  by Lemma 3.3.1 (i). The image of this morphism equals  $F$  by Lemma 3.3.3. We have thus found  $\sigma \in \text{Aut}_{k\text{-alg}}(F)$  such that  $\sigma(x) = y \neq x$ , proving (i).

(ii)  $\implies$  (i) : Let  $x \in F$ . Let  $S$  be the set of those  $\sigma(x)$ , where  $\sigma$  runs over  $\text{Aut}_{k\text{-alg}}(F)$ . 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

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

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

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

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

DEFINITION 3.3.5. An algebraic field extension  $F/k$  is called *Galois* if it satisfies the conditions of Proposition 3.3.4.

LEMMA 3.3.6. *Let  $F/k$  be a Galois extension, and  $E/k$  a Galois subextension of  $F/k$ . Then every element of  $\text{Gal}(F/k)$  restricts to an element of  $\text{Gal}(E/k)$ , and the induced morphism  $\text{Gal}(F/k) \rightarrow \text{Gal}(E/k)$  is surjective.*

PROOF. Let  $\sigma \in \text{Gal}(F/k)$ . Then  $\sigma(E) = E$  by Lemma 3.3.3, proving the first statement. Let now  $\tau \in \text{Gal}(E/k)$ . Let  $\bar{F}$  be an algebraic closure of  $F$ . Then the morphism  $E \xrightarrow{\tau} E \subset \bar{F}$  extends to a morphism of  $k$ -algebras  $F \rightarrow \bar{F}$  by Lemma 3.3.1 (i), whose image equals  $F$  by Lemma 3.3.3. We have thus extended  $\tau$  to an element of  $\text{Gal}(F/k)$ .  $\square$

LEMMA 3.3.7. *Let  $F/k$  be a Galois extension. Then every element of  $F$  is contained in a finite Galois subextension of  $F/k$ .*

PROOF. Let  $x \in F$ . The elements  $\sigma(x) \in F$  for  $\sigma \in \text{Gal}(F/k)$  are roots of the minimal polynomial of  $x$  over  $k$ , hence are in finite number. Let  $L$  be the subfield of  $F$  generated by these elements. Since  $F/k$  is Galois, for every  $y \in L - k$  we may find  $\sigma \in \text{Gal}(F/k)$  such that  $\sigma(y) \neq y$  (Proposition 3.3.4). But  $\sigma$  maps  $L$  to itself by construction of  $L$ , hence restricts to an element of  $\text{Aut}_{k\text{-alg}}(L)$ . This proves that  $L/k$  is Galois (Proposition 3.3.4).  $\square$

PROPOSITION 3.3.8. *Let  $F/k$  be a Galois extension. The groups  $\text{Gal}(L/k)$ , 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  $\text{Gal}(F/k)$ .*

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 3.3.7. The morphisms  $\text{Gal}(L'/k) \rightarrow \text{Gal}(L/k)$  for  $L \subset L' \in \mathcal{F}$  are given by restricting automorphisms (see Lemma 3.3.6).

By Lemma 3.3.7 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 3.3.6)

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

Let now  $\sigma^L \in \text{Gal}(L/k)$  be a family of elements representing an element of  $\varprojlim \text{Gal}(L/k)$ . Let  $x \in F$ . By Lemma 3.3.7, there exists  $L \in \mathcal{F}$  such that  $x \in L$ . Moreover, if  $L' \in \mathcal{F}$  contains  $x$ , there exists  $L'' \in \mathcal{F}$  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  $L \in \mathcal{F}$  containing  $x$ . We have thus defined a map  $\sigma: F \rightarrow F$  restricting to  $\sigma^L$  for each finite Galois extension  $L/k$ . It is easy to verify that  $\sigma$  is indeed an automorphism of the  $k$ -algebra  $F$ .  $\square$

DEFINITION 3.3.9. Let  $F/k$  be a Galois extension. By Proposition 3.3.8 the group  $\text{Gal}(F/k)$  is profinite, hence is endowed with a topology called the *Krull topology*.

THEOREM 3.3.10 (Krull). *The associations*

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

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

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

PROOF. Let  $E/k$  be a subextension of  $F/k$ . The extension  $F/E$  is separable and normal, hence  $F^{\text{Gal}(F/E)} = F$  by Proposition 3.3.4. Assume that  $E/k$  is finite. Then  $E$

is contained in a finite Galois subextension  $E'$  of  $F/k$  by Lemma 3.3.7. The subgroup  $\text{Gal}(F/E)$  is open in  $\text{Gal}(F/k)$ , hence also closed, because it is the preimage of  $\text{Gal}(E'/E)$  under the projection  $\text{Gal}(F/k) \rightarrow \text{Gal}(E'/k)$  (by definition of the topology). When  $E/k$  is arbitrary (not necessarily finite), it is the union of its finite subextensions, so that  $\text{Gal}(F/E)$  is an intersection of closed subgroups in  $\text{Gal}(F/k)$ , hence is closed.

Conversely, let  $H \subset \text{Gal}(F/k)$  be a closed subgroup. Let  $E = F^H$ . Then  $H \subset \text{Gal}(F/E)$ . Assume  $\sigma \in \text{Gal}(F/E)$  does not belong to  $H$ . By Lemma 3.2.5 (i), the open subset  $\text{Gal}(F/k) - H$  contains a subset of the  $\sigma \text{Gal}(F/L)$ , where  $L/k$  is a finite Galois subextension of  $F/k$ . Let  $H'$  be the image of  $H$  under the morphism  $\text{Gal}(F/k) \rightarrow \text{Gal}(L/k)$ , and set  $E' = L^{H'} = E \cap L$ . The extension  $L/E'$  is Galois, and  $H' = \text{Gal}(L/E')$  by Proposition 3.3.2. In particular we may find  $h \in H$  such that  $h|_L = \sigma|_L \in \text{Gal}(L/E')$ . But then  $h \in H \cap \sigma \text{Gal}(F/L)$ , a contradiction. We have proved that  $H = \text{Gal}(F/E)$ .

Now assume that  $H$  is an open subgroup of  $\text{Gal}(F/k)$ . By Lemma 3.2.5 (i), there exists a finite Galois subextension  $L$  of  $F/k$  such that  $\text{Gal}(F/L) \subset H$ . Then  $F^H$  is contained in  $F^{\text{Gal}(F/L)} = L$ , hence is finite.

If  $E/k$  is a Galois subextension, the subgroup  $\text{Gal}(F/E)$  is normal, being the kernel of the morphism  $\text{Gal}(F/k) \rightarrow \text{Gal}(E/k)$ . Conversely let  $H$  be a normal subgroup of  $\text{Gal}(F/k)$ , and  $E = F^H$ . Let  $x \in E$ . Then for any  $\sigma \in \text{Gal}(F/k)$  and  $h \in H$ , we have  $h \circ \sigma(x) = \sigma \circ \sigma^{-1} \circ h \circ \sigma(x) = \sigma(x)$  (as  $\sigma^{-1} \circ h \circ \sigma \in H$  fixes  $x$ ), proving that  $\sigma(x) \in E$ . Thus  $E$  is stable under the action of  $\text{Gal}(F/k)$ , and  $E^{\text{Aut}_k\text{-alg}(E)} \subset F^{\text{Gal}(F/k)} = k$ , so that  $E/k$  is Galois by Proposition 3.3.4.  $\square$

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

PROOF. (i): Let  $\bar{F}$  be an algebraic closure of  $F$ . By Lemma 3.3.1, we find a morphism of  $k$ -algebras  $L \rightarrow \bar{F}$ . Its image consists of elements which are separable over  $F$ , hence is contained in  $F$ . This proves (i).

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

PROPOSITION 3.3.12. *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 has a monic 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  $x$ , and consider the morphism of  $k$ -algebras  $K \rightarrow F$  mapping  $x$  to  $y$ . As  $F$  is separable over  $K$ , this morphism extends to a morphism of  $k$ -algebras  $\sigma: F \rightarrow F$  by Lemma 3.3.11 (i), which is an isomorphism by Lemma 3.3.11 (ii).



We have thus constructed  $\sigma \in \text{Aut}_{k\text{-alg}}(F)$  such that  $\sigma(x) \neq x$ , proving that  $F$  is Galois (Proposition 3.3.4).  $\square$

REMARK 3.3.13. By Lemma 3.3.11, a separable closure of  $k$  is unique up to isomorphism of  $k$ -algebras. But by Proposition 3.3.12 and Proposition 3.3.4, such isomorphism is nonunique, unless  $k$  is separably closed. For this reason, we will usually fix a separable closure  $k_s$  of  $k$ .

EXAMPLE 3.3.14. 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  $\text{Gal}(F_n/k)$  is cyclic of order  $n$ , generated by the automorphism  $x \mapsto x^q$ . We deduce that (see Example 3.2.4)

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

#### 4. Galois descent

In this section we fix a (possibly infinite) Galois extension  $F/k$ , and consider the profinite group  $\Gamma = \text{Gal}(F/k)$ . When  $\gamma \in \Gamma$  and  $\lambda \in F$ , we will write  $\gamma\lambda$  instead of  $\gamma(\lambda)$ .

Let us first formalise an argument that will be used repeatedly.

LEMMA 3.4.1. *Let  $U, W$  be  $k$ -vector spaces. Assume that a group  $G$  acts by  $k$ -linear automorphisms on  $U$ . Then the induced  $G$ -action on  $W \otimes_k U$  satisfies  $(W \otimes_k U)^G = W \otimes_k (U^G)$ .*

PROOF. Clearly  $W \otimes_k (U^G) \subset (W \otimes_k U)^G$ . Let now  $e_i$  for  $i \in I$  be a  $k$ -basis of  $W$ . For each  $i \in I$ , let  $e_i^*: W \rightarrow k$  be the linear map sending an element to its  $i$ -th coordinate in the above basis, and consider the  $k$ -linear map

$$\epsilon_i: W \otimes_k U \xrightarrow{e_i^* \otimes \text{id}_U} k \otimes_k U = U.$$

Then for any  $x \in W \otimes_k U$ , we have

$$x = \sum_{i \in I} e_i \otimes \epsilon_i(x).$$

Since each  $\epsilon_i$  is  $G$ -equivariant, it maps  $(W \otimes_k U)^G$  into  $U^G$ , and the statement follows.  $\square$

DEFINITION 3.4.2. Let  $V$  be an  $F$ -vector space. A  $\Gamma$ -action on  $V$  is called *semilinear* if for all  $v \in V$  and  $\lambda \in k$  and  $\gamma \in \Gamma$ , we have in  $V$

$$\gamma(\lambda v) = (\gamma\lambda)(\gamma v).$$

LEMMA 3.4.3. *Let  $W$  be a  $k$ -vector space. Then the  $\Gamma$ -action on  $W_F = W \otimes_k F$  via the second factor is semilinear and continuous. The subset  $(W_F)^\Gamma$  of  $W_F$  coincides with  $W = W \otimes_k k$ .*

PROOF. The semilinearity is clear, and the last statement follows from Lemma 3.4.1, since  $F^\Gamma = k$ . It only remains to prove the continuity. An arbitrary element  $w \in W_F$  is of the form  $w_1 \otimes \lambda_1 + \cdots + w_n \otimes \lambda_n$ , where  $w_1, \dots, w_n \in W$  and  $\lambda_1, \dots, \lambda_n \in F$ . By Lemma 3.3.7, the elements  $\lambda_1, \dots, \lambda_n$  are contained in some finite Galois subextension

$L/k$  of  $F/k$ . Then the subgroup  $\text{Gal}(F/L) \subset \Gamma$  is open in  $\Gamma$  (Theorem 3.3.10) and fixes  $w$ , proving the continuity (see Lemma 3.2.9).  $\square$

LEMMA 3.4.4 (Dedekind). *Let  $A$  be a  $k$ -algebra and  $K/k$  a field extension. Let  $\sigma_1, \dots, \sigma_n$  be pairwise distinct morphisms of  $k$ -algebras  $A \rightarrow K$ . Then the elements*

$$\sigma_1, \dots, \sigma_n \in \text{Hom}_{k\text{-alg}}(A, K) = \text{Hom}_{K\text{-alg}}(A_K, K) \subset \text{Hom}_K(A_K, K)$$

*are linearly independent over  $K$ . In particular  $n \leq \dim_k A$  when  $A$  is finite-dimensional.*

PROOF. Assume that

$$(3.4.a) \quad a_1\sigma_1 + \dots + a_m\sigma_m = 0.$$

where  $a_1, \dots, a_m \in K$  are not all zero. Pick such a relation, where  $m \in \{1, \dots, n\}$  is minimal. Then  $m \neq 1$  (as  $\sigma_1 \neq 0$ ), and there exists  $i \in \{1, \dots, m-1\}$  such that  $a_i \neq 0$  (as  $\sigma_m \neq 0$ ). Since  $\sigma_i \neq \sigma_m$ , we may find  $z \in A$  such that  $\sigma_i(z) \neq \sigma_m(z)$ . Since the maps  $\sigma_1, \dots, \sigma_m$  are multiplicative, it follows from (3.4.a) that

$$(3.4.b) \quad a_1\sigma_1(z)\sigma_1 + \dots + a_m\sigma_m(z)\sigma_m = 0.$$

Subtracting  $\sigma_m(z)$  times Equation (3.4.a) to (3.4.b) yields

$$a_1(\sigma_1(z) - \sigma_m(z))\sigma_1 + \dots + a_{m-1}(\sigma_{m-1}(z) - \sigma_m(z))\sigma_{m-1} = 0.$$

Since  $a_i(\sigma_i(z) - \sigma_m(z)) \neq 0$ , we have found a contradiction with the minimality of  $m$ .

The last statement follows from the fact that  $\dim_K \text{Hom}_K(A_K, K) = \dim_K A_K = \dim_k A$ .  $\square$

PROPOSITION 3.4.5 (Galois descent). *Let  $V$  be an  $F$ -vector space. If  $\Gamma$  acts continuously on  $V$  by semilinear automorphisms, then the natural morphism  $V^\Gamma \otimes_k F \rightarrow V$  is bijective.*

PROOF. Denote by  $\varphi$  the morphism  $V^\Gamma \otimes_k F \rightarrow V$ . The proof of the injectivity of  $\varphi$  is a recast of the proof of Proposition 3.3.2. Namely, assume that the kernel of  $\varphi$  contains a nonzero element  $v = v_1 \otimes \lambda_1 + \dots + v_r \otimes \lambda_r$  with  $v_i \in V^\Gamma$  and  $\lambda_i \in F$  for all  $i = 1, \dots, r$ . Choose  $r$  minimal with this property. Then  $v_1, \dots, v_r$  are linearly independent over  $k$ . Replacing  $v$  with  $\lambda_1^{-1}v$ , we may assume that  $\lambda_1 = 1$ . Since  $0 = \varphi(v) = \lambda_1 v_1 + \dots + \lambda_r v_r$  and the elements  $v_1, \dots, v_r$  are linearly independent over  $k$ , there is  $j \in \{2, \dots, r\}$  such that  $\lambda_j$  does not lie in  $k$ . Since  $k = F^\Gamma$ , we may find  $\gamma \in \Gamma$  such that  $\gamma\lambda_j \neq \lambda_j$ . By semilinearity of the  $\Gamma$ -action on  $V$ , the morphism  $\varphi$  is  $\Gamma$ -equivariant, hence  $\gamma v$  lies in the kernel of  $\varphi$ . Thus

$$v - \gamma v = \sum_{i=1}^r v_i \otimes \lambda_i - \sum_{i=1}^r v_i \otimes \gamma\lambda_i = \sum_{i=2}^r v_i \otimes (\lambda_i - \gamma\lambda_i)$$

is in the kernel of  $\varphi$ . This element is nonzero, because  $v_2, \dots, v_r$  are linearly independent over  $k$  and  $\lambda_j - \gamma\lambda_j \neq 0$ . We have obtained a contradiction with the minimality of  $r$ . This proves that  $\varphi$  is injective.

Conversely let  $v \in V$ . By continuity of the  $\Gamma$ -action on  $V$ , we may find a finite Galois extension  $L/k$  such that  $v$  is fixed by  $\text{Gal}(F/L)$  (see Lemma 3.2.9 and Theorem 3.3.10). Let  $e_1, \dots, e_n$  be a basis of the  $k$ -vector space  $L$ . The group  $\text{Gal}(L/F)$  has order  $n$  (by

Proposition 3.3.2), and by Lemma 3.3.6 we may find preimages  $\gamma_1, \dots, \gamma_n \subset \Gamma$  of the elements of  $\text{Gal}(L/k)$ . Consider the elements

$$(3.4.c) \quad w_j = \sum_{i=1}^n (\gamma_i e_j)(\gamma_i v) \in V \quad \text{for } j = 1, \dots, n.$$

Let  $\gamma \in \Gamma$ . Since  $\Gamma$  is the disjoint union of the subsets  $\gamma_1 \text{Gal}(F/L), \dots, \gamma_n \text{Gal}(F/L)$ , for each  $i \in \{1, \dots, n\}$  there is a unique  $p \in \{1, \dots, n\}$  such that  $\gamma_p^{-1} \gamma \gamma_i \in \Gamma$  belongs to the subgroup  $\text{Gal}(F/L)$ . Therefore, for every  $j \in \{1, \dots, n\}$ , we have

$$\gamma w_j = \sum_{i=1}^n (\gamma \gamma_i e_j)(\gamma \gamma_i v) = \sum_{p=1}^n (\gamma_p e_j)(\gamma_p v) = w_j,$$

proving that  $w_j \in V^\Gamma$ . The matrix  $(\gamma_i e_j)_{i,j} \in M_n(L)$  is invertible by Dedekind's Lemma 3.4.4. Let  $m_{i,j} \in L$  be the coefficients of its inverse. By (3.4.c), we have

$$\gamma_i v = \sum_{j=1}^n m_{i,j} w_j \quad \text{for } i = 1, \dots, n.$$

These elements lie in the image of  $\varphi$  (as each  $w_j$  belongs to  $V^\Gamma$ ). There is  $i \in \{1, \dots, n\}$  such that  $\gamma_i$  is the preimage of  $1 \in \text{Gal}(L/k)$ , hence belongs to  $\text{Gal}(F/L)$  and thus fixes  $v$ . Then  $v = \gamma_i v$  belongs to the image of  $\varphi$ .  $\square$

## CHAPTER 4

## Étale and Galois algebras

Étale algebras are generalisations of finite separable field extensions, and share many of their properties. The category of étale algebras has the advantage of being stable under extension of scalars, which provides a very useful flexibility lacking if one works only with separable extensions. In this chapter, we show that an étale algebra is the same thing as a finite set with a continuous action of the absolute Galois group. Shifting the point of view in this fashion will be central in the next chapter.

In the same spirit, Galois  $G$ -algebras, introduced at the end of this chapter, generalise finite Galois field extensions while being stable under extension of scalars. These algebras will provide a guiding example for the next chapter, since they constitute a simple type of torsors, objects which will figure prominently in the sequel.

This chapter begins with a brief introduction to the language of categories, which provides a suitable framework to express the above mentioned results.

By contrast with the previous ones, this chapter only deals with *commutative* algebras, and as such has a slightly different flavour. Its purpose is nonetheless to provide motivation to develop a more general theory of torsors, that will then be applied to the noncommutative case.

## 1. Categories

In this section, we briefly introduce a language that will permit a convenient formulation of certain results. We will not make a very extensive use of it, and so limit ourselves to very basic considerations leading to the notion of equivalence of categories.

DEFINITION 4.1.1. A *category*  $\mathcal{C}$  consists of the following data:

- (i) a class of objects,
- (ii) for each ordered pair of objects  $A, B$  a set of morphisms  $\text{Hom}_{\mathcal{C}}(A, B)$ ,
- (iii) a specified element  $\text{id}_A \in \text{Hom}_{\mathcal{C}}(A, A)$  for every  $A \in \text{Ob}(\mathcal{C})$ ,
- (iv) a map (called *composition law*)  $\text{Hom}_{\mathcal{C}}(A, B) \times \text{Hom}_{\mathcal{C}}(B, C) \rightarrow \text{Hom}_{\mathcal{C}}(A, C)$  denoted by  $(f, g) \mapsto g \circ f$ , for every objects  $A, B, C$ .

We write  $f: A \rightarrow B$  to indicate that  $f \in \text{Hom}_{\mathcal{C}}(A, B)$ . These data are subject to the following axioms

- (a)  $\text{id}_B \circ f = f = f \circ \text{id}_A$  for every  $f: A \rightarrow B$ ,
- (b)  $h \circ (g \circ f) = (h \circ g) \circ f$  for every  $f: A \rightarrow B, g: B \rightarrow C, h: C \rightarrow D$ .

A morphism  $f: A \rightarrow B$  in  $\mathcal{C}$  is called an *isomorphism* if there exists  $g: B \rightarrow A$  such that  $g \circ f = \text{id}_A$  and  $f \circ g = \text{id}_B$ .

REMARK 4.1.2. We will often write  $X \in \mathcal{C}$  to mean that  $X$  is an object of  $\mathcal{C}$ .

REMARK 4.1.3. The meaning of the word “class” in the above definition is left to the imagination of the reader. Observe that the objects do not necessarily form a set, for instance in the category **Sets** defined just below.

EXAMPLE 4.1.4. The category **Sets** is defined by letting its objects be the sets, its morphisms the maps of sets, the composition law is given by composition of maps. Similarly, one defines the category of groups (denoted by **Groups**), of abelian groups (denoted by **Ab**), of rings, of  $k$ -algebras,...

When  $\mathcal{B}, \mathcal{C}$  are categories, a *functor*  $\mathcal{F}: \mathcal{B} \rightarrow \mathcal{C}$  is the data of an object  $\mathcal{F}(B) \in \mathcal{C}$  for every object  $B \in \mathcal{B}$ , and a morphism  $\mathcal{F}(f): \mathcal{F}(B) \rightarrow \mathcal{F}(B')$  in  $\mathcal{C}$  for every morphism  $f: B \rightarrow B'$  in  $\mathcal{B}$ , subject to the following conditions:

- (a)  $\mathcal{F}(\text{id}_B) = \text{id}_{\mathcal{F}(B)}$  for every  $B \in \mathcal{B}$ ,
- (b)  $\mathcal{F}(g) \circ \mathcal{F}(f) = \mathcal{F}(g \circ f)$  for every  $f: B \rightarrow B'$  and  $g: B' \rightarrow B''$  in  $\mathcal{B}$ .

When  $\mathcal{B} = \mathcal{C}$ , setting  $\mathcal{F}(B) = B$  and  $\mathcal{F}(f) = f$  for all  $B$  and  $f$  as above defines a functor  $\text{id}_{\mathcal{B}}: \mathcal{B} \rightarrow \mathcal{B}$ .

If  $\mathcal{F}, \mathcal{G}: \mathcal{B} \rightarrow \mathcal{C}$  are functors, a *morphism of functors* (or natural transformation)  $\varphi: \mathcal{F} \rightarrow \mathcal{G}$  is the data of a morphism  $\varphi_B: \mathcal{F}(B) \rightarrow \mathcal{G}(B)$  in  $\mathcal{C}$  for every  $B \in \mathcal{B}$  such that for every morphism  $f: B \rightarrow B'$  in  $\mathcal{B}$ , we have

$$\mathcal{G}(f) \circ \varphi_B = \varphi_{B'} \circ \mathcal{F}(f).$$

When  $\mathcal{F} = \mathcal{G}$ , setting  $\varphi_B = \text{id}_{\mathcal{F}(B)}$  for all  $B \in \mathcal{B}$  defines a morphism of functors  $\text{id}_{\mathcal{F}}: \mathcal{F} \rightarrow \mathcal{F}$ . Morphisms of functors can be composed in an obvious way. A morphism of functors  $\varphi: \mathcal{F} \rightarrow \mathcal{G}$  is called an *isomorphism* if there is a morphism of functors  $\psi: \mathcal{G} \rightarrow \mathcal{F}$  such that  $\psi \circ \varphi = \text{id}_{\mathcal{F}}$  and  $\varphi \circ \psi = \text{id}_{\mathcal{G}}$ . Observe that  $\varphi$  is an isomorphism if and only if each  $\varphi_B$  for  $B \in \mathcal{B}$  is an isomorphism in  $\mathcal{C}$ .

An *equivalence of categories*  $\mathcal{B} \simeq \mathcal{C}$  is the data of a pair of functors  $\mathcal{F}: \mathcal{B} \rightarrow \mathcal{C}$  and  $\mathcal{G}: \mathcal{C} \rightarrow \mathcal{B}$  together with a pair of isomorphisms of functors  $\text{id}_{\mathcal{B}} \rightarrow \mathcal{G} \circ \mathcal{F}$  and  $\text{id}_{\mathcal{C}} \rightarrow \mathcal{F} \circ \mathcal{G}$ .

Given a category  $\mathcal{C}$ , the *opposite category*  $\mathcal{C}^{\text{op}}$  is defined as follows. The objects of  $\mathcal{C}^{\text{op}}$  are the objects of  $\mathcal{C}$ , and  $\text{Hom}_{\mathcal{C}^{\text{op}}}(A, B) = \text{Hom}_{\mathcal{C}}(B, A)$  for every  $A, B \in \mathcal{C}$ . If  $A \in \mathcal{C}$  the morphism  $\text{id}_A \in \text{Hom}_{\mathcal{C}^{\text{op}}}(A, A)$  corresponds to the morphism  $\text{id}_A \in \text{Hom}_{\mathcal{C}}(A, A)$ . Composition of morphisms is defined by the map

$$\text{Hom}_{\mathcal{C}^{\text{op}}}(A, B) \times \text{Hom}_{\mathcal{C}^{\text{op}}}(B, C) = \text{Hom}_{\mathcal{C}}(B, A) \times \text{Hom}_{\mathcal{C}}(C, B) \rightarrow \text{Hom}_{\mathcal{C}}(C, A) = \text{Hom}_{\mathcal{C}^{\text{op}}}(A, C)$$

where the middle map is the composition map in  $\mathcal{C}$ .

A *contravariant functor*  $\mathcal{B} \rightarrow \mathcal{C}$  is a functor  $\mathcal{B}^{\text{op}} \rightarrow \mathcal{C}$ . We define in an obvious way the notions of morphism of contravariant functors, contravariant equivalence of categories,...

## 2. Étale algebras

Let us fix a separable closure  $k_s$  of  $k$ . Let  $A$  be a  $k$ -algebra. We define

$$\mathbf{X}(A) = \text{Hom}_{k\text{-alg}}(A, k_s) = \text{Hom}_{k_s\text{-alg}}(A_{k_s}, k_s).$$

REMARK 4.2.1. By Proposition 3.3.12 (i), the set  $\mathbf{X}(A)$  does not depend, up to bijection, on the choice of  $k_s$ . In particular the integer  $|\mathbf{X}(A)|$  does not depend on this choice.

LEMMA 4.2.2. *We have  $|\mathbf{X}(A)| \leq \dim_k A$ .*

PROOF. This follows from Dedekind's Lemma 3.4.4.  $\square$

DEFINITION 4.2.3. A commutative  $k$ -algebra  $A$  is called *étale* if it is finite-dimensional and  $|\mathbf{X}(A)| = \dim_k A$ . A morphism of étale  $k$ -algebras is just a morphism of  $k$ -algebras between étale algebras. This yields the category of étale  $k$ -algebras  $\mathbf{Et}_k$ .

LEMMA 4.2.4. *Let  $K/k$  be a field extension. Then the  $k$ -algebra  $K$  is étale if and only if the extension  $K/k$  is finite separable.*

PROOF. If  $K$  is étale, then  $\mathbf{X}(K) \neq \emptyset$ , hence  $K$  can be embedded in  $k_s$  over  $k$ , which implies that  $K/k$  is separable. Conversely, let  $K$  be a separable field extension of  $k$ . Let  $F$  be an algebraic closure of  $k_s$ . There are  $[K : k]$  distinct morphisms of  $k$ -algebras  $K \rightarrow F$  by Lemma 3.3.1 (iii). Any element of the image of such a morphism is separable over  $k$ , hence belongs to  $k_s$ . We have thus produced  $[K : k]$  distinct elements of  $\mathbf{X}(K)$ .  $\square$

LEMMA 4.2.5. *Let  $L/k$  be a field extension and  $A$  an étale  $k$ -algebra. Then the  $L$ -algebra  $A_L$  is étale.*

PROOF. Let  $L_s$  be a separable closure of  $L$ . By Lemma 3.3.11 (i) there is a morphism of  $k$ -algebras  $k_s \rightarrow L_s$ . Such a morphism is injective, hence distinct morphisms  $A \rightarrow k_s$  give rise to distinct morphisms  $A_L \rightarrow k_s \rightarrow L_s$ . So  $|\mathbf{X}(A_L)| = |\mathbf{X}(A)| = \dim_k A = \dim_L A_L$ .  $\square$

LEMMA 4.2.6. *If  $k$  is separably closed, then every étale  $k$ -algebra is isomorphic to  $k^n$  for some integer  $n$ .*

PROOF. Assume that  $A$  is an étale  $k$ -algebra of dimension  $n$ , and let  $f_1, \dots, f_n$  be the pairwise distinct elements of  $\mathbf{X}(A)$ . By Dedekind's Lemma 3.4.4, these elements are linearly independent over  $k$ , hence generate the  $n$ -dimensional  $k$ -vector space  $\text{Hom}_k(A, k)$ . In particular the intersection of their kernels is zero. Thus the morphism of  $k$ -algebras  $A \rightarrow k^n$  given by  $a \mapsto (f_1(a), \dots, f_n(a))$  is injective, hence bijective by dimensional reasons.  $\square$

Recall that an element  $r$  of a ring  $R$  is called *nilpotent* if  $r^n = 0$  for some integer  $n$ , and that the ring  $R$  is called *reduced* if it contains no nonzero nilpotent element.

REMARK 4.2.7. Let  $R, S$  be rings. Then  $R \times S$  is reduced if and only if  $R$  and  $S$  are reduced. Indeed a pair of nonzero nilpotent elements of  $R$  and  $S$  give rise to a nonzero nilpotent element of  $R \times S$ . Conversely, if  $r \in R$  (resp.  $s \in S$ ) is nonzero nilpotent, then  $(r, 0) \in R \times S$  (resp.  $(0, s) \in R \times S$ ) is so.

LEMMA 4.2.8. *An étale  $k$ -algebra is reduced.*

PROOF. If  $x$  is a nilpotent element of  $A$ , every  $k$ -algebra morphism  $A \rightarrow k_s$  factors uniquely through  $A \rightarrow A/xA$ . In other words, the map  $\mathbf{X}(A/xA) \rightarrow \mathbf{X}(A)$  is bijective. If  $x \neq 0$ , then

$$|\mathbf{X}(A)| = |\mathbf{X}(A/xA)| \leq \dim_k(A/xA) < \dim_k A,$$

and  $A$  is not étale.  $\square$

LEMMA 4.2.9. *Let  $A, B$  be finite-dimensional  $k$ -algebras.*

(i) *We have  $\mathbf{X}(A \times B) = \mathbf{X}(A) \sqcup \mathbf{X}(B)$ .*

(ii) The  $k$ -algebra  $A \times B$  is étale if and only if  $A$  and  $B$  are étale.

PROOF. (i): The surjective morphisms of  $k$ -algebras  $A \times B \rightarrow A$  and  $A \times B \rightarrow B$  allow us to view  $\mathbf{X}(A)$  and  $\mathbf{X}(B)$  as subsets of  $\mathbf{X}(A \times B)$ . Let  $f \in \mathbf{X}(A \times B)$ . The image of  $f$  is a field by Lemma 2.4.2, hence the kernel of  $f$  is a maximal ideal  $\mathfrak{m}$  of  $A \times B$ . There exist ideals  $I \subset A$  and  $J \subset B$  such that  $\mathfrak{m} = I \times J$  (every ideal of  $A \times B$  is of this form), and the maximality of  $\mathfrak{m}$  implies that  $I = A$  or  $J = B$ , and that  $I \neq A$  or  $J \neq B$ . This proves that  $f$  belongs to exactly one of the subsets  $\mathbf{X}(A)$  and  $\mathbf{X}(B)$ .

(ii): Since  $\dim_k(A \times B) = \dim_k A + \dim_k B$ , this follows from (i) and Lemma 4.2.2.  $\square$

LEMMA 4.2.10. *A reduced finite-dimensional  $k$ -algebra is a product of fields extension of  $k$ .*

PROOF. Let  $A$  be such an algebra. Then  $A$  is artinian, hence every prime ideal of  $A$  is maximal (exercise). Any pair of distinct maximal ideals are coprime. Since  $A$  is reduced (Lemma 4.2.8), the intersection of all maximal ideals is zero (the nilradical is the intersection of all prime ideals). It follows from the Chinese remainder theorem that  $A$  is isomorphic to the product of the fields  $A/\mathfrak{m}$ , where  $\mathfrak{m}$  runs over the maximal ideals of  $A$ .  $\square$

PROPOSITION 4.2.11. *A finite-dimensional  $k$ -algebra is étale if and only if it is a product of separable field extensions of  $k$ .*

PROOF. An étale  $k$ -algebra is a product of fields by Lemma 4.2.8 and Lemma 4.2.10. In view of Lemma 4.2.9, the statement follows from Lemma 4.2.4.  $\square$

PROPOSITION 4.2.12. *Let  $A$  be a finite-dimensional commutative  $k$ -algebra, and  $n = \dim_k A$ . Then the following conditions are equivalent:*

- (i) The  $k$ -algebra  $A$  is étale.
- (ii) The  $k_s$ -algebra  $A_{k_s}$  is isomorphic to  $(k_s)^n$ .
- (iii) The  $k$ -algebra  $A$  is a product of separable field extensions of  $k$ .
- (iv) If  $\bar{k}$  is an algebraic closure of  $k$ , then the ring  $A_{\bar{k}}$  is reduced.
- (v) If  $L/k$  is a field extension, then the ring  $A_L$  is reduced.

PROOF. (i)  $\iff$  (iii): Proposition 4.2.11.

(i)  $\implies$  (ii): This follows from Lemma 4.2.5 and Lemma 4.2.6.

(ii)  $\implies$  (i): The projections  $(k_s)^n \rightarrow k_s$  yield  $n$  pairwise distinct elements of  $\mathbf{X}(A)$ .

(i)  $\implies$  (v): This follows from Lemma 4.2.5 and Lemma 4.2.8.

(v)  $\implies$  (iv): Clear.

(iv)  $\implies$  (iii): The ring  $A$  is a product of fields by Lemma 4.2.10. Let  $K$  be one of these fields, and  $x \in K$ . Let  $B$  be the  $k$ -subalgebra of  $K$  generated by  $x$ . Then  $B$  is isomorphic to  $k[X]/P$ , where  $P$  is the minimal polynomial over  $k$  of  $x$ . The ring  $\bar{k}[X]/P \simeq B_{\bar{k}}$  is reduced, being contained in  $K_{\bar{k}}$ , which is reduced because  $A_{\bar{k}}$  is so (in view of Remark 4.2.7). This implies that  $P$  is separable: indeed if  $P = (X - a)Q$  where  $Q \in \bar{k}[X]$  and  $a \in \bar{k}$  are such that  $Q(a) = 0$ , then  $P \mid Q^2$ , hence  $Q$  defines a nonzero nilpotent element of  $\bar{k}[X]/P$ .  $\square$

COROLLARY 4.2.13. *Let  $L/k$  be a field extension and  $A$  a  $k$ -algebra. If the  $L$ -algebra  $A_L$  is étale, then so is the  $k$ -algebra  $A$ .*

PROOF. Let  $\bar{k}$  be an algebraic closure of  $k$ , and  $\bar{L}$  an algebraic closure of  $L$ . By Lemma 3.3.11 (i), we may view  $\bar{k}$  as a subfield of  $\bar{L}$ . The ring  $A_{\bar{L}}$  is reduced by assumption (and the criterion (v) in Proposition 4.2.12), hence so is its subring  $A_{\bar{k}}$ . This proves that  $A$  is étale by the criterion (iv) in Proposition 4.2.12.  $\square$

Let us write  $\Gamma = \text{Gal}(k_s/k)$ . If  $f \in \mathbf{X}(A)$  and  $\gamma \in \Gamma$ , we set  $\gamma f = \gamma \circ f \in \mathbf{X}(A)$ . This yields an action of the group  $\Gamma$  on the set  $\mathbf{X}(A)$ .

LEMMA 4.2.14. *Let  $A$  be a finite-dimensional  $k$ -algebra. Then the  $\Gamma$ -action on  $\mathbf{X}(A)$  is continuous (Definition 3.2.10).*

PROOF. Let  $L$  be a finite extension of  $k$  in  $k_s$ , and containing the image  $f(A) \subset k_s$  of all  $f \in \mathbf{X}(A)$  (recall that  $\mathbf{X}(A)$  is finite, and that each  $f(A)$  has finite dimension over  $k$ ). Then every element of  $\mathbf{X}(A)$  is fixed by the open subgroup  $\text{Gal}(k_s/L)$  of  $\Gamma$ , and the statement follows from Lemma 3.2.9.  $\square$

Let us denote by  $\mathbf{Fsets}_\Gamma$  the category whose objects are finite  $\Gamma$ -sets and morphisms are  $\Gamma$ -equivariant maps. We have just seen that  $\mathbf{X}(A) \in \mathbf{Fsets}_\Gamma$  for any étale  $k$ -algebra  $A$ . If  $\varphi: A \rightarrow B$  is a morphism of étale  $k$ -algebras, there is an induced map  $\mathbf{X}(B) \rightarrow \mathbf{X}(A)$  given by  $f \mapsto f \circ \varphi$ , and one sees easily that  $\mathbf{X}$  defines a contravariant functor  $\mathbf{Et}_k \rightarrow \mathbf{Fsets}_\Gamma$ .

Let now  $X$  be a finite  $\Gamma$ -set. The set

$$\mathbf{M}(X) = \{\text{maps } X \rightarrow k_s\}.$$

is naturally a  $k_s$ -algebra (via pointwise operations). This algebra is isomorphic to  $(k_s)^n$ , where  $n$  is the cardinality of  $X$ . The  $\Gamma$ -actions on  $k_s$  and  $X$  induce a  $\Gamma$ -action on  $\mathbf{M}(X)$ ; namely for  $f \in \mathbf{M}(X)$  and  $\gamma \in \Gamma$  we have

$$(\gamma f)(x) = \gamma \circ f(\gamma^{-1}x) \quad \text{for all } x \in X.$$

Then the fixed subset  $\mathbf{M}(X)^\Gamma$  is the subset of  $\Gamma$ -equivariant maps  $X \rightarrow k_s$ .

LEMMA 4.2.15. *The  $\Gamma$ -action on  $\mathbf{M}(X)$  is continuous and semilinear (Definition 3.4.2).*

PROOF. Let  $\gamma \in \Gamma$  and  $f \in \mathbf{M}(X)$ . For any  $x \in X$  and  $\lambda \in k$ , we have

$$(\gamma(\lambda f))(x) = \gamma \circ (\lambda f)(\gamma^{-1}x) = \gamma(\lambda) \gamma \circ f(\gamma^{-1}x) = \gamma(\lambda)(\gamma f(x)),$$

so that the  $\Gamma$ -action on  $\mathbf{M}(X)$  is semilinear.

Let now  $f \in \mathbf{M}(X)$ . There exists an open subgroup  $U_1$  (resp.  $U_2$ ) of  $\Gamma$  such that  $U_1$  (resp.  $U_2$ ) acts trivially on the finite set  $X$  (resp.  $f(X)$ ). Then  $U_1 \cap U_2$  is an open subgroup of  $\Gamma$  fixing  $f$ .  $\square$

We deduce from Proposition 3.4.5 that the natural morphism of  $k_s$ -algebras

$$\mathbf{M}(X)^\Gamma \otimes_k k_s \rightarrow \mathbf{M}(X)$$

is bijective. Since  $\mathbf{M}(X) \simeq (k_s)^n$ , we conclude that  $\mathbf{M}(X)^\Gamma$  is an étale  $k$ -algebra of dimension  $n$ . To a map of finite  $\Gamma$ -sets  $\alpha: X \rightarrow Y$  corresponds a morphism of étale  $k$ -algebras  $\mathbf{M}(Y)^\Gamma \rightarrow \mathbf{M}(X)^\Gamma$  given by  $f \mapsto f \circ \alpha$ , and one sees easily that  $\mathbf{M}^\Gamma: X \mapsto \mathbf{M}(X)^\Gamma$  defines a contravariant functor  $\mathbf{Fsets}_\Gamma \rightarrow \mathbf{Et}_k$ .





## Bibliography

- [Dra83] P. K. Draxl. *Skew fields*, volume 81 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.
- [GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition of [MR2266528].
- [Ker07] Ina Kersten. *Brauergruppen*. Universitätsverlag Göttingen, Göttingen, 2007. <https://univerlag.uni-goettingen.de/bitstream/handle/3/isbn-978-3-938616-89-5/brauergruppen.pdf>.
- [KMRT98] Max-Albert Knus, Alexander S. Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions. With a preface by J. Tits*. Providence, RI: American Mathematical Society, 1998.
- [Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.
- [Pie82] Richard S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982. Studies in the History of Modern Science, 9.
- [Ser62] Jean-Pierre Serre. *Corps locaux*. Publications de l’Institut de Mathématique de l’Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.
- [Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.
- [Sta] The Stacks Project Authors. Stacks Project. <http://stacks.math.columbia.edu>.