

# Brauer Groups of fields

Olivier Houton

Ludwig-Maximilians-Universität München

Winter semester 2020/2021

## Contents

Note on the literature	3
<b>Part 1. Noncommutative Algebra</b>	<b>5</b>
Chapter 1. Quaternion algebras	7
1. The norm form	7
2. Quadratic splitting fields	12
3. Biquaternion algebras	14
Chapter 2. Simple algebras	17
1. Wedderburn's Theorem	17
2. The commutant	20
3. Skolem–Noether's Theorem	23
Chapter 3. Central simple algebras and scalars extensions	25
1. The index	25
2. Splitting fields	26
3. Separable splitting fields	29
4. Finite division rings, real division algebras	30
5. The Brauer group, I	31
<b>Part 2. Torsors</b>	<b>33</b>
Chapter 4. Infinite Galois theory	35
1. Profinite sets	35
2. Profinite groups	37
3. Infinite Galois extensions	40
4. Galois descent	45
Chapter 5. Étale and Galois algebras	49
1. Categories	49
2. Étale algebras	50
3. Characteristic polynomials in étale algebras	53
4. Finite sets with a Galois action	55
5. Galois algebras	57
Chapter 6. Torsors, cocycles, and twisted forms	61
1. Torsors	61
2. Twisted forms	62

CONTENTS	2
3. Examples of twisted forms	67
4. 1-cocycles	68
Chapter 7. Applications of torsors theory	75
1. Kummer theory	75
2. Artin-Schreier theory	77
Bibliography	79

### Note on the literature

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

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



## Part 1

# Noncommutative Algebra



## CHAPTER 1

**Quaternion algebras**

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

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

**1. The norm form**

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

We fix a base field  $k$ . A  $k$ -algebra is a ring  $A$  equipped with a structure of  $k$ -vector space such that the multiplication map  $A \times A \rightarrow A$  is  $k$ -bilinear. A morphism of  $k$ -algebras is a ring morphism which is  $k$ -linear. If  $A$  is nonzero, 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 (i.e.  $2 \neq 0$  in  $k$ ).

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

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

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*.

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

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



PROOF. It will suffice to prove that the elements  $1, i, j, ij$  are linearly independent over  $k$ . Since  $i$  anticommutes with  $j$ , the elements  $1, i, j$  must be linearly independent (recall that the characteristic of  $k$  differs from 2). Now assume that  $ij = u + vi + wj$ , with  $u, v, w \in k$ . Then

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

hence  $u = v = 0$  by linear independence of  $1, i$ . So  $ij = wj$ , hence  $ij^2 = wj^2$  and thus  $bi = bw$ , a contradiction with the linear independence of  $1, i$ .  $\square$

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

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

PROOF. (i) : We let  $i', j'$  be the standard generators of  $(b, a)$ , and apply Lemma 1.1.2 with  $i = j'$  and  $j = i'$ .

(ii) : We let  $i'', j''$  be the standard generators of  $(a\alpha^2, b\beta^2)$ , and apply Lemma 1.1.2 with  $i = \alpha^{-1}i''$  and  $j = \beta^{-1}j''$ .  $\square$

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

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

PROOF. The matrices

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

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

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

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

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

PROOF. This follows from the computation

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

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, for any  $p, q \in Q$ :

- (i)  $q \mapsto \bar{q}$  is  $k$ -linear.

- (ii)  $\bar{\bar{q}} = q$ .
- (iii)  $q = \bar{q} \iff q \in k$ .
- (iv)  $q = -\bar{q} \iff q \in Q_0$ .
- (v)  $q\bar{q} \in k$ .
- (vi)  $q\bar{q} = \bar{q}q$ .
- (vii)  $\overline{pq} = \bar{q}\bar{p}$ .

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

Observe that the norm map is multiplicative:

$$N(pq) = N(p)N(q) \quad \text{for all } p, q \in Q.$$

If  $a, b \in k^\times$  are such that  $Q = (a, b)$  and  $q = x + yi + zj + wij$  with  $x, y, z, w \in k$ , then

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

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 two-sided inverse of  $N(q)^{-1}\bar{q}$ . Conversely, if  $p \in Q$  is such that  $pq = 1$ , 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 first need some definitions.

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

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

Of course, a similar argument shows that a right inverse of  $a$  is automatically a two-sided inverse.

DEFINITION 1.1.12. Let  $A$  be a commutative finite-dimensional  $k$ -algebra. The (algebra) *norm map*  $N_{A/k}: A \rightarrow k$  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

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

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

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

In the second case, let  $\alpha \in k(\sqrt{a})$  be such that  $\alpha^2 = a$  (such an element is determined only up to sign by the field extension  $k(\sqrt{a})/k$ ). Every element of  $k(\sqrt{a})$  is represented as  $x + y\alpha$  for uniquely determined  $x, y \in k$ , and

$$(1.1.d) \quad N_{k(\sqrt{a})/k}(x + y\alpha) = x^2 - ay^2.$$

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  $k$ , and choose  $\alpha \in k(\sqrt{a})$  such that  $\alpha^2 = a$ . Let  $q = x + yi + zj + wj$  be a nontrivial zero of the norm map, where  $x, y, z, w \in k$ . Then by the formula (1.1.c)

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

hence  $x^2 - ay^2 = b(z^2 - aw^2)$ . Assume that  $z^2 - aw^2 = 0$ . Then  $z = w = 0$ , because  $a$  is not a square. Also  $x^2 - ay^2 = 0$ , and for the same reason  $x = y = 0$ . Thus  $q = 0$ , a contradiction. Therefore  $z^2 - aw^2 \neq 0$ , and by (1.1.d)

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

(iv)  $\Rightarrow$  (v) : Let  $\alpha \in k(\sqrt{a})$  be such that  $\alpha^2 = a$ . If  $\alpha \in k$ , then we may take  $x = \alpha^{-1}$  and  $y = 0$ . If  $\alpha \notin k$ , then by (iv) there are  $u, v \in k$  such that  $b = N_{k(\sqrt{a})/k}(u + v\alpha)$ . Then  $b = u^2 - av^2$  by (1.1.d). If  $u \neq 0$ , we may take  $x = vu^{-1}$  and  $y = u^{-1}$ . Assume that  $u = 0$ . Then  $b = -av^2$ , and in particular  $v \neq 0$ . Let

$$x = \frac{a+1}{2a} \quad \text{and} \quad y = \frac{a-1}{2av}.$$

Then

$$ax^2 + by^2 = ax^2 - av^2y^2 = \frac{a^2 + 2a + 1}{4a} - \frac{a^2 - 2a + 1}{4a} = 1.$$

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

(vi)  $\Rightarrow$  (i) : By Lemma 1.1.4 (and Lemma 1.1.3 (ii)) we may assume that  $a$  is not a square in  $k$ , so that  $y \neq 0$ . Applying Lemma 1.1.14 below with  $u = xy^{-1}$ ,  $v = zy^{-1}$  and  $c = b$  yields  $(a, b) \simeq (a, b^2)$ . Since  $(a, b^2) \simeq (1, a)$  (by Lemma 1.1.3), we obtain (i) using Lemma 1.1.4 below.  $\square$

LEMMA 1.1.14. Let  $a, b, c \in k^\times$ , and assume that  $au^2 + c = v^2$  for some  $u, v \in k$ . Then  $(a, b) \simeq (a, bc)$ .

PROOF. Denote by  $i', j'$  the standard generators of  $(a, bc)$ . Set

$$i = i', \quad j = c^{-1}(vj' + ui'j') \in (a, bc).$$

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

$$j^2 = c^{-2}(bcv^2 - abc u^2) = bc^{-1}(v^2 - au^2) = b.$$

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

DEFINITION 1.1.15. A quaternion algebra satisfying the conditions of Proposition 1.1.13 will be called *split* (observe that this does not depend on the choice of  $a, b \in k^\times$ ).

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

EXAMPLE 1.1.16. Assume that  $k$  is *quadratically closed*, i.e. that every element of  $k$  is a square. Then for every  $a, b \in k^\times$ , we have  $(a, b) \simeq (1, b) \simeq M_2(k)$  by Lemma 1.1.4 (and Lemma 1.1.3 (ii)). Therefore every quaternion  $k$ -algebra splits.

EXAMPLE 1.1.17. Assume that the field  $k$  is finite, with  $q$  elements. As the group  $k^\times$  is cyclic of order  $q - 1$ , there are exactly  $1 + (q - 1)/2$  squares in  $k$ . Thus the sets  $\{ax^2 | x \in k\}$  and  $\{1 - by^2 | y \in k\}$  both consist of  $1 + (q - 1)/2$  elements; as subsets of the set  $k$  having  $q$  elements, they must intersect. It follows from the criterion (v) in Proposition 1.1.13 that  $(a, b)$  splits. Therefore *every quaternion algebra over a finite field is split*.

EXAMPLE 1.1.18. Let  $k = \mathbb{R}$ . The quaternion algebra  $(-1, -1)$  is not split, by Proposition 1.1.13 (v). Since  $k^\times/k^{\times 2} = \{1, -1\}$ , and taking into account Lemma 1.1.4 (as well as Lemma 1.1.3), we see that there are exactly two isomorphism classes of  $k$ -algebras, namely  $M_2(k)$  and  $(-1, -1)$ .

Let us record another useful consequence of Lemma 1.1.14.

PROPOSITION 1.1.19. *Let  $a, b, c \in k^\times$ . If  $(a, c)$  is split, then  $(a, bc) \simeq (a, b)$ .*

PROOF. Since  $(a, c)$  is split, by Proposition 1.1.13 (iv) and (1.1.d) there are  $u, v \in k$  such that  $c = v^2 - au^2$ . The statement follows from Lemma 1.1.14.  $\square$

PROPOSITION 1.1.20. *Let  $Q, Q'$  be quaternion algebras, with respective pure quaternion subspaces  $Q_0, Q'_0$ . Then  $Q \simeq Q'$  if and only if there is a  $k$ -linear map  $\varphi: Q_0 \rightarrow Q'_0$  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 1.1.20, assuming some basic quadratic form theory. It illustrates the strong connections between the theories of quaternion algebras and quadratic forms. It can be safely ignored, and will not be used in the sequel.

COROLLARY 1.1.21. *Two quaternion algebras are isomorphic if and only if their norm forms are isometric.*

PROOF. Let  $Q$  be a quaternion algebra and  $N: Q \rightarrow k$  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  $N|_k = \langle 1 \rangle$ . So we have a decomposition  $N \simeq \langle 1 \rangle \perp (N|_{Q_0})$ . This quadratic form is nondegenerate (e.g. by (1.1.c)), hence a morphism  $\varphi$  as in Proposition 1.1.20 is automatically an isometry. The corollary follows, by Witt's cancellation Theorem (see for instance [Lam05, Theorem 4.2]).  $\square$

## 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 nonzero  $k$ -algebra is called *central* if its center equals  $k$ .

LEMMA 1.2.2. *Every quaternion algebra is central.*

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

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

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

PROOF. Let  $L \subset D$  be a subalgebra isomorphic to  $k(\sqrt{a})$ , and  $\alpha \in L$  such that  $\alpha^2 = a$ . Since  $\alpha$  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 2 over  $L$ , hence dimension 4 over  $k$ , and thus coincides with  $D$  by dimensional reasons. In particular the  $k$ -algebra  $D$  is generated by  $\alpha, \beta$ . 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 and  $D$  is nonzero, this morphism is injective. Its image  $L$  is a field, and coincides with the  $k$ -subalgebra of  $D$  generated by  $d$ . Now  $D$  is a vector space over  $L$ , and  $\dim_L D \cdot \dim_k L = \dim_k D = 4$ . We cannot have  $\dim_k L = 4$ , for  $D = L$  would then be commutative, and so would not be central over  $k$ . The case  $\dim_k L = 1$  is also excluded, since by assumption  $d \notin k$ . So we must have  $\dim_k L = 2$ .  $\square$

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

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

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

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  $k(t)$ . Writing  $Q \simeq (a, b)$  for some  $a, b \in k^\times$ , this means that  $ax^2 + by^2 = z^2$  has a nontrivial solution in  $k(t)$ , by Proposition 1.1.13. Clearing denominators we may assume that  $x, y, z \in k[t]$ , and that one of  $x, y, z$  is not divisible by  $t$ . Then  $x(0), y(0), z(0)$  is a nontrivial solution in  $k$ , hence  $Q$  splits. Therefore *every quaternion algebra splitting over  $k(t)$  splits over  $k$ .*

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

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

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

(ii)  $\Rightarrow$  (iii) : If  $Q$  is split, then  $Q \simeq (1, a) \simeq (a, 1)$  by Lemma 1.1.4, and (iii) was observed in Remark 1.2.3. Thus we assume that  $Q$  is division. Let  $\alpha \in k(\sqrt{a})$  be such that  $\alpha^2 = a$ . Then there are  $p, q \in Q$  not both zero such that  $N(p \otimes 1 + q \otimes \alpha) = 0$  by Proposition 1.1.13. Set  $r = p\bar{q} \in Q$ . In view of (1.2.a), we have

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

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 in  $Q \otimes_k Q'$

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

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

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

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

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

Assume that  $q_1 q_2 = q_2 q_1$ . Let  $K$  be the  $k$ -subalgebra of  $Q$  generated by  $q_1, q_2$ . We claim that if  $K \neq k$ , then  $K$  is a quadratic field extension of  $k$ . Indeed, this is true by Lemma 1.2.5 if  $q_1 \in k$ , so we will assume that  $q_1 \notin k$ . Then the  $k$ -subalgebra  $K_1$  of  $Q$  generated by  $q_1$  is a quadratic field extension of  $k$ , by the same lemma. If  $q_2 \notin K_1$ , then  $1, q_2$  is a  $K_1$ -basis of  $Q$ , so that  $K = Q$ . This is not possible since  $q_1$  and  $q_2$  commute (as  $Q$  is central). Thus  $q_2 \in K_1$ , and  $K = K_1$  is as required, proving the claim. If  $K \neq k$ , then Proposition 1.2.9 thus implies that  $Q$  splits over  $K$ , and since (ii) does not hold, by the same proposition  $K \otimes_k Q'$  must remain division. This conclusion also holds if  $K = k$ . Thus in any case  $x \in K \otimes_k Q'$  admits a left inverse.

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

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

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

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

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

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

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

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

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

There are isomorphisms of  $k$ -algebras

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

Moreover every element of  $A$  commutes with every element of  $A'$ . Therefore the  $k$ -linear map  $f: A \otimes_k A' \rightarrow (a, b) \otimes_k (a, c)$  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.  $\square$

PROPOSITION 1.3.4. *Let  $Q, Q'$  be quaternion algebras. Then*

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

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

Assume now that  $Q \otimes_k Q' \simeq M_4(k)$ . Since  $M_4(k)$  is not division, by Albert's Theorem 1.3.2, there are  $a, b, c \in k^\times$  such that  $Q \simeq (a, b)$  and  $Q' \simeq (a, c)$ . If  $(a, bc)$  splits, then Proposition 1.1.19 implies that  $(a, b) \simeq (a, b^2c) \simeq (a, c)$ , as required. So we assume that  $D = (a, bc)$  is division, and come to a contradiction. By Lemma 1.3.3, we have

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

The element of  $M_2(D)$  corresponding to the matrix

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

is an endomorphism  $\varphi$  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  $\lambda_1 \neq 0$ . Let  $f = \varphi(e_2)$ . Then  $\varphi(e_1) = -\lambda_1^{-1}\lambda_2 f$ , hence  $\varphi(D^{\oplus 2}) = Df$ . Thus  $\varphi(f) = \mu f$  for some  $\mu \in D$ , and

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

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

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

## CHAPTER 2

## Simple algebras

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

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

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

## 1. Wedderburn's Theorem

A module (resp. ideal) will mean a left module (resp. ideal). When  $R$  is a ring, the ring of  $n$  by  $n$  matrices will be denoted by  $M_n(R)$ . If  $M, N$  are  $R$ -modules, we denote the set of morphisms of  $R$ -modules  $M \rightarrow N$  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) Transposing matrices induces an isomorphism  $M_n(R)^{\text{op}} \simeq M_n(R^{\text{op}})$ .

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.

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

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

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

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 subring  $R \subset M_n(R)$ , and generate  $M_n(R)$  as an  $R$ -module. Taking the  $(i,j)$ -th coefficient yields a morphism of two-sided  $R$ -modules  $\gamma_{i,j}: M_n(R) \rightarrow R$ . For any  $m \in M_n(R)$ , we have

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

and

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

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

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

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

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

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

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

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

and therefore  $I_r \subset Bm$ . We have proved that  $I_r$  is a simple  $B$ -module, or equivalently a minimal nonzero ideal of  $B$ . If  $I$  is any other such ideal, then there is a surjective morphism of  $B$ -modules  $B \rightarrow I$  (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  $R \simeq \text{End}_B(I_r)^{\text{op}} \simeq \text{End}_B(I)^{\text{op}}$ .  $\square$

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

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

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

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

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

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

**REMARK 2.1.11.** In the literature, the artinian property is sometimes included in the definition of simple rings. So what we call “artinian simple rings” are simply referred to as “simple rings”.

**PROPOSITION 2.1.12.** *Let  $A$  be an artinian simple ring.*

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

**PROOF.** Since  $A$  is artinian, it admits a minimal nonzero ideal  $S$ . Then  $S$  is a simple  $A$ -module. Moreover the two-sided ideal  $SA$  generated by  $S$  in  $A$  is nonzero, hence  $SA = A$  by simplicity of  $A$ . In particular there are elements  $a_1, \dots, a_p \in A$  such that  $1 \in Sa_1 + \dots + Sa_p$ . 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 2.1.13 (Wedderburn).** *Let  $A$  be an artinian simple ring (resp. a finite-dimensional simple  $k$ -algebra). Then  $A$  is isomorphic to  $M_n(D)$  for some integer  $n$  and division ring (resp. finite-dimensional division  $k$ -algebra)  $D$ . Such a ring (resp.  $k$ -algebra)  $D$  is unique up to isomorphism, and the centers of  $A$  and  $D$  are isomorphic.*

**PROOF.** Recall that in any case  $A$  is artinian (Example 2.1.10). Let  $S$  be a simple  $A$ -module, which exists by Proposition 2.1.12. Then the ring  $E = \text{End}_A(S)$  is division by Schur's Lemma 2.1.2. By Proposition 2.1.12 there is an integer  $n$  such that  $A \simeq S^{\oplus n}$  as  $A$ -modules. In view of Lemma 2.1.4 (with  $R = A$  and  $e = 1$ ), we have

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

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

## 2. The commutant

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

$$(2.2.a) \quad A \otimes_k B \simeq B \otimes_k A \quad ; \quad a \otimes b \mapsto b \otimes a.$$

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

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

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

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

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

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

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

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

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

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

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

PROOF. Let  $C = \mathcal{Z}_{A \otimes_k B}(A' \otimes_k k)$ . Certainly  $\mathcal{Z}_A(A') \otimes_k B \subset C$ . Any element  $c \in C$  may be written as  $c = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$  for some  $n \in \mathbb{N}$ , with  $a_1, \dots, a_n \in A$  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  $A \otimes_k B$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We can now summarise our results as follows:

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

PROOF. Combine Proposition 2.2.6, Proposition 2.2.4 and Proposition 2.2.5.  $\square$

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

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

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

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

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 2.2.3.  $\square$

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

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

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

PROOF. By Proposition 2.1.12, there exist a simple  $B$ -module  $S$  and integers  $r, n$  such that  $B \simeq S^{\oplus r}$  and  $A \simeq S^{\oplus n}$  as  $B$ -modules. The  $k$ -algebra  $D = \text{End}_B(S)^{\text{op}}$  is division by Schur's Lemma 2.1.2. We have, by Lemma 2.2.10

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

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

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

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

(ii): Let  $a = \dim_k A, b = \dim_k B, c = \dim_k C, d = \dim_k D, s = \dim_k S$ . Taking the dimensions in (2.2.b) and (2.2.c) yields  $ac = n^2d$  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  $a = bc$ .

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

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

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

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

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

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

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

### 3. Skolem–Noether's Theorem

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

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

PROOF. This follows from Proposition 2.1.12. Indeed let  $S$  be a simple  $A$ -module. Then every  $A$ -module  $M$  of finite dimension over  $k$  (which is necessarily finitely generated) is isomorphic to  $S^{\oplus n}$  for some  $n \in \mathbb{N}$ . Then  $\dim_k M = n \dim_k S$ , hence the integer  $n$  is determined by  $\dim_k M$ .  $\square$



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

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

PROOF. Let  $\varphi: A^f \rightarrow A^g$  be an isomorphism of  $B \otimes_k A^{\text{op}}$ -modules. 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. On the other hand

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

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

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

COROLLARY 2.3.4. *Every automorphism of a finite-dimensional central simple  $k$ -algebra  $A$  is inner, i.e. of the form  $x \mapsto a^{-1}xa$  for some  $a \in A^\times$ .*

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

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

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

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

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

## CHAPTER 3

## Central simple algebras and scalars extensions

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

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

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

## 1. The index

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

LEMMA 3.1.1. *Let  $A$  be a  $k$ -algebra and  $L/k$  a field extension. Then  $A$  is a finite-dimensional central simple  $k$ -algebra if and only if  $A_L$  is a finite-dimensional central simple  $L$ -algebra.*

PROOF. Since  $\dim_k A = \dim_L A_L$  and  $\mathcal{Z}(A_L) = \mathcal{Z}(A) \otimes_k L$  by Proposition 2.2.4, the  $k$ -algebra  $A$  is finite-dimensional (resp. central) if and only if the  $L$ -algebra  $A_L$  is so. Observe that the ring  $L$  is simple (Remark 2.1.6). Thus the equivalence follows from Proposition 2.2.5 and Proposition 2.2.6.  $\square$

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

PROOF. Let  $D$  be a division  $k$ -algebra, and  $B$  a finite-dimensional subalgebra. Let  $b$  be a nonzero element of  $B$ . The  $k$ -linear map  $B \rightarrow B$  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 3.1.3. *If  $k$  is algebraically closed, the only finite-dimensional division  $k$ -algebra is  $k$ .*

PROOF. Let  $D$  be a finite-dimensional division  $k$ -algebra. Pick an element  $x \in D$ . The  $k$ -subalgebra of  $D$  generated by  $x$  is commutative, hence a field by Lemma 3.1.2. It

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

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

**PROOF.** This follows from Wedderburn's Theorem 2.1.13 and Proposition 3.1.3.  $\square$

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

**DEFINITION 3.1.6.** When  $A$  is a finite-dimensional central simple  $k$ -algebra, the integer  $d \in \mathbb{N}$  such that  $d^2 = \dim_k A$  is called the *degree* of  $A$  and denoted  $\deg(A)$ .

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

**DEFINITION 3.1.7.** Two finite-dimensional central simple  $k$ -algebras  $A, B$  are called *Brauer-equivalent* if there exist integers  $m, n$  and an isomorphism of  $k$ -algebras  $M_n(A) \simeq M_m(B)$ .

This defines an equivalence relation on the set of isomorphism classes of finite-dimensional central simple  $k$ -algebras (recall that  $M_n(M_m(A)) \simeq M_{nm}(A)$  for any  $k$ -algebra  $A$ ). Wedderburn's Theorem 2.1.13 implies that each Brauer-equivalence class contains exactly one isomorphism class of division algebras.

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

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

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

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

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

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

## 2. Splitting fields

**DEFINITION 3.2.1.** A finite-dimensional central simple  $k$ -algebra is called *split* if it is isomorphic to the matrix algebra  $M_n(k)$  for some integer  $n$  (which must then coincide with  $\deg(A)$ ). A field extension  $L/k$  is called a *splitting field* of  $A$  if the  $L$ -algebra  $A_L = A \otimes_k L$  is split.

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

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

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

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

so that  $B$  is Brauer-equivalent to  $A$ .  $\square$

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

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

**PROOF.** By the Proposition 3.2.2, we may assume that  $\deg(A) = [L : k]$ . Then  $\text{ind}(A)$  divides  $\deg(A) = [L : k]$ .  $\square$

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

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

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

from which the statement follows.  $\square$

**PROPOSITION 3.2.5.** *Let  $D$  be a finite-dimensional central division  $k$ -algebra, and  $L \subset D$  a commutative subalgebra. Then  $L$  is a field, and the following are equivalent:*

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

**PROOF.** The first assertion follows from Lemma 3.1.2.

(i)  $\Leftrightarrow$  (iii) : This has been proved in Lemma 3.2.4.

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

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

(ii)  $\Rightarrow$  (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)  $\Rightarrow$  (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 3.2.6. A subalgebra  $L$  satisfying the equivalent conditions of Proposition 3.2.5 is called a *maximal subfield*.

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

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

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

PROPOSITION 3.2.8. *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 3.1.9. By Corollary 3.2.7, there exists a field extension  $E/L$  splitting the  $L$ -algebra  $A_L$  and such that  $[E : L] = \text{ind}(A_L)$ . Then  $E$  is a splitting field for the  $k$ -algebra  $A$ , and it follows from Corollary 3.2.3 that

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

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

PROOF. Proposition 3.2.8 yields

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

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

PROPOSITION 3.2.10. *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. By Corollary 3.2.7, there exists an extension  $L/k$  splitting the  $k$ -algebra  $A$  and 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 3.2.8 to the  $k$ -algebra  $A \otimes_k B$ , and Lemma 3.1.9 to the  $k$ -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 3.2.8 to the algebra  $B$ , and Proposition 3.2.8 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 3.2.11. *If  $D, D'$  are finite-dimensional central division  $k$ -algebras of coprime degrees, then  $D \otimes_k D'$  is division.*

PROOF. Proposition 3.2.10 yields

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

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

### 3. Separable splitting fields

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

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

**PROPOSITION 3.3.1.** *Let  $D$  be a finite-dimensional division  $k$ -algebra. If  $D$  is not commutative, then  $D$  contains a nontrivial separable field extension of  $k$ .*

**PROOF.** By Lemma 3.1.2, the  $k$ -subalgebra generated by any element of  $D$  is a field (being commutative). Assume for a contradiction that no such field is a nontrivial separable extension of  $k$ . Since algebraic extensions of fields of characteristic zero are separable, we may assume that  $k$  has characteristic  $p > 0$ . Let  $d \in D$ . Since  $D$  is finite-dimensional over  $k$ , there is a nonzero polynomial  $P \in k[X]$  such that  $P(d) = 0$ . Since  $D$  contains no nonzero zerodivisors (being division), we may assume that  $P$  is irreducible. We may find a power  $q$  of  $p$  such that  $P(X) = Q(X^q)$ , where  $Q \in k[Y]$  and  $Q \notin k[Y^p]$ . The polynomial  $Q$  is irreducible (because  $P$  is so), hence separable (as it does not lie in  $k[Y^p]$ ). Since  $Q(d^q) = 0$ , we must have  $d^q \in k$ , by our assumption.

Let now  $a \in D$  be such that  $a \notin \mathcal{Z}(D)$ . Consider the  $k$ -algebra automorphism  $\sigma: D \rightarrow D$  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 3.3.2.** *Assume that  $k$  is separably closed (i.e. admits no nontrivial separable extension). Then every finite-dimensional division  $k$ -algebra is commutative. In particular, every finite-dimensional central simple  $k$ -algebra splits.*

**PROOF.** The first statement follows from Proposition 3.3.1. In particular  $k$  is the only finite-dimensional central division  $k$ -algebra, which implies the second statement by Wedderburn's Theorem 2.1.13.  $\square$

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

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

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

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

**PROOF.** We may assume that  $A$  is division, in which case the statement follows from Theorem 3.3.3 (in view of Proposition 3.2.5).  $\square$

#### 4. Finite division rings, real division algebras

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

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

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

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

By the theory of finite fields, the extension  $L/k$  is isomorphic to the splitting field of the polynomial  $X^{q^n} - X \in k[X]$ . Therefore if  $L'$  is another maximal subfield of  $D$ , there exists an isomorphism of  $k$ -algebras  $\sigma : L \rightarrow L'$ . Applying Skolem–Noether's Theorem 2.3.3 to the pair of morphisms  $L \subset D$  and  $L \xrightarrow{\sigma} L' \subset D$  (recall that  $L$  is a simple ring, being a field) shows that there exists  $e \in D^\times$  such that  $L' = \sigma(L) = e^{-1}Le \subset D$ . This proves that the above action is transitive.

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

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

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

**THEOREM 3.4.2** (Frobenius, 1877). *Every finite-dimensional division  $\mathbb{R}$ -algebra is isomorphic to  $\mathbb{R}$ , or to  $\mathbb{C}$ , or to the quaternion  $\mathbb{R}$ -algebra  $(-1, -1)$ .*

**PROOF.** Let  $D$  be a finite-dimensional division  $\mathbb{R}$ -algebra, and  $k$  its center. Then  $k$  is a finite extension of  $\mathbb{R}$ , hence  $k = \mathbb{R}$  or  $k \simeq \mathbb{C}$ . In the latter case, we have  $D \simeq \mathbb{C}$

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

### 5. The Brauer group, I

Let us denote by  $[A]$  the Brauer-equivalence class (Definition 3.1.8) of a finite-dimensional central simple  $k$ -algebra  $A$ . In view of Proposition 2.2.9, the operation  $([A], [B]) \mapsto A \otimes_k B$  endows the set of equivalence classes with the structure of an abelian group, where

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

DEFINITION 3.5.1. The group of Brauer-equivalence classes is called the *Brauer group* of  $k$ , and is denoted by  $\text{Br}(k)$ .

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

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

EXAMPLE 3.5.3. It follows respectively from Corollary 3.3.2, Theorem 3.4.1 and Theorem 3.4.2 that:

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

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

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

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

DEFINITION 3.5.6. 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  $\text{Br}(L/k)$ .

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

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

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



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

REMARK 3.5.8. Let  $A \neq k$  be a split finite-dimensional central simple algebra. Then  $A$  contains an element  $x \neq 0$  such that  $x^2 = 0$ . Indeed we may assume that  $A = M_r(k)$  for some  $r > 1$ , and then take for  $x$  the matrix whose only nontrivial entry is 1 in the upper right corner.

LEMMA 3.5.9. *Let  $L/k$  be a field extension. Then*

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

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

PROOF. We show that every finite-dimensional central division  $k$ -algebra  $D$  splitting over  $L$  splits over a finitely generated subextension of  $L$ , proceeding by induction on the degree of  $D$  (for all fields  $k$  simultaneously). We may assume that  $D \neq k$ . Then  $D \otimes_k L$  contains an element  $x \neq 0$  such that  $x^2 = 0$  (Remark 3.5.8). Writing  $x = d_1 \otimes \lambda_1 + \cdots + d_n \otimes \lambda_n$ , where  $d_1, \dots, d_n \in D$  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 2.1.13. So by induction it splits over a finitely generated extension  $K$  of  $K'$ . Then  $K$  is a finitely generated extension of  $k$  splitting  $D$ .  $\square$

PROPOSITION 3.5.10. *If  $L$  is a purely transcendental extension of  $k$ , then*

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

PROOF. If  $L = k(t_i, i \in I)$ , then every element of  $L$  belongs to a subextension of  $L/k$  generated by finitely many  $t_i$ 's (such element is a quotient of two polynomials, and a given polynomial involves only finitely many variables). Therefore every finitely generated subextension  $K/k$  is contained in a subextension of  $L/k$  generated by finitely many  $t_i$ 's. In view of Lemma 3.5.9, we may thus assume that  $I$  is finite. Using induction we reduce to the case  $|I| = 1$ , that is  $L = k(t)$ . Let  $D \neq k$  be a finite-dimensional central division  $k$ -algebra which splits over  $k(t)$ . Then  $D \otimes_k k(t)$  contains an element  $x \neq 0$  such that  $x^2 = 0$  (Remark 3.5.8). We may write

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

where  $d_i \in D$  and  $f_i, g_i \in k[t]$  for all  $i$ . Choosing such a decomposition with  $n$  minimal, we see that the elements  $d_i \in D$  must be linearly independent over  $k$ . Multiplying  $x$  with an appropriate element of  $k[t]$ , we may assume that  $g_1 = \cdots = g_n = 1$ , and that there is  $j \in \{1, \dots, n\}$  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 4

## Infinite Galois theory

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

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

## 1. Profinite sets

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

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

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

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

These data must satisfy the following conditions:

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

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

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

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

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

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

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

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

PROOF. Let  $U \subset E$  be an open subset, and  $u \in U$ . By definition of the profinite topology, there are  $\alpha_1, \dots, \alpha_n \in \mathcal{A}$  and  $x_i \in E_{\alpha_i}$  for  $i = 1, \dots, n$  such that the set  $\pi_{\alpha_1}^{-1}\{x_1\} \cap \dots \cap \pi_{\alpha_n}^{-1}\{x_n\}$  is contained in  $U$ , and contains  $u$ . Let us choose  $\alpha \in \mathcal{A}$  such that  $\alpha_i \leq \alpha$  for all  $i \in \{1, \dots, n\}$  (recall that  $\mathcal{A} \neq \emptyset$ ). 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 4.1.7. *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  $\alpha \in \mathcal{A}$  such that  $f_{\beta\alpha}(T_\beta) \subset T_\alpha$  for each  $\alpha \leq \beta$ . Consider the set  $\mathcal{T}$  of all subsystems  $(T_\alpha)$  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  $\alpha \in \mathcal{A}$ , 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  $\alpha \in \mathcal{A}$ . 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  $\beta \in \mathcal{A}$  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  $\gamma \in \mathcal{A}$  and  $x \in T_\gamma$ . For  $\alpha \in \mathcal{A}$ , we set

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

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 4.1.8. *Every profinite set is compact.*

PROOF. Let  $U_i$  for  $i \in I$  be a family of open subsets covering  $E$ . We need to find a finite subset  $J \subset I$  such that the subsets  $U_i$  for  $i \in J$  cover  $E$ . While doing so, by Lemma 4.1.6 we may assume that each  $U_i$  is of the form  $\pi_{\alpha_i}^{-1}\{x_i\}$ , where  $\alpha_i \in \mathcal{A}$  and  $x_i \in E_{\alpha_i}$ .

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

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

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

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

Conversely:

LEMMA 4.1.11. *Assume that each  $E_\alpha$  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  $\gamma \in \mathcal{A}$  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 4.1.7. Its image in  $y \in E$  satisfies  $\pi_\gamma(y) = x$ .  $\square$

## 2. Profinite groups

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

DEFINITION 4.2.1. When each  $E_\alpha$  appearing in Definition 4.1.2 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. When each  $E_\alpha$  is finite, the topological group  $E$  is called a *profinite group*.

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

EXAMPLE 4.2.3. Let  $p$  be a prime number. The groups  $\mathbb{Z}/p^n\mathbb{Z}$  for  $n \in \mathbb{N}$ , together with the maps  $\mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}$  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 4.2.4. 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  $\widehat{\mathbb{Z}}$ .

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

LEMMA 4.2.5. (i) Let  $U \subset \Gamma$  be an open subset and  $u \in U$ . Then there exists  $\alpha \in \mathcal{A}$  such that  $uU_\alpha \subset U$ .

(ii) A subgroup of  $\Gamma$  is open if and only if it is closed and has finite index.

(iii) If a subgroup of  $\Gamma$  contains an open subgroup, it is open.

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

REMARK 4.2.6. Let  $\mathcal{U}$  be the set of open normal subgroups of  $\Gamma$ , ordered by letting  $U \leq V$  when  $V \subset U$ . Then  $\mathcal{U}$  is a directed set, and 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 (exercise). Thus every profinite group admits a canonical representation as an inverse limit.

DEFINITION 4.2.7. Let  $p$  be a prime number. Recall that a  $p$ -group is a finite group whose order is a power of  $p$ . A *pro- $p$ -group* is an inverse limit of  $p$ -groups. A subgroup  $P$  of  $\Gamma$  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 if  $P$  is a pro- $p$ -Sylow subgroup of  $\Gamma$ , then the image of  $P$  in  $\Gamma/U$  is a Sylow  $p$ -group, for every open normal subgroup  $U$  of  $\Gamma$ .

PROPOSITION 4.2.8. The profinite group  $\Gamma$  admits a pro- $p$ -Sylow subgroup.

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

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

LEMMA 4.2.9. *Let  $X$  be a set with an action of the profinite group  $\Gamma$ . The following conditions are equivalent:*

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

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

(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 4.2.5 (iii). Thus  $U_{x,y}$  is open, being either empty or the image of  $U_{x,x}$  under a self-homeomorphism of  $\Gamma$ . 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).  $\square$

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

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

PROOF. By assumption, 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  $F$ .  $\square$

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

LEMMA 4.2.12. *Let  $X$  be a discrete  $\Gamma$ -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  $\Gamma$ . Conversely, any map  $\Gamma^n \rightarrow X$  factoring through  $(\Gamma/U)^n \rightarrow X$  for some open normal subgroup  $U$  of  $\Gamma$  is continuous.*



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

Let now  $f: \Gamma^n \rightarrow X$  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 4.1.8. Therefore  $Y$  is compact. Being also discrete, the set  $Y$  is finite. Since  $X$  is a discrete  $\Gamma$ -set, there is an open subgroup  $U'$  in  $\Gamma$  fixing all the elements of  $Y$  (Lemma 4.2.11). Shrinking  $U'$ , we may assume that it is normal in  $\Gamma$  (by Lemma 4.2.5 (i) with  $u = 1$ ). We have achieved  $f(\Gamma^n) \subset X^{U'}$ .

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

### 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. The only nontrivial fact that we will use without proof is the existence of algebraic closures.

When  $A, B$  are  $k$ -algebras, we will denote by  $\text{Hom}_{k\text{-alg}}(A, B)$  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 4.3.1. *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 an upper bound. By Zorn's lemma, we find a maximal element  $(K, \sigma)$ . Let  $x \in L$ , and  $P \in k[X]$  be the minimal polynomial of  $x$  over  $K$ . Then  $P$  has a root  $y$  in the algebraically closed field  $F$ . The subextension  $E$  of  $L/K$  generated by  $x$  is isomorphic to  $K[X]/P$ , and mapping  $x$  to  $y$  induces a  $k$ -algebra morphism  $E \rightarrow F$  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  $P \in k[X]$  the minimal polynomial of  $x$  over  $k$ . The subextension  $K$  of  $L/k$  generated by  $x$  is isomorphic to  $k[X]/P$ , and morphisms of  $k$ -algebras  $K \rightarrow F$  correspond to roots of  $P$  in  $F$ . There are at most (resp. exactly, if  $L/k$  is separable and  $F$  is algebraically closed)  $\deg P = [K : k]$

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  $L \rightarrow F$ .  $\square$

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

**PROPOSITION 4.3.2.** *Let  $L/k$  be a finite field extension. Let  $G$  be a subgroup of  $\text{Aut}_{k\text{-alg}}(L)$  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 4.3.1 (iii). In particular  $G$  is finite, and it will suffice to prove that  $|G| \geq [L : k]$ . Let  $M$  be the set of maps  $G \rightarrow L$ , 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 the elements  $x_1, \dots, x_r$  are linearly independent over  $k$  and  $0 = \varphi(v)(\text{id}_L) = x_1 y_1 + \cdots + x_r y_r$ , there exists  $j \in \{2, \dots, r\}$  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 thus  $|G| \geq [L : k]$ , as required.  $\square$

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

**LEMMA 4.3.3.** *Let  $L/k$  be a normal field extension and  $F/k$  a field extension. Then all morphisms of  $k$ -algebras  $L \rightarrow F$  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  $\mathcal{P}$ . We prove that  $E$  is the common image. 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  $x$  over  $k$ , proving that  $\sigma(L) \subset E$ . Conversely, let  $y \in E$ , and pick  $P \in \mathcal{P}$  such that  $P(y) = 0$ . As  $L/k$  is normal, we may find  $x_1, \dots, x_n \in L$  such that  $P = (X - x_1) \cdots (X - x_n)$  in  $L[X]$ , hence

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

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

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

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

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

(ii)  $\Rightarrow$  (i) : Let  $x \in F$ . Let  $S$  be the set of those  $\sigma(x) \in F$ , where  $\sigma$  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

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

Every  $\sigma \in \text{Aut}_{k\text{-alg}}(F)$  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 a product of pairwise distinct monic linear factors over  $F$ .  $\square$

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

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

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

LEMMA 4.3.7. *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 4.3.3, proving the first statement. Let now  $\tau \in \text{Gal}(E/k)$ . Let  $\overline{F}$  be an algebraic closure of  $F$ . Then the morphism  $E \xrightarrow{\tau} E \subset \overline{F}$  extends to a morphism of  $k$ -algebras  $F \rightarrow \overline{F}$  by Lemma 4.3.1 (i), whose image equals  $F$  by Lemma 4.3.3. We have thus extended  $\tau$  to an element of  $\text{Gal}(F/k)$ .  $\square$

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

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

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

**PROPOSITION 4.3.9.** *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 4.3.8. The morphisms  $\text{Gal}(L'/k) \rightarrow \text{Gal}(L/k)$  for  $L, L' \in \mathcal{F}$  with  $L \subset L'$  are given by restricting automorphisms (see Lemma 4.3.7).

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

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

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 4.3.8, there exists  $L \in \mathcal{F}$  such that  $x \in L$ . Moreover, if another extension  $L' \in \mathcal{F}$  contains  $x$ , then there exists an extension  $L'' \in \mathcal{F}$  containing  $L$  and  $L'$ , so that  $\sigma^L(x) = \sigma^{L''}(x) = \sigma^{L'}(x)$ . Therefore  $\sigma^L(x) \in F$  does not depend on the choice of the extension  $L \in \mathcal{F}$  containing  $x$ . We have thus defined a map  $\sigma: F \rightarrow F$  restricting to  $\sigma^L$  for each finite Galois subextension  $L/k$  of  $F/k$ . It is easy to verify that  $\sigma$  is indeed an automorphism of the  $k$ -algebra  $F$ .  $\square$

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

**THEOREM 4.3.11 (Krull).** *The associations*

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

*yield inclusion-reversing, mutually inverse bijections between subextensions  $E$  of  $F/k$  and closed subgroups  $H$  of  $\text{Gal}(F/k)$ . 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  $E$  be a subextension of  $F/k$ . By Lemma 4.3.6 we have  $F^{\text{Gal}(F/E)} = E$ . If  $E/k$  is finite, it is contained in a finite Galois subextension  $E'$  of  $F/k$  by Lemma 4.3.8. The subgroup  $\text{Gal}(F/E)$  is then 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 the subextension  $E$  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 4.2.5 (i), the open complement of  $H$  in  $\text{Gal}(F/k)$  contains a subset of the  $\sigma \text{Gal}(F/L)$ , where  $L$  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 4.3.2. In particular we may find  $h \in H$  such that

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

Now assume that  $H$  is an open subgroup of  $\text{Gal}(F/k)$ . By Lemma 4.2.5 (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  $E$  is a Galois subextension of  $F/k$ , 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  $h \in H$ , the automorphism  $\sigma^{-1} \circ h \circ \sigma \in \text{Gal}(F/k)$  belongs to  $H$ , hence fixes  $x$ . Therefore

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

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

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

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

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

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

PROOF. Let  $F$  be a separable closure of  $k$ , and  $x \in F - k$ . The minimal polynomial  $P \in k[X]$  of  $x$  over  $k$  is separable of degree at least two. Its image in  $F[X]$  thus possesses an irreducible factor  $Q$  such that  $Q(x) \neq 0$ . The field  $F[X]/Q$  is a separable extension of  $F$ , hence equals  $F$ . It follows that  $Q = X - y$  for some  $y \in F$  distinct from  $x$ . Let  $K$  be the subextension of  $F/k$  generated by  $x$ . Then  $X \mapsto x$  induces an isomorphism of  $k$ -algebras  $k[X]/P \simeq K$ , and we may thus define a morphism of  $k$ -algebras  $K \rightarrow F$  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 4.3.12 (i), which is an isomorphism by Lemma 4.3.12 (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 4.3.4).  $\square$

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

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

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

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

#### 4. Galois descent

Let us fix a Galois extension  $F/k$  and denote by  $\Gamma$  the profinite group  $\text{Gal}(F/k)$ . When  $\gamma \in \Gamma$  and  $\lambda \in F$ , we will write  $\gamma\lambda$  instead of  $\gamma(\lambda)$ . In this section, we characterise those  $F$ -vector spaces  $V$  equipped with a  $\Gamma$ -action, which are of the form  $V_0 \otimes_k F$  for some  $k$ -vector space  $V_0$ , and describe how to recover  $V_0$  from  $V$ .

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

LEMMA 4.4.1. *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 of  $W$  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 claim that

$$(4.4.a) \quad x = \sum_{i \in I} e_i \otimes \epsilon_i(x).$$

Indeed this is easily verified when  $x = w \otimes u$  for  $w \in W, u \in U$ , and the general case follows since both sides of the formula are  $k$ -linear. Since each map  $\epsilon_i$  is  $G$ -equivariant, it maps  $(W \otimes_k U)^G$  into  $U^G$ , and the statement follows from (4.4.a).  $\square$

DEFINITION 4.4.2. Let  $V$  be an  $F$ -vector space. A  $\Gamma$ -action on  $V$  is called *semilinear* if for all  $v \in V$  and  $\lambda \in F$  and  $\gamma \in \Gamma$ , we have in  $V$

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

Let  $V, V'$  be  $F$ -vector equipped with a semilinear  $\Gamma$ -action. Then  $V \oplus V'$  and  $V \otimes_F V'$  inherit a semilinear  $\Gamma$ -action. So does  $\text{Hom}_F(V, V')$ , by setting, for  $f \in \text{Hom}_F(V, V')$  and  $\gamma \in \Gamma$

$$(4.4.b) \quad (\gamma f)(u) = \gamma(f(\gamma^{-1}u)) \quad \text{for } u \in U.$$

LEMMA 4.4.3. *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 4.4.1, 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 4.3.8, the elements  $\lambda_1, \dots, \lambda_n$  are contained in some finite Galois subextension  $L$  of  $F/k$ . Then the subgroup  $\text{Gal}(F/L) \subset \Gamma$  is open (Theorem 4.3.11) and fixes  $w$ , proving the continuity (see Lemma 4.2.9).  $\square$

LEMMA 4.4.4 (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  $n \leq \dim_k A$ .*

PROOF. Assume that

$$(4.4.c) \quad a_1 \sigma_1 + \cdots + a_m \sigma_m = 0.$$

where  $a_1, \dots, a_m \in K$  are not all zero. Pick such a relation, where  $m \in \{1, \dots, n\}$  is minimal. In particular  $a_m \neq 0$ , and  $m > 1$ . As  $\sigma_m \neq 0$ , there exists  $i \in \{1, \dots, m-1\}$  such that  $a_i \neq 0$ . 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 (4.4.c) that

$$(4.4.d) \quad a_1 \sigma_1(z) \sigma_1 + \cdots + a_m \sigma_m(z) \sigma_m = 0.$$

Subtracting  $\sigma_m(z)$  times Equation (4.4.c) to (4.4.d) yields

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

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 4.4.5 (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 4.3.2. Namely, assume that the kernel of  $\varphi$  contains a nonzero element  $v = v_1 \otimes \lambda_1 + \cdots + v_r \otimes \lambda_r$  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 the elements  $v_1, \dots, v_r$  are linearly independent over  $k$  and  $0 = \varphi(v) = \lambda_1 v_1 + \cdots + \lambda_r v_r$ , there exists  $j \in \{2, \dots, r\}$  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 subextension  $L$  of  $F/k$  such that  $v$  is fixed by  $\text{Gal}(F/L)$  (see Lemma 4.2.9 and Theorem 4.3.11). Let  $e_1, \dots, e_n$  be a basis of the  $k$ -vector space  $L$ . The group  $\text{Gal}(L/k)$  has cardinality  $n$  (Proposition 4.3.2), and by Lemma 4.3.7 we may find preimages  $\gamma_1, \dots, \gamma_n \subset \Gamma$  of the elements of  $\text{Gal}(L/k)$ . Consider the elements

$$(4.4.e) \quad w_j = \sum_{i=1}^n (\gamma_i e_j)(\gamma_i v) \in V \quad \text{for } j = 1, \dots, n.$$

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 4.4.4. Let  $m_{i,j} \in L$  be the coefficients of its inverse. By (4.4.e), 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  $\varphi$ .  $\square$

REMARK 4.4.6. Let  $A$  be an  $F$ -algebra. Assume that  $\Gamma$  acts continuously by semi-linear automorphisms on the  $F$ -vector space  $A$ , and that the multiplication map of  $A$  is compatible with the  $\Gamma$ -action, in the sense that

$$(\gamma a)(\gamma b) = \gamma(ab) \quad \text{for all } a, b \in A.$$

Then  $A^\Gamma$  is a  $k$ -algebra, and the morphism  $A^\Gamma \otimes_k F \rightarrow A$  is an isomorphism of  $k$ -algebras.





## CHAPTER 5

## 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, a feature providing 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, as they constitute a simple type of torsors, objects which will figure prominently in the next chapter.

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 5.1.1. 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 5.1.2. We will often write  $X \in \mathcal{C}$  to mean that  $X$  is an object of  $\mathcal{C}$ .

REMARK 5.1.3. 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 5.1.4. 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  $\mathcal{B}$ , the following diagram commutes

$$\begin{array}{ccc} \mathcal{F}(B) & \xrightarrow{\varphi_B} & \mathcal{G}(B) \\ \mathcal{F}(f) \downarrow & & \downarrow \mathcal{G}(f) \\ \mathcal{F}(B') & \xrightarrow{\varphi_{B'}} & \mathcal{G}(B') \end{array}$$

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 5.2.1. By Remark 4.3.14, the set  $\mathbf{X}(A)$  does not depend, up to bijection, on the choice of the separable closure  $k_s$  of  $k$ . In particular its cardinality  $|\mathbf{X}(A)| \in \mathbb{N} \cup \{\infty\}$  does not depend on any choice.

LEMMA 5.2.2. *We have  $|\mathbf{X}(A)| \leq \dim_k A$ .*

PROOF. This follows from Dedekind's Lemma 4.4.4.  $\square$

DEFINITION 5.2.3. A commutative  $k$ -algebra  $A$  is called *étale* if it is finite-dimensional and  $|\mathbf{X}(A)| = \dim_k A$ . Decreeing that a morphism of étale  $k$ -algebras is a morphism of  $k$ -algebras between étale algebras, we define the category of étale  $k$ -algebras, which we denote by  $\mathbf{Et}_k$ .

LEMMA 5.2.4. *Let  $K/k$  be a field extension. Then the  $k$ -algebra  $K$  is étale if and only if the extension  $K/k$  is finite and separable.*

PROOF. Since  $K$  is a field, we have  $\dim_k K \geq 1$ . Thus 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, assume that  $K/k$  is finite and separable. Let  $F$  be an algebraic closure of  $k_s$ . There are  $[K : k]$  distinct morphisms of  $k$ -algebras  $K \rightarrow F$  by Lemma 4.3.1 (iii). Let  $f : K \rightarrow F$  be a morphism of  $k$ -algebras. Let  $x \in K$ , and let  $P \in k[X]$  be the minimal polynomial of  $x$  over  $k$ . Then  $P$  is separable, and  $f(x) \in F$  is a root of  $P$ . Therefore  $f(x)$  is separable over  $k$ , hence belongs to  $k_s$ . We have thus produced  $[K : k] = \dim_k K$  distinct elements of  $\mathbf{X}(K)$ .  $\square$

LEMMA 5.2.5. *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 4.3.12 (i) there exists a morphism of  $k$ -algebras  $\sigma : k_s \rightarrow L_s$ . Denote by  $\mu : k_s \otimes_k L \rightarrow L_s$  the morphism of  $k$ -algebras given by  $x \otimes y \mapsto \sigma(x)y$  for  $x \in k_s$  and  $y \in L$ . Every morphism of  $k$ -algebras  $f : A \rightarrow k_s$  induces a morphism of  $L$ -algebras

$$\tilde{f} : A_L \xrightarrow{f_L} (k_s)_L = k_s \otimes_k L \xrightarrow{\mu} L_s,$$

which fits into the commutative diagram

$$\begin{array}{ccc} A_L & \xrightarrow{\tilde{f}} & L_s \\ a \mapsto a \otimes 1 \uparrow & & \uparrow \sigma \\ A & \xrightarrow{f} & k_s \end{array}$$

Since  $\sigma$  is injective (as  $k_s$  is a field), we see that if  $f, g \in \mathbf{X}(A)$  are such that  $\tilde{f} = \tilde{g}$ , then  $f = g$ . Therefore  $|\mathbf{X}(A_L)| \geq |\mathbf{X}(A)| = \dim_k A = \dim_L A_L$ .  $\square$

PROPOSITION 5.2.6. *Assume that  $k = k_s$ , and let  $A$  be an étale  $k$ -algebra. Let  $M$  be the set of maps  $\mathbf{X}(A) \rightarrow k$ , with its  $k$ -algebra structure given by pointwise operations. Then the morphism of  $k$ -algebras  $A \rightarrow M$  sending  $a \in A$  to the map  $f \mapsto f(a)$  is an isomorphism.*

PROOF. Let  $n = \dim_k A$ . By Dedekind's Lemma 4.4.4, the  $n$  elements of  $\mathbf{X}(A)$  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 the statement is injective, hence bijective by dimensional reasons.  $\square$

COROLLARY 5.2.7. *If  $k$  is separably closed, then every étale  $k$ -algebra is isomorphic to  $k^n$  for some integer  $n$ .*

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 5.2.8. 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 5.2.9. *An étale  $k$ -algebra is reduced.*

PROOF. Let  $A$  be a finite-dimensional  $k$ -algebra. If  $x$  is a nilpotent element of  $A$ , every morphism of  $k$ -algebras  $A \rightarrow k_s$  maps  $x$  to zero, hence factors uniquely through the quotient morphism  $A \rightarrow A/xA$ . In other words, the natural 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 5.2.10. *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 the  $k$ -algebras  $A$  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 3.1.2, 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 5.2.2.  $\square$

PROPOSITION 5.2.11. *Every commutative reduced finite-dimensional  $k$ -algebra is a product of field extensions of  $k$ .*

PROOF. Let  $A$  be such an algebra. Let  $I$  be the intersection of maximal ideals of  $A$ . Since  $A$  is artinian, we can find<sup>1</sup> a finite set of maximal ideals  $M$  of  $A$  such that  $I = \bigcap_{\mathfrak{m} \in M} \mathfrak{m}$ . Consider the natural morphism of  $k$ -algebras

$$\psi: A \rightarrow \prod_{\mathfrak{m} \in M} A/\mathfrak{m}.$$

If  $\mathfrak{m}, \mathfrak{m}'$  are distinct elements of  $M$ , we have  $1 \in \mathfrak{m} + \mathfrak{m}'$ . This yields an element  $e_{\mathfrak{m}, \mathfrak{m}'} \in \mathfrak{m}'$  such that  $e_{\mathfrak{m}, \mathfrak{m}'} = 1 \pmod{\mathfrak{m}}$ . The element

$$e_{\mathfrak{m}} = \prod_{\mathfrak{m}' \in M - \{\mathfrak{m}\}} e_{\mathfrak{m}, \mathfrak{m}'} \in A$$

has image 1 in  $A/\mathfrak{m}$ , and 0 in  $A/\mathfrak{m}'$  for  $\mathfrak{m} \in M - \{\mathfrak{m}\}$ . It follows that the  $A$ -module  $\prod_{\mathfrak{m} \in M} A/\mathfrak{m}$  is generated by the elements  $\psi(e_{\mathfrak{m}})$  for  $\mathfrak{m} \in M$ . Since the morphism  $\psi$  is  $A$ -linear, we conclude that  $\psi$  is surjective.

<sup>1</sup>the set of maximal ideals of  $A$  is actually finite, but we will not need this fact.

Let now  $x \in I$ . Then, as  $A$  is artinian, we can find  $n \in \mathbb{N}$  such that the elements  $x^n$  and  $x^{n+1}$  generate the same ideal of  $A$ . This yields  $a \in A$  such that  $x^n = ax^{n+1}$ , and thus  $x^n(1 - ax) = 0$ . If  $1 - ax \in \mathfrak{m}$  for some maximal ideal  $\mathfrak{m}$  of  $A$ , then  $1 \in \mathfrak{m} + I = \mathfrak{m}$ , hence  $\mathfrak{m} = A$ , a contradiction. Thus  $1 - ax$  belongs to no maximal ideal of  $A$ , in other words  $1 - ax \in A^\times$ . We deduce that  $x^n = 0$ , hence  $x = 0$  since  $A$  is reduced. As  $I = \ker \psi$ , this proves the injectivity of  $\psi$ .  $\square$

COROLLARY 5.2.12. *Every étale  $k$ -algebra is a finite product of field extensions of  $k$ .*

PROOF. This follows from Lemma 5.2.9 and Proposition 5.2.11.  $\square$

We are now in position to formulate the main result of this section, we provides various characterisations of étale algebras.

PROPOSITION 5.2.13. *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 isomorphic to 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)  $\Rightarrow$  (ii) : This follows from Lemma 5.2.5 and Corollary 5.2.7.

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

(iii)  $\Rightarrow$  (i) : This follows from Lemma 5.2.10 (ii) and Lemma 5.2.4.

(i)  $\Rightarrow$  (v) : This follows from Lemma 5.2.5 and Lemma 5.2.9.

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

(iv)  $\Rightarrow$  (iii) : The  $k$ -algebra  $A$  is a finite product of field extensions by Proposition 5.2.11. Let  $K/k$  be one of these field extensions, 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 of  $x$  over  $k$ . 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 5.2.8). This implies that  $P \in k[X]$  is separable : indeed if  $P = (X - a)Q \in \bar{k}[X]$  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  $\bar{k}[X]/P$ .  $\square$

The characterisations of Proposition 5.2.13 can be used to provide a simple proof of the fact that the property of being étale “descends” under extension of the base field.

COROLLARY 5.2.14. *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 4.3.12 (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 5.2.13), hence so is its subring  $A_{\bar{k}}$ . This proves that  $A$  is étale by the criterion (iv) in Proposition 5.2.13.  $\square$

### 3. Characteristic polynomials in étale algebras

In this section, we provide explicit formulas computing the norm and trace of elements of étale algebras. As an application, we deduce transitivity properties of the norm and trace maps. We will consider more generally characteristic polynomials of elements of

étale algebras, of which the norm and trace are specific coefficients. This permits to prove statements for the norm and trace simultaneously, as well as generalise them to the other coefficients of the characteristic polynomial.

DEFINITION 5.3.1. Let  $A$  be a finite-dimensional  $k$ -algebra, and  $n = \dim_k A$ . The *characteristic polynomial* of an element  $a \in A$  is the polynomial

$$\text{Cp}_{A/k}(a) = \det(X \text{id}_A - l_a) \in k[X],$$

where  $l_a: A \rightarrow A$  is the map given by  $x \mapsto ax$  (viewed as a  $k$ -linear map). Writing this polynomial as  $a_n X^n + \dots + a_0$  where  $a_0, \dots, a_n \in k$ , we define the norm and trace of  $a$  as

$$N_{A/k}(a) = (-1)^n a_0 \quad \text{and} \quad \text{Tr}_{A/k}(a) = -a_{n-1}.$$

Observe that if  $K/k$  is a field extension, then for any  $a \in A$

$$\text{Cp}_{A_K/K}(a \otimes 1) = \text{Cp}_{A/k}(a) \in k \subset K.$$

PROPOSITION 5.3.2. *Let  $A$  be an étale  $k$ -algebra. Then for any  $a \in A$ , we have*

$$\text{Cp}_{A/k}(a) = \prod_{f \in \mathbf{X}(A)} (X - f(a)).$$

*In particular*

$$N_{A/k}(a) = \prod_{f \in \mathbf{X}(A)} f(a) \quad \text{and} \quad \text{Tr}_{A/k}(a) = \sum_{f \in \mathbf{X}(A)} f(a).$$

PROOF. We may replace  $k$  with  $k_s$ , and thus by Proposition 5.2.6 assume that  $A$  admits a  $k$ -basis  $e_f$  for  $f \in \mathbf{X}(A)$  such that  $e_f e_g = 0$  if  $f \neq g$  and  $e_f^2 = e_f$ , and for every  $a \in A$

$$a = \sum_{f \in \mathbf{X}(A)} f(a) e_f.$$

Then  $ae_f = f(a)e_f$  for every  $f \in \mathbf{X}(A)$ . Computing the characteristic polynomial using the basis  $e_f$  for  $f \in \mathbf{X}(A)$  yields the result.  $\square$

COROLLARY 5.3.3. *Let  $K/k$  be a finite separable field extension and  $A$  a finite-dimensional  $K$ -algebra. Then the  $K$ -algebra  $A$  is étale if and only if the  $k$ -algebra  $A$  is étale. If this is the case, we have*

$$N_{K/k} \circ N_{A/K} = N_{A/k} \quad \text{and} \quad \text{Tr}_{K/k} \circ \text{Tr}_{A/K} = \text{Tr}_{A/k}.$$

PROOF. Let  $K_s$  be a separable closure of  $K$  and denote by  $\mathbf{X}(A/K)$  the set of morphisms of  $K$ -algebras  $A \rightarrow K_s$ . For each  $f \in \mathbf{X}(K)$  choose a morphism of  $k$ -algebras  $\tilde{f}: K_s \rightarrow k_s$  extending  $f$  (this is possible by Lemma 4.3.12 (i)). Consider the map

$$\alpha: \mathbf{X}(K) \times \mathbf{X}(A/K) \rightarrow \mathbf{X}(A) \quad ; \quad (f, g) \mapsto \tilde{f} \circ g.$$

If  $f, f' \in \mathbf{X}(K)$  and  $g, g' \in \mathbf{X}(A/K)$  are such that  $\tilde{f} \circ g = \tilde{f}' \circ g': A \rightarrow k_s$ , composing with the unique morphism of  $K$ -algebras  $K \rightarrow A$  we see that  $f = f'$ . Therefore  $\tilde{f} = \tilde{f}'$ , hence  $g = g'$  (by injectivity of  $\tilde{f}$ ), proving that  $\alpha$  is injective.

Now let  $h \in \mathbf{X}(A)$ . Let  $f \in \mathbf{X}(K)$  be the restriction of  $h$  along the inclusion  $K \subset A$ . Let us view  $k_s$  as a  $K$ -algebra via  $f$ . Then  $h: A \rightarrow k_s$  is a morphism of  $K$ -algebras, and  $\tilde{f}: K_s \rightarrow k_s$  is an isomorphism of  $K$ -algebras by Lemma 4.3.12 (ii). So we may set  $g = \tilde{f}^{-1} \circ h \in \mathbf{X}(A/K)$ . Then  $\tilde{f} \circ g = h$ , proving that  $\alpha$  is surjective.

Thus, using Lemma 5.2.2,

$$|\mathbf{X}(A/K)| \cdot |\mathbf{X}(K)| = |\mathbf{X}(A)| \leq \dim_k A = \dim_K A \cdot [K : k] = \dim_K A \cdot |\mathbf{X}(K)|,$$

we see that the  $k$ -algebra  $A$  is étale if and only if the  $K$ -algebra  $A$  is étale.

Assume that this is the case. We use the fact the every element of  $\mathbf{X}(A)$  is of the form  $\tilde{f} \circ g \in \mathbf{X}(A)$  for  $f \in \mathbf{X}(K)$  and  $g \in \mathbf{X}(A/K)$ . If  $a \in A$  then, in view of Proposition 5.3.2

$$\begin{aligned} N_{K/k} \circ N_{A/K}(a) &= \prod_{f \in \mathbf{X}(K)} f \left( \prod_{g \in \mathbf{X}(A/K)} g(a) \right) \\ &= \prod_{f \in \mathbf{X}(K)} \prod_{g \in \mathbf{X}(A/K)} \tilde{f} \circ g(a) \\ &= \prod_{h \in \mathbf{X}(A)} h(a) \\ &= N_{A/k}(a), \end{aligned}$$

and similarly

$$\begin{aligned} \mathrm{Tr}_{K/k} \circ \mathrm{Tr}_{A/K}(a) &= \sum_{f \in \mathbf{X}(K)} f \left( \sum_{g \in \mathbf{X}(A/K)} g(a) \right) \\ &= \sum_{f \in \mathbf{X}(K)} \sum_{g \in \mathbf{X}(A/K)} \tilde{f} \circ g(a) \\ &= \sum_{h \in \mathbf{X}(A)} h(a) \\ &= \mathrm{Tr}_{A/k}(a). \end{aligned} \quad \square$$

REMARK 5.3.4. Corollary 5.3.3 can be generalised using other methods to the case when  $K/k$  is a finite field extension and  $A$  an arbitrary finite-dimensional  $k$ -algebra.

#### 4. Finite sets with a Galois action

Let us write  $\Gamma = \mathrm{Gal}(k_s/k)$ . Let  $A$  be a  $k$ -algebra. If  $f \in \mathbf{X}(A)$  and  $\gamma \in \Gamma$ , we set  $\gamma f = \gamma \circ f \in \mathbf{X}(A)$ . This defines a left action of the group  $\Gamma$  on the set  $\mathbf{X}(A)$ .

LEMMA 5.4.1. *Let  $A$  be a finite-dimensional  $k$ -algebra. Then the  $\Gamma$ -action on  $\mathbf{X}(A)$  is continuous (Definition 4.2.10).*

PROOF. Let  $f \in \mathbf{X}(A)$ . Since  $A$  is finite-dimensional over  $k$ , the subalgebra  $L = f(A) \subset k_s$  is a field (Lemma 3.1.2), of finite degree as an extension of  $k$ . The open subgroup  $\mathrm{Gal}(k_s/L)$  fixes  $f$ , and the statement follows from Lemma 4.2.9.  $\square$

Let us denote by  $\mathbf{Fsets}_\Gamma$  the category whose objects are finite discrete  $\Gamma$ -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, the map  $\mathbf{X}(B) \rightarrow \mathbf{X}(A)$  given by  $f \mapsto f \circ \varphi$  is  $\Gamma$ -equivariant, and one sees easily that  $\mathbf{X}$  defines a contravariant functor  $\mathbf{Et}_k \rightarrow \mathbf{Fsets}_\Gamma$ .

Let now  $X$  be a finite discrete  $\Gamma$ -set of cardinality  $n$ . The set

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



is naturally a commutative  $k_s$ -algebra (via pointwise operations), which is isomorphic to  $(k_s)^n$ . The  $\Gamma$ -actions on  $k_s$  and  $X$  induce a left  $\Gamma$ -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  $\mathbf{M}(X)^\Gamma$  coincides with the subset of  $\Gamma$ -equivariant maps  $X \rightarrow k_s$ .

LEMMA 5.4.2. *If  $X$  is a finite discrete  $\Gamma$ -set, the  $\Gamma$ -action on  $\mathbf{M}(X)$  is continuous and semilinear (Definition 4.4.2).*

PROOF. Let  $\gamma \in \Gamma$  and  $f \in \mathbf{M}(X)$ . For any  $x \in X$  and  $\lambda \in k_s$ , 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 4.4.5 that the natural morphism of  $k_s$ -algebras

$$(5.4.a) \quad \mathbf{M}(X)^\Gamma \otimes_k k_s \rightarrow \mathbf{M}(X)$$

is bijective. Since  $\mathbf{M}(X) \simeq (k_s)^n$ , we conclude that  $\mathbf{M}(X)^\Gamma$  is an étale  $k$ -algebra of dimension  $n$  (see Proposition 5.2.13). To a map of finite discrete  $\Gamma$ -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  $\mathbf{Fsets}_\Gamma \rightarrow \mathbf{Et}_k$ .

Let  $A$  be a  $k$ -algebra. If  $a \in A$ , then the map  $\Phi_A(a): \mathbf{X}(A) \rightarrow k_s$  given by  $f \mapsto f(a)$  is  $\Gamma$ -equivariant. We thus define a morphism of  $k$ -algebras

$$\Phi_A: A \rightarrow \mathbf{M}^\Gamma(\mathbf{X}(A)).$$

LEMMA 5.4.3. *Let  $A$  be a finite-dimensional  $k$ -algebra. Then  $A$  is étale if and only if  $\Phi_A$  is an isomorphism.*

PROOF. Since the  $k$ -algebra  $\mathbf{M}^\Gamma(\mathbf{X}(A))$  is étale, so will be  $A$  if  $\Phi_A$  is an isomorphism. Conversely if  $A$  is étale, the composite

$$A_{k_s} = A \otimes_k k_s \xrightarrow{\Phi_A \otimes_k k_s} \mathbf{M}^\Gamma(\mathbf{X}(A)) \otimes_k k_s \xrightarrow{(5.4.a)} \mathbf{M}(\mathbf{X}(A)) = \mathbf{M}(\mathbf{X}(A_{k_s}))$$

sends  $a$  to  $f \mapsto f(a)$ , hence is an isomorphism by Proposition 5.2.6 (applied to the  $k_s$ -algebra  $A_{k_s}$ ). It follows that  $\Phi_A \otimes_k k_s$  is an isomorphism, hence so is  $\Phi_A$  (exercise).  $\square$

We can now establish our first interesting equivalence of categories.

THEOREM 5.4.4. *Let  $\Gamma = \text{Gal}(k_s/k)$ . The functors  $\mathbf{X}$  and  $\mathbf{M}^\Gamma$  define a contravariant equivalence of categories  $\mathbf{Et}_k \simeq \mathbf{Fsets}_\Gamma$ .*

PROOF. Let  $X$  be a finite discrete  $\Gamma$ -set. Consider the map

$$\Psi_X: X \rightarrow \mathbf{X}(\mathbf{M}(X)^\Gamma)$$

mapping  $x \in X$  to the morphism of  $k$ -algebras  $\mathbf{M}(X)^\Gamma \rightarrow k_s$  given by  $f \mapsto f(x)$ . For  $\gamma \in \Gamma$  and  $x \in X$ , we have for all  $f \in \mathbf{M}(X)^\Gamma$

$$\Psi_X(\gamma x)(f) = f(\gamma x) = \gamma(f(x)) = \gamma(\Psi_X(x)(f)),$$

so that the map  $\Psi_X$  is  $\Gamma$ -equivariant. This map is also injective: if  $f(x) = f(x')$  for all  $f \in \mathbf{M}(X)$ , taking for  $f$  the map

$$y \mapsto \begin{cases} 1 & \text{if } y = x, \\ 0 & \text{otherwise,} \end{cases}$$

we see that  $x = x'$ . Since the source and target of the map  $\Psi_X$  have the same finite number of elements, the map  $\Psi_X$  is bijective.

Conversely, we have seen in Lemma 5.4.3 that the morphism  $\Phi_A: A \rightarrow \mathbf{M}^\Gamma(\mathbf{X}(A))$  is bijective when  $A$  is étale  $k$ -algebra.

To conclude note that  $\Psi$  and  $\Phi$  in fact define functors.  $\square$

The theorem implies that operations on étale algebras correspond bijectively to operations on finite discrete  $\Gamma$ -sets, and that properties of objects in one category can be read off on the other category. Here are a few examples:

REMARK 5.4.5. If  $X, Y$  are finite discrete  $\Gamma$ -sets, there are natural  $\Gamma$ -equivariant isomorphisms of  $k$ -algebras

$$\mathbf{M}^\Gamma(X \sqcup Y) \simeq \mathbf{M}^\Gamma(X) \times \mathbf{M}^\Gamma(Y) \quad ; \quad \mathbf{M}^\Gamma(X \times Y) \simeq \mathbf{M}^\Gamma(X) \otimes_k \mathbf{M}^\Gamma(Y).$$

Thus under the equivalence of Theorem 5.4.4 disjoint unions, resp. direct products, of finite discrete  $\Gamma$ -sets correspond to direct products, resp. tensor products, of étale  $k$ -algebras.

REMARK 5.4.6. A nonzero étale  $k$ -algebra  $A$  is a field if and only if  $\Gamma$  acts transitively on the set  $\mathbf{X}(A)$ . Indeed, as  $A$  is a product of fields by Corollary 5.2.12, this follows from Remark 5.4.5.

REMARK 5.4.7. Assume that  $\Gamma$  acts trivially on the finite set  $X$ . Then  $\mathbf{M}^\Gamma(X)$  may be identified with the  $k$ -algebra consisting of the maps  $X \rightarrow k$ . In particular  $\mathbf{M}^\Gamma(X) \simeq k^n$  as  $k$ -algebra, where  $n = |X|$ .

## 5. Galois algebras

In this section we fix a finite group  $G$ . As before  $k_s$  denotes a separable closure of  $k$ , and we write  $\Gamma = \text{Gal}(k_s/k)$ .

DEFINITION 5.5.1. A commutative  $k$ -algebra endowed with a left action of  $G$  by automorphisms of  $k$ -algebras will be called a  $G$ -algebra (over  $k$ ). A morphism of  $G$ -algebras is a  $G$ -equivariant morphism of  $k$ -algebras between  $G$ -algebras.

If  $A$  is a  $G$ -algebra, then the set  $\mathbf{X}(A)$  is naturally equipped with a right  $G$ -action by  $\Gamma$ -equivariant permutations. Explicitly for  $g \in G$  and  $f \in \mathbf{X}(A)$ , we have  $f \cdot g = f \circ g$ . Conversely, if  $X$  is discrete  $\Gamma$ -set with a right  $G$ -action, then  $\mathbf{M}^\Gamma(X)$  is a  $G$ -algebra.

PROPOSITION 5.5.2. *Let  $A$  be a nonzero étale  $G$ -algebra over  $k$ . Then the following are equivalent:*

- (i)  $A^G = k$ ,
- (ii)  $G$  acts transitively on  $\mathbf{X}(A)$ .

PROOF. We use the correspondence established in Theorem 5.4.4. Let  $X = \mathbf{X}(A)$ , and consider the discrete  $\Gamma$ -set  $Y = X/G$ . Since a map  $Y \rightarrow k_s$  is the same thing as a map  $X \rightarrow k_s$  which is  $G$ -invariant as an element of  $\mathbf{M}(X) = A_{k_s}$ , we have

$$\mathbf{M}^\Gamma(Y) = \mathbf{M}^\Gamma(X/G) = \mathbf{M}^\Gamma(X)^G = A^G.$$

It follows that  $A^G$  is an étale  $k$ -algebra such that  $\mathbf{X}(A^G) = Y$ . Thus  $A^G = k$  if and only if  $Y$  is a single point, i.e.  $G$  acts transitively on  $X$  (recall that  $X$  is nonempty, since  $A$  is nonzero).  $\square$

DEFINITION 5.5.3. Let  $A$  be an étale  $G$ -algebra over  $k$ . We say that  $A$  is a *Galois  $G$ -algebra* (over  $k$ ) if the following conditions hold:

- (a)  $A^G = k$ ,
- (b)  $\dim_k A = |G|$ .

A morphism of Galois  $G$ -algebras is a morphism of  $G$ -algebras between Galois  $G$ -algebras. We have thus defined the category of Galois  $G$ -algebras (over  $k$ ).

If  $L/k$  is a field extension, it follows from Lemma 4.4.1, Corollary 5.2.14 and Lemma 5.2.5 that a  $G$ -algebra  $A$  is Galois over  $k$  if and only if  $A_L$  is Galois over  $L$ .

EXAMPLE 5.5.4. Let  $L/k$  be a field extension of finite degree. The following may be deduced from Proposition 4.3.2. If the field extension  $L/k$  is Galois, then  $L$  is a Galois  $\text{Gal}(L/k)$ -algebra over  $k$ . Conversely, if  $L$  is a  $G$ -algebra, then  $L/k$  is a Galois field extension, and the morphism  $G \rightarrow \text{Gal}(L/k)$  is bijective.

EXAMPLE 5.5.5. Consider the set  $S$  consisting of all maps  $G \rightarrow k$ , with the  $k$ -algebra structure given by pointwise operations. The group  $G$  naturally acts on  $S$ : if  $f$  is a map  $G \rightarrow k$  and  $g \in G$ , then  $g \cdot f$  is the map  $G \rightarrow k$  given by  $x \mapsto f(x \cdot g)$ . The  $k$ -algebra  $S$  is isomorphic to  $k^{|G|}$ , hence is étale of dimension  $|G|$ . Moreover  $S^G$  is the set of constant maps  $G \rightarrow k$ , which coincides with  $k \subset S$ . Therefore  $S$  is a Galois  $G$ -algebra. We have  $\mathbf{X}(S) = G$  with the trivial  $\Gamma$ -action (see Remark 5.4.7), and the  $G$ -action given by right multiplication.

The correspondence between étale  $k$ -algebras and finite discrete  $\Gamma$ -sets admits the following specialisation to the Galois  $G$ -algebras:

PROPOSITION 5.5.6. *The functors  $\mathbf{X}$  and  $\mathbf{M}^\Gamma$  induce a contravariant equivalence between the categories of Galois  $G$ -algebras and the category of nonempty finite discrete  $\Gamma$ -sets with a simply transitive  $G$ -action.*

PROOF. In view of the correspondence of Theorem 5.4.4, this follows from Proposition 5.5.2, since a transitive  $G$ -action on a set of cardinality  $|G|$  is simply transitive, and conversely any nonempty set with a simply transitive  $G$ -action has cardinality  $|G|$ .  $\square$

DEFINITION 5.5.7. We say that a Galois  $G$ -algebra  $A$  is *split* if  $\Gamma$  acts trivially on the set  $\mathbf{X}(A)$ .

It follows from Proposition 5.5.6 that a Galois  $G$ -algebra is split if and only if it is isomorphic to the algebra  $S$  of Example 5.5.5.

Had we defined Galois  $G$ -algebras over commutative algebras (as opposed to just fields), the next statement would assert that a Galois algebra splits when scalars are extended to itself.

PROPOSITION 5.5.8. *Let  $A$  be a Galois  $G$ -algebra, and consider the split  $G$ -algebra  $S$  of Example 5.5.5. Then there is an isomorphism of  $k$ -algebras  $A \otimes_k A \simeq S \otimes_k A$ , which is  $G$ -equivariant for the actions via the first factors, and  $A$ -linear for the module structures via the second factors.*

PROOF. Let  $X = \mathbf{X}(A)$ . Since  $G$  act simply transitively on  $X$ , the map  $\alpha: G \times X \rightarrow X \times X$  given by  $(g, x) \mapsto (x \cdot g, x)$  is bijective. It is  $\Gamma$ -equivariant, if we let  $\Gamma$  act trivially on  $G$ . Under the equivalence of Theorem 5.4.4, this yields an isomorphism of  $k$ -algebras  $\beta: A \otimes_k A \rightarrow S \otimes_k A$ . Since  $\alpha$  is  $G$ -equivariant for the right  $G$ -actions via the first factors, it follows that  $\beta$  is  $G$ -equivariant for the left  $G$ -actions via the first factors.

To prove the last statement, note that the composite  $G \times X \xrightarrow{\alpha} X \times X \rightarrow X$ , where the last map is the second projection, coincides with the projection  $G \times X \rightarrow X$ . Therefore the composite  $A \rightarrow A \otimes_k A \rightarrow S \otimes_k A$ , where the first map is  $a \mapsto 1 \otimes a$ , coincides with the morphism of  $k$ -algebras  $A \rightarrow S \otimes_k A$  given by  $a \mapsto 1 \otimes a$ .  $\square$

Proposition 5.5.8 will be exploited via the next corollary.

COROLLARY 5.5.9. *Let  $A$  be a Galois  $G$ -algebra, and  $A \rightarrow K$  a morphism of  $k$ -algebras, where  $K$  is a field. Then the Galois  $G$ -algebra  $A_K$  over  $K$  is split.*

PROOF. Let  $f: A \rightarrow K$  be the morphism. Since the image of  $f$  is a field (by Lemma 3.1.2), we may replace  $K$  with the image of  $f$ , and thus assume that  $f$  is surjective. Let  $I = \ker f$ , so that  $A/I = K$ . Then the isomorphism of  $A$ -modules  $\beta: A \otimes_k A \rightarrow S \otimes_k A$  of Proposition 5.5.8 induces an isomorphism of  $K$ -vector spaces  $\beta': A \otimes_k K \rightarrow S \otimes_k K$ , and it follows from Proposition 5.5.8 that  $\beta'$  is a morphism of  $G$ -algebras over  $K$ .  $\square$

We conclude this section with formulas expressing traces, resp. norms, in Galois  $G$ -algebras in terms of sums, resp. products, of “conjugates”, which generalise the familiar case of Galois field extensions.

PROPOSITION 5.5.10. *Let  $A$  be a Galois  $G$ -algebra. Then for any  $a \in A$ , we have in  $k[X]$  (using the notation of Definition 5.3.1)*

$$\mathrm{Cp}_{A/k}(a) = \prod_{g \in G} (X - g \cdot a).$$

*In particular, we have in  $k$ ,*

$$\mathrm{N}_{A/k}(a) = \prod_{g \in G} g \cdot a \quad \text{and} \quad \mathrm{Tr}_{A/k}(a) = \sum_{g \in G} g \cdot a.$$

PROOF. Pick an element  $f$  in the nonempty set  $\mathbf{X}(A)$ . Then  $\mathbf{X}(A) = \{f \circ g | g \in G\}$ , hence the formula follows from Proposition 5.3.2.  $\square$



## CHAPTER 6

**Torsors, cocycles, and twisted forms**

In this chapter we introduce the notion of torsor (also called principal homogeneous space), under a group  $G$  equipped with a continuous action of the absolute Galois group. Such objects coincide with  $G$  as sets, but carry a different Galois action.

Torsors naturally appear in the study of twisted forms of algebraic objects, that is, objects defined over a base field, which become isomorphic to a given object (called split) over the separable closure of the base field. In this situation, the group  $G$  is the automorphism group of the split object. Examples of twisted forms include étale algebras, Galois algebras, finite-dimensional central simple algebras, nondegenerate quadratic forms,...

A related notion is that of 1-cocycles. These objects provide a more computational approach to torsors, and admit higher dimensional generalisations which will be explored in the next chapters. The set of 1-cocycles is endowed with a natural equivalence relation, so that the set of equivalence classes (called the first cohomology set) is in bijection with the set of isomorphism classes of twisted forms, or of torsors. An important subtlety is that twisted forms correspond to torsors, but not to 1-cocycles; this is only true “up to isomorphism”, and therefore some care is required when working with twisted forms and 1-cocycles. Another pitfall is that, as one might expect, the cohomology of various groups are related by exact sequences, but these are only sequences of pointed sets. In particular such sequences only provide information concerning the fiber over the split object.

**1. Torsors**

In this section  $\Gamma$  is a profinite group, and  $G$  a discrete  $\Gamma$ -group (Definition 4.2.10). We will denote  $\Gamma$ -actions on a set by  $x \mapsto \gamma x$  for  $\gamma \in \Gamma$ , and left, resp. right,  $G$ -actions by  $x \mapsto g \cdot x$ , resp.  $x \mapsto x \cdot g$ , for  $g \in G$ . In particular, the group operation in  $G$  will be denoted by  $(g, h) \mapsto g \cdot h$ .

DEFINITION 6.1.1. A left  $G$ -action on a discrete  $\Gamma$ -set  $X$  is called *compatible* if

$$\gamma(g \cdot x) = (\gamma g) \cdot (\gamma x) \quad \text{for } x \in X \text{ and } g \in G.$$

Similarly, a right  $G$ -action on a discrete  $\Gamma$ -set  $X$  is called *compatible* if

$$\gamma(x \cdot g) = (\gamma x) \cdot (\gamma g) \quad \text{for } x \in X \text{ and } g \in G.$$

DEFINITION 6.1.2. Let  $P$  be a discrete  $\Gamma$ -set equipped with a compatible right  $G$ -action. We say that  $P$  is a  $G$ -torsor if  $P$  is nonempty and the  $G$ -action on  $P$  is simply transitive. A morphism of  $G$ -torsors is a map between torsors compatible with the  $\Gamma$ - and  $G$ -actions. We have thus defined the category of  $G$ -torsors.

Observe that a morphism of  $G$ -torsors is always bijective (because of the simple transitivity of the  $G$ -action), and the inverse map is automatically  $\Gamma$ - and  $G$ -equivariant. Thus all morphisms of  $G$ -torsors are isomorphisms.

EXAMPLE 6.1.3. Let  $\Gamma = \text{Gal}(k_s/k)$ , and  $G$  a finite group considered as a discrete  $\Gamma$ -group with trivial  $\Gamma$ -action. We have seen in Proposition 5.5.6 that the category of  $G$ -torsors is equivalent to the opposite of the category of Galois  $G$ -algebras over  $k$ .

Let  $X$  be a discrete  $\Gamma$ -set with a compatible left  $G$ -action, and let  $P$  be a  $G$ -torsor. We now describe a procedure that yields another discrete  $\Gamma$ -set  ${}_P X$ , called *the twist of  $X$  by  $P$* .

DEFINITION 6.1.4. We define an equivalence relation on the set  $P \times X$  by letting  $(p, x)$  be equivalent to  $(p \cdot g, g^{-1} \cdot x)$ , whenever  $p \in P, x \in X, g \in G$ . The set of equivalence classes will be denoted by  ${}_P X$ .

Setting  $\gamma(p, x) = (\gamma p, \gamma x)$  for  $p \in P, x \in X, \gamma \in \Gamma$  defines a  $\Gamma$ -action on the set  ${}_P X$ .

LEMMA 6.1.5. *The  $\Gamma$ -action on  ${}_P X$  is continuous.*

PROOF. Let  $(p, x)$  be an arbitrary element of  ${}_P X$ , where  $p \in P$  and  $x \in X$ . By continuity of the  $\Gamma$ -actions on  $P$  and  $X$ , there are open subgroups  $U$  and  $V$  in  $\Gamma$  fixing respectively  $p$  and  $x$ . Then  $U \cap V$  is an open subgroup in  $\Gamma$  which fixes  $(p, x) \in {}_P X$ .  $\square$

To each element  $p \in P$  correspond a bijection

$$(6.1.a) \quad \pi_p: X \rightarrow {}_P X, \quad x \mapsto (p, x).$$

This map is not  $\Gamma$ -equivariant in general; in fact we have for any  $p \in P, x \in X, \gamma \in \Gamma$ ,

$$(6.1.b) \quad \pi_p(\gamma x) = \gamma \pi_{\gamma^{-1}p}(x).$$

Also observe that, for any  $p \in P, x \in X, g \in G$ ,

$$(6.1.c) \quad \pi_p(g \cdot x) = \pi_{p \cdot g}(x).$$

Let now  $F/k$  be a Galois field extension, and  $\Gamma = \text{Gal}(F/k)$ . Assume that  $V$  is an  $F$ -vector space, equipped with a semilinear continuous left  $\Gamma$ -action and a compatible left  $G$ -action by  $F$ -automorphisms. Then the set  ${}_P V$  is naturally an  $F$ -vector space, the  $\Gamma$ -action on  ${}_P V$  is semilinear, and for  $p \in P$  the map  $\pi_p: V \rightarrow {}_P V$  is  $F$ -linear. The set  $\text{Hom}_F(V, {}_P V)$  is naturally endowed with a  $\Gamma$ -action, given by the formula of (4.4.b). Setting, for  $g \in G$  and  $f \in \text{Hom}_F(V, {}_P V)$

$$(f \cdot g)(v) = f(g \cdot v) \quad \text{for } v \in V,$$

defines a right  $G$ -action on the set  $\text{Hom}_F(V, {}_P V)$ .

LEMMA 6.1.6. *The map  $P \rightarrow \text{Hom}_F(V, {}_P V)$  given by  $p \mapsto \pi_p$  is  $\Gamma$ - and  $G$ -equivariant.*

PROOF. This follows from (6.1.b) and (6.1.c).  $\square$

## 2. Twisted forms

Let us denote by  $\text{Sep}_k$  the category of separable field extensions<sup>1</sup> of  $k$ , a morphism between two such extensions being just a morphism of  $k$ -algebras. Let  $\mathcal{F}$  be a functor  $\text{Sep}_k \rightarrow \text{Sets}$ . For any  $L \in \text{Sep}_k$ , the group  $\text{Aut}_{k\text{-alg}}(L)$  naturally acts on  $\mathcal{F}(L)$ ; explicitly if  $\gamma \in \text{Aut}_{k\text{-alg}}(L)$  and  $x \in \mathcal{F}(L)$ , then  $\gamma x = \mathcal{F}(\gamma)(x)$ .

<sup>1</sup>recall that for us a separable field extension is algebraic.

DEFINITION 6.2.1. We will say that  $\mathcal{F}$  is a sheaf of sets, or simply a  $k$ -set (this terminology is nonstandard), if for all morphisms  $K \rightarrow L$  in  $\mathbf{Sep}_k$  with  $L/K$  Galois, the  $\mathrm{Gal}(L/K)$ -action on the set  $\mathcal{F}(L)$  is continuous, and the map

$$\mathcal{F}(K) \rightarrow \mathcal{F}(L)^{\mathrm{Gal}(L/K)}$$

is bijective. A morphism of  $k$ -sets is just a morphism of functors between  $k$ -sets. The notion of  $k$ -groups is defined similarly.

REMARK 6.2.2. Let  $k_s$  be a separable closure of  $k$ , and  $\Gamma = \mathrm{Gal}(k_s/k)$ . Observe that if  $\mathcal{F}$  a  $k$ -set, then  $\mathcal{F}(k_s)$  is a discrete  $\Gamma$ -set. Conversely let  $X$  be a discrete  $\Gamma$ -set. For  $L \in \mathbf{Sep}_k$  and  $\varphi \in \mathrm{Hom}_{k\text{-alg}}(L, k_s)$ , let us set  $X_\varphi = X^{\mathrm{Gal}(k_s/\varphi(L))}$ . Let  $L \rightarrow L'$  be a morphism in  $\mathbf{Sep}_k$ . By Lemma 4.3.12, there exist  $\varphi \in \mathrm{Hom}_{k\text{-alg}}(L, k_s)$  and  $\varphi' \in \mathrm{Hom}_{k\text{-alg}}(L', k_s)$ , and for any such pair there exists  $\alpha \in \mathrm{Gal}(k_s/k)$  such that  $\alpha \circ \varphi = \varphi' \circ f$ . The action of  $\alpha$  on  $X$  induces a map  $X_\varphi \rightarrow X_{\varphi'}$ . Any other choice for  $\alpha$  is of the form  $\alpha \circ \gamma$  where  $\gamma \in \mathrm{Gal}(k_s/\varphi(L))$ , hence induces the same map  $X_\varphi \rightarrow X_{\varphi'}$ . It follows that, when  $L \in \mathbf{Sep}_k$  is fixed, the sets  $X_\varphi$  for  $\varphi \in \mathrm{Hom}_{k\text{-alg}}(L, k_s)$  form an inverse system (here the set  $\mathrm{Hom}_{k\text{-alg}}(L, k_s)$  is directed by letting  $\varphi' \leq \varphi$  for every  $\varphi, \varphi'$ ). We denote by  $\mathcal{F}(L)$  its inverse limit. Observe that the projections  $\mathcal{F}(L) \rightarrow X_\varphi$  are bijections (all maps  $X_\varphi \rightarrow X_{\varphi'}$  are bijections)<sup>2</sup>; taking  $L = k_s$  and  $\varphi = \mathrm{id}$ , we obtain a canonical identification  $\mathcal{F}(k_s) = X$ . Moreover the association  $L \mapsto \mathcal{F}(L)$  naturally defines a  $k$ -set  $\mathcal{F}$ . From the construction, we see that if  $\mathcal{F}, \mathcal{G}$  are  $k$ -sets, then every  $\Gamma$ -equivariant map  $\mathcal{F}(k_s) \rightarrow \mathcal{G}(k_s)$  is induced by a unique morphism of  $k$ -sets  $\mathcal{F} \rightarrow \mathcal{G}$  (recall that  $\mathcal{F}(L) = \mathcal{F}(k_s)^{\mathrm{Gal}(k_s/L)}$  for any subextension  $L$  of  $k_s/k$ ).

EXAMPLE 6.2.3. Any set (resp. group)  $X$  defines a  $k$ -set (resp. group) taking the value  $X$  on every separable extension  $L/k$ . We will denote again by  $X$  this  $k$ -set (resp. group), and refer to it as the constant set (resp. group)  $X$ . Note that all Galois group actions on  $X$  are trivial.

EXAMPLE 6.2.4. Let  $V$  be a vector space over  $k$ . Every morphism  $E \rightarrow L$  in  $\mathbf{Sep}_k$  induces a group morphism  $V_E \rightarrow V_L$ , so that we may define a functor  $\mathbf{Sep}_k \rightarrow \mathbf{Groups}$  by  $L \mapsto V_L$ . We have proved in Lemma 4.4.3 that this functor is in fact a  $k$ -group.

When  $V = k$ , we will denote this  $k$ -group by  $\mathbb{G}_a$ . Thus  $\mathbb{G}_a(L) = L$  (as groups) for any separable extension  $L/k$ .

Let us now fix an integer  $n \in \mathbb{N}$  and a collection of integers  $m_1, \dots, m_n, m'_1, \dots, m'_n \in \mathbb{N}$ . When  $V$  is a vector space over a field  $K$  we will write

$$T(V) = \bigoplus_{i=1}^n \mathrm{Hom}_K(V^{\otimes m_i}, V^{\otimes m'_i}),$$

and if  $\varphi: V \rightarrow W$  is an isomorphism of  $K$ -vector spaces, we will write

$$T(\varphi) = \bigoplus_{i=1}^n \mathrm{Hom}_K((\varphi^{-1})^{\otimes m_i}, \varphi^{\otimes m'_i}): T(V) \rightarrow T(W).$$

If  $\psi: U \rightarrow V$  is another isomorphism of  $K$ -vector spaces, then

$$(6.2.a) \quad T(\varphi) \circ T(\psi) = T(\varphi \circ \psi).$$

---

<sup>2</sup>in other words: we may define  $\mathcal{F}(L) = X_\varphi$ , because up to a unique bijection, the set  $X_\varphi$  depends only on  $L$ , and not depend on the choice of  $\varphi: L \rightarrow k_s$ .



In fact we thus defined a functor  $T$  from the subcategory of  $K$ -vector spaces, where morphisms are the  $K$ -automorphisms, to itself.

Let  $L/k$  is a field extension, and  $V$  a  $k$ -vector space. We view  $V_L = V \otimes_k L$  as an  $L$ -vector space. Taking  $K = L$  in the above construction we obtain an  $L$ -vector space  $T(V_L)$ . There is a natural  $k$ -linear map  $T(V) \rightarrow T(V_L)$ , and we will denote by  $x_L \in T(V_L)$  the image of an element  $x \in T(V)$ .

REMARK 6.2.5. The natural  $L$ -linear map  $T(V)_L \rightarrow T(V_L)$  need not be an isomorphism (unless for instance  $\dim_k V < \infty$ , or  $L/k$  is finite).

Let us now fix a Galois extension  $F/k$ , and set  $\Gamma = \text{Gal}(F/k)$ .

If  $W$  is an  $F$ -vector space with a semilinear  $\Gamma$ -action, then  $T(W)$  inherits a semilinear  $\Gamma$ -action (see the paragraph just below Definition 4.4.2).

When  $W, W'$  are  $F$ -vector spaces, let us denote by  $\text{Isom}_F(W, W')$  the set of isomorphisms of  $F$ -vector spaces  $W \rightarrow W'$ . If  $W, W'$  are equipped with a semilinear  $\Gamma$ -action, the group  $\Gamma$  acts on  $\text{Isom}_F(W, W') \subset \text{Hom}_F(W, W')$  by the formula (4.4.b).

LEMMA 6.2.6. *Let  $W, W'$  be  $F$ -vector spaces with a semilinear  $\Gamma$ -action. Then the morphism  $\text{Isom}_F(W, W') \rightarrow \text{Isom}_F(T(W), T(W'))$  given by  $\varphi \mapsto T(\varphi)$  is  $\Gamma$ -equivariant.*

PROOF. Let  $U_1, U'_1, U_2, U'_2$  be  $F$ -vector spaces with a semilinear  $\Gamma$ -action, and  $\varphi: U_1 \rightarrow U_2$ ,  $\varphi': U'_1 \rightarrow U'_2$  be  $F$ -linear isomorphisms. Let  $\gamma \in \Gamma$ . Then clearly  $\gamma(\varphi \oplus \varphi') = (\gamma\varphi) \oplus (\gamma\varphi')$  and  $\gamma(\varphi \otimes \varphi') = (\gamma\varphi) \otimes (\gamma\varphi')$ . Let now

$$\psi = \text{Hom}_F(\varphi^{-1}, \varphi'): \text{Hom}_F(U_1, U'_1) \rightarrow \text{Hom}_F(U_2, U'_2).$$

For  $f \in \text{Hom}_F(U_1, U'_1)$ , we have

$$(\gamma\psi)(f) = \gamma(\psi(\gamma^{-1}f)) = \gamma \circ \varphi' \circ \gamma^{-1} \circ f \circ \gamma \circ \varphi^{-1} \circ \gamma^{-1} = (\gamma\varphi') \circ f \circ (\gamma\varphi),$$

proving that  $\gamma\psi = \text{Hom}_F((\gamma\varphi)^{-1}, \gamma\varphi')$ . In view of the construction of the functor  $T$ , this proves the statement.  $\square$

LEMMA 6.2.7. *If  $V$  is a  $k$ -vector space, the natural  $k$ -linear map  $T(V) \rightarrow T(V_F)$  induces an isomorphism  $T(V) \simeq T(V_F)^\Gamma$ .*

PROOF. Let  $U, U'$  be  $k$ -vector spaces. From the  $\Gamma$ -equivariant identifications  $U_F \oplus U'_F = (U \oplus U')_F$  and  $U_F \otimes_F U'_F = (U \otimes_k U')_F$ , we deduce that by Lemma 4.4.3

$$(U_F \oplus U'_F)^\Gamma = U \oplus U' \quad \text{and} \quad (U_F \otimes_F U'_F)^\Gamma = U \otimes_k U'.$$

Now the  $\Gamma$ -action on  $U'_F$  induces a  $\Gamma$ -action on  $\text{Hom}_k(U, U'_F)$ , and the identification  $\text{Hom}_F(U_F, U'_F) = \text{Hom}_k(U, U'_F)$  given by  $f \mapsto f|_U$  is  $\Gamma$ -equivariant. Thus

$$(\text{Hom}_F(U_F, U'_F))^\Gamma = \text{Hom}_k(U, U'_F)^\Gamma = \text{Hom}_k(U, (U'_F)^\Gamma) = \text{Hom}_k(U, U'),$$

and the statement follows as above from the construction of  $T$ .  $\square$

We now fix a  $k$ -vector space  $S$  and element  $s \in T(S)$ . Recall that we fixed a Galois extension  $F/k$ , and set  $\Gamma = \text{Gal}(F/k)$ .

DEFINITION 6.2.8. An  $F/k$ -twisted form, or simply a twisted form, of  $(S, s)$  is a pair  $(R, r)$ , where  $R$  is a  $k$ -vector space and  $r \in T(R)$  so that there exists an isomorphism of  $F$ -vector spaces  $\varphi: S_F \rightarrow R_F$  such that  $T(\varphi)(s_F) = r_F$ . A morphism  $(R, r) \rightarrow (R', r')$  of twisted forms of  $(S, s)$  is an isomorphism of  $k$ -vector spaces  $\psi: R \rightarrow R'$  such that  $T(\psi)(r) = r'$ . This defines a category of twisted forms of  $(S, s)$ .

REMARK 6.2.9. The isomorphism  $\varphi$  is *not* part of the data, we only require that it exists.

Let  $(R, r)$  be a twisted form of  $(S, s)$ . For every separable extension  $L/k$ , consider the set

$$\mathcal{I}(L) = \left\{ \begin{array}{l} \text{isomorphisms of } L\text{-vector spaces } \varphi: S_L \rightarrow R_L \\ \text{such that } T(\varphi)(s_L) = r_L. \end{array} \right\}$$

When  $f: E \rightarrow L$  is a morphism in  $\mathbf{Sep}_k$  and  $\varphi \in \mathcal{I}(E)$ , the map  $\mathcal{I}(f)(\varphi) = \varphi \otimes_E \text{id}_L$  fits into the commutative diagram

$$(6.2.b) \quad \begin{array}{ccc} S_E & \xrightarrow{\varphi} & R_E \\ \text{id}_S \otimes_k f \downarrow & & \downarrow \text{id}_R \otimes_k f \\ S_L & \xrightarrow{\mathcal{I}(f)(\varphi)} & R_L \end{array}$$

We have thus defined a functor  $\mathcal{I}: \mathbf{Sep}_k \rightarrow \mathbf{Sets}$ . When necessary, we will use the more precise notation  $\mathcal{I}_{(R,r)}$  for this functor. It follows from the diagram (6.2.b) (with  $E = L$  and  $f = \gamma$ ) that the action of  $\gamma \in \text{Aut}_{k\text{-alg}}(L)$  on  $\varphi \in \mathcal{I}(L)$  is given by

$$(6.2.c) \quad \gamma\varphi = (\text{id}_R \otimes_k \gamma) \circ \varphi \circ (\text{id}_S \otimes_k \gamma^{-1}).$$

In particular, when  $L = F$  we recover the action induced by that on  $\text{Isom}_F(S_F, R_F) \subset \text{Hom}_F(S_F, R_F)$  (see (4.4.b)).

We will make the following assumption:

$$(6.2.d) \quad \begin{array}{l} \text{There exists a finite subset } B \subset S \text{ such that the elements of } \mathcal{I}(L) \\ \text{are determined by their restrictions to } B \subset S_L. \end{array}$$

Note that the assumption (6.2.d) is satisfied when the  $k$ -vector space  $S$  is finite-dimensional (taking for  $B$  a  $k$ -basis of  $S$ ).

PROPOSITION 6.2.10. *Under the assumption (6.2.d), the functor  $\mathcal{I}$  is a  $k$ -set.*

PROOF. Let  $f: K \rightarrow L$  be a morphism in  $\mathbf{Sep}_k$  so that  $L/K$  is Galois, and  $\varphi \in \mathcal{I}(L)$ . Since  $\text{Gal}(L/K)$  acts continuously on  $R_L$  (by Lemma 4.4.3), we may find an open normal subgroup  $U$  of  $\text{Gal}(L/K)$  acting trivially on  $\varphi(b \otimes 1) \in R_L$  for  $b \in B$ . Then for any  $\gamma \in U$  and  $b \in B$ , we have by (6.2.c)

$$\gamma\varphi(b \otimes 1) = (\text{id}_R \otimes_k \gamma) \circ \varphi \circ (\text{id}_S \otimes_k \gamma^{-1})(b \otimes 1) = \varphi(b \otimes 1),$$

so that the subgroup  $U$  fixes  $\varphi$ . We have proved that  $\mathcal{I}(L)$  is a discrete  $\text{Gal}(L/K)$ -set.

Since the morphism  $\text{id}_R \otimes_k f: R_K \rightarrow R_L$  is injective, the diagram (6.2.b) (with  $E = K$ ) implies that  $\mathcal{I}(f): \mathcal{I}(K) \rightarrow \mathcal{I}(L)$  is injective. Assume now that  $\varphi$  lies in  $\mathcal{I}(L)^{\text{Gal}(L/K)}$ . In view of the formula (6.2.c), the morphism  $\varphi: S_L \rightarrow R_L$  is  $\text{Gal}(L/K)$ -invariant. In view of Lemma 4.4.3, there is an induced  $K$ -linear map

$$\psi = \varphi^{\text{Gal}(L/K)}: S_K \rightarrow R_K,$$

which is an isomorphism (with inverse  $(\varphi^{-1})^{\text{Gal}(L/K)}$ ). We have  $\psi_L = \varphi$  by Proposition 4.4.5, and the condition  $T(\varphi)(s_L) = r_L$  implies that  $T(\psi)(s_K) = r_K$  (because  $T(R_K) \rightarrow T(R_L)$  is injective). We have thus constructed an element  $\psi \in \mathcal{I}(K)$  mapping to  $\varphi \in \mathcal{I}(L)$ .  $\square$

In the special case  $(R, r) = (S, s)$ , the functor  $\mathcal{I}$  is naturally a  $k$ -group that we denote by  $\text{Aut}(S, s)$ . Thus for every separable extension  $L/k$

$$\text{Aut}(S, s)(L) = \{L\text{-automorphisms } \varphi \text{ of } S_L \text{ such that } T(\varphi)(s_L) = s_L\}.$$

In general  $\mathcal{I}(L)$  is equipped with a simply transitive right  $\text{Aut}(S, s)(L)$ -action. Thus  $\text{Aut}(S, s)(F)$  is a discrete  $\Gamma$ -group, and  $\mathcal{I}(F)$  is an  $\text{Aut}(S, s)(F)$ -torsor.

We now start with an  $\text{Aut}(S, s)(F)$ -torsor  $P$  and construct a twisted form  $(R, r)$  of  $(S, s)$ . Consider the discrete  $\Gamma$ -set  ${}_P S_F$  introduced in Definition 6.1.4. The element  $s_F \in T(S_F)$  is  $\text{Aut}(S, s)(F)$ -invariant (by definition of  $\text{Aut}(S, s)$ ). It thus follows from (6.1.c) that its image  $r' = T(\pi_p)(s_F) \in T({}_P S_F)$  does not depend on the choice of  $p \in P$ . The element  $r'$  is  $\Gamma$ -invariant, because for  $\gamma \in \Gamma$

$$\begin{aligned} \gamma r' &= \gamma(T(\pi_p)(s_F)) = (\gamma T(\pi_p))(\gamma s_F) && \text{by (4.4.b)} \\ &= T(\gamma \pi_p)(\gamma s_F) && \text{by Lemma 6.2.6} \\ &= T(\gamma \pi_p)(s_F) && \text{as } s_F \text{ is defined over } k \\ &= T(\pi_{\gamma p})(s_F) && \text{by Lemma 6.1.6} \\ &= r' && \text{as } r' \text{ does not depend on } p. \end{aligned}$$

Setting  $R = ({}_P S_F)^\Gamma$ , we have a  $\Gamma$ -equivariant identification of  $F$ -vector spaces  $R_F = {}_P S_F$  by Proposition 4.4.5. The element  $r'$  lies in  $T({}_P S_F)^\Gamma = T(R_F)^\Gamma$ . By Lemma 6.2.7, this implies that  $r' = r_F$  for some  $r \in T(R)$ . The choice of an element  $p \in P$  yields an isomorphism  $\varphi: S_F \xrightarrow{\pi_p} {}_P S_F = R_F$  such that  $T(\varphi)(s_F) = r_F$ . We have thus constructed a twisted form  $(R, r)$  of  $(S, s)$ , which will be denoted by  $(R(P), r(P))$  when necessary.

PROPOSITION 6.2.11. *The above defined associations*

$$(R, r) \mapsto \mathcal{I}_{(R, r)}(F) \quad \text{and} \quad P \mapsto (R(P), r(P))$$

*induce an equivalence between the categories of  $\text{Aut}(S, s)(F)$ -torsors and of twisted forms of  $(S, s)$ .*

PROOF. Let  $(R, r)$  be a twisted form of  $(S, s)$ , and set  $P = \mathcal{I}_{(R, r)}(F)$ . The isomorphism of  $F$ -vector spaces

$$u: R_F \xrightarrow{\varphi^{-1}} S_F \xrightarrow{\pi_\varphi} {}_P S_F = R(P)_F$$

does not depend on the choice of  $\varphi \in P$ , since for  $g \in \text{Aut}(S, s)(F)$ , we have by (6.1.c)

$$\pi_{\varphi \cdot g} \circ (\varphi \cdot g)^{-1} = \pi_\varphi \circ g \circ g^{-1} \circ \varphi^{-1} = \pi_\varphi \circ \varphi^{-1}.$$

We have  $T(u)(r_F) = T(\pi_\varphi)(s_F) = r(P)_F$  (by construction of  $r(P)$ ). The morphism  $u$  is  $\Gamma$ -equivariant, since for  $\gamma \in \Gamma$  we have by (6.2.c) and (6.1.b)

$$\begin{aligned} u \circ (\text{id}_R \otimes \gamma) &= \pi_\varphi \circ \varphi^{-1} \circ (\text{id}_R \otimes \gamma) \\ &= \pi_\varphi \circ (\text{id}_S \otimes \gamma) \circ (\gamma^{-1} \varphi^{-1}) \\ &= (\text{id}_{R(P)} \otimes \gamma) \circ \pi_{\gamma^{-1} \varphi} \circ (\gamma^{-1} \varphi^{-1}) \\ &= (\text{id}_{R(P)} \otimes \gamma) \circ u, \end{aligned}$$

where we used the independence of  $u$  in the choice of  $\varphi$  for the last step. In view of Lemma 4.4.3, the isomorphism  $u$  induces an isomorphism  $u^\Gamma: R \rightarrow R(P)$  of  $K$ -vector

spaces such that  $T(u^\Gamma)(r) = r(P)$ . Therefore  $u^\Gamma$  induces an isomorphism of twisted forms  $(R, r) \simeq (R(P), r(P))$ .

Conversely, let  $P$  be a  $\text{Aut}(S, s)(F)$ -torsor, and write  $(R, r) = (R(P), r(P))$ . It follows from Lemma 6.1.6 that the map  $v: P \rightarrow \mathcal{I}_{(R, r)}(F)$  sending  $p \in P$  to the map  $S_F \xrightarrow{\pi_p} {}_P S_F = R_F$  is an isomorphism of  $\text{Aut}(S, s)(F)$ -torsors.

To conclude, it only remains to notice that these associations define functors, and that the isomorphisms  $u$  and  $v$  are functorial.  $\square$

### 3. Examples of twisted forms

In this section, we provide a few examples of situations where the setting of §6.2 applies. First, note that Proposition 6.2.10 yields many examples of  $k$ -groups:

EXAMPLE 6.3.1. Let  $W$  be a  $k$ -vector of finite dimension. Taking  $s = 0$  and  $T(V) = V$  yields the  $k$ -group  $\text{GL}(W)$ , which satisfies for any separable field extension  $L/k$ .

$$\text{GL}(W)(L) = \text{Aut}_L(W_L).$$

When  $n$  is an integer, we write  $\text{GL}_n = \text{GL}(k^n)$ , as well as  $\mathbb{G}_m = \text{GL}_1$ .

EXAMPLE 6.3.2. More generally, let  $A$  be a finite-dimensional  $k$ -algebra and  $S$  an  $A$ -module, of finite dimension over  $k$ . The  $A$ -module structure is given by a  $k$ -linear map  $S \otimes_k A \rightarrow S$ . After choosing a  $k$ -basis of  $A$ , we may set  $T(V) = \text{Hom}_k(V \otimes_k A, V)$ . Then

$$L \mapsto \text{Aut}_{A_L}(S_L)$$

defines a  $k$ -group. When  $S = A^{\oplus n}$ , we denote this  $k$ -group by  $\text{GL}_n(A)$ . In particular we have  $\text{GL}_1(A)(L) = (A_L)^\times$  for all separable field extensions  $L/k$ .

Let us now fix a  $k$ -algebra  $S$ , which is assumed to be finitely generated (i.e. coincides with the subalgebra generated by some finite subset). Set  $T(V) = \text{Hom}_k(V \otimes_k V, V)$ . The multiplication in  $S$  defines an element  $s \in T(S)$ , and the condition (6.2.d) is satisfied. Therefore

$$L \mapsto \text{Aut}_{L\text{-alg}}(S_L)$$

defines a  $k$ -group.

Let  $A$  be a  $k$ -algebra such that  $A_F \simeq S_F$  as  $F$ -algebras. Then the  $k$ -vector space  $A$  together with the product of  $A$ , viewed as an element of  $\text{Hom}_k(A \otimes_k A, A)$ , define a twisted form of  $(S, s)$ . Conversely, let  $(R, r)$  be a twisted form of  $(S, s)$ . Then  $r$  defines a product  $R \otimes_k R \rightarrow R$ . The induced product on  $R_F$  defines a  $F$ -algebra structure (isomorphic to  $S_F$ ). Since  $R \rightarrow R_F$  is injective, this implies that the product on  $R$  is associative (and commutative if  $S$  is so). We claim that

$$(\gamma a)(\gamma b) = \gamma(ab) \in R_F \quad \text{for } \gamma \in \Gamma, \text{ and } a, b \in R_F.$$

Indeed under the identification  $F \simeq F \otimes_F F$  the automorphism corresponds to  $\gamma \otimes \gamma$  (as  $\gamma$  is multiplicative), hence  $\gamma(a \otimes b)$  corresponds to  $(\gamma a) \otimes (\gamma b)$  under the isomorphism  $(R \otimes_k R)_F \simeq R_F \otimes_F R_F$ . Since  $r_F: (R \otimes_k R)_F \simeq R_F \otimes_F R_F \rightarrow R_F$  is  $\Gamma$ -equivariant (being defined over  $k$ ), the claim follows. Using the claim, we see that

$$\gamma 1 = (\gamma 1)1 = (\gamma 1)(\gamma \gamma^{-1} 1) = \gamma(1 \gamma^{-1} 1) = \gamma \gamma^{-1} 1 = 1 \in R_F,$$

so that  $1 \in R \subset R_F$ , and it follows that the product on  $R$  defines a  $k$ -algebra structure.

In conclusion, a twisted form of  $(S, s)$  is precisely a  $k$ -algebra  $A$  (commutative if  $S$  is so) such that  $A_F \simeq S_F$  as  $F$ -algebras. Note that if the twisted form  $(R, r)$  corresponds

to the  $\text{Aut}(S, s)(F)$ -torsor  $P$  under the correspondence of Proposition 6.2.11, then the  $k$ -algebra  $R$  may be identified with  ${}_P S_F$ , with its natural product. We have thus proved:

**PROPOSITION 6.3.3.** *Let  $S$  be a finitely generated  $k$ -algebra. There is a contravariant equivalence between the category of  $k$ -algebras  $A$  such that  $A_F \simeq S_F$  as  $F$ -algebras, and the category of  $\text{Aut}_{F\text{-alg}}(S_F)$ -torsors.*

We now list a few typical applications of Proposition 6.3.3, where  $F = k_s$ . Variants may be obtained by taking  $F/k$  an arbitrary Galois extension (yielding classifications of objects “split by  $F/k$ ”).

**EXAMPLE 6.3.4.** (Étales algebras) Étale  $k$ -algebras of dimension  $n$  are twisted forms of the  $k$ -algebra  $k^n$  (see Proposition 5.2.13). The group  $\Gamma$  acts trivially on the set  $\mathbf{X}(k^n)$ , which consists of  $n$  points. From the equivalence of categories given in Theorem 5.4.4, it follows that  $\text{Aut}_{k\text{-alg}}(k^n)$  is the symmetric group  $\mathfrak{S}_n$ . Thus étale  $k$ -algebras of dimension  $n$  correspond to  $\mathfrak{S}_n$ -torsors (where  $\mathfrak{S}_n$  is given the trivial  $\text{Gal}(k_s/k)$ -action).

**EXAMPLE 6.3.5.** (Galois  $G$ -algebras) Let  $G$  be a finite group, viewed as a discrete  $\Gamma$ -group with the trivial  $\text{Gal}(k_s/k)$ -action. Consider the split Galois  $G$ -algebra  $S$  described in Example 5.5.5. Its automorphism group is the group of  $G$ -equivariant automorphisms of the set  $\mathbf{X}(S) = G$ , which coincides with  $G$ . Therefore Galois  $G$ -algebras correspond to  $G$ -torsors. One may see that the  $G$ -torsor corresponding to a  $G$ -algebra  $A$  is isomorphic to  $\mathbf{X}(A)$ , thus recovering Proposition 5.5.6.

**EXAMPLE 6.3.6.** (Quadratic forms) Let  $n$  be an integer and assume that the characteristic of  $k$  is not 2. A basic result in quadratic form theory asserts that all nondegenerate quadratic forms of rank  $n$  are twisted forms of the “split” quadratic form  $q$  given by  $(x_1, \dots, x_n) \mapsto x_1^2 + \dots + x_n^2$ . For each separable field extension  $L/k$ , let  $O_n(L)$  be the group of isometries of the quadratic form  $q_L$ . Then  $O_n$  defines a  $k$ -group by Proposition 6.2.10, and  $O_n(k_s)$ -torsors correspond to isometry classes of nondegenerate quadratic forms of rank  $n$ .

**EXAMPLE 6.3.7.** (Central simple algebras) Let  $n$  be an integer. Setting for each separable field extension  $L/k$

$$\text{PGL}_n(L) = \text{Aut}_{L\text{-alg}}(M_n(L))$$

defines a  $k$ -group by Proposition 6.2.10. In view of Corollary 3.3.4, finite-dimensional central simple  $k$ -algebras of degree  $n$  correspond to  $\text{PGL}_n(k_s)$ -torsors.

#### 4. 1-cocycles

In this section we fix a profinite group  $\Gamma$ . Let  $G$  be a discrete  $\Gamma$ -group. As before, we denote by  $g \mapsto \gamma g$  the action on  $G$  of  $\gamma \in \Gamma$  and by  $(g, h) \mapsto g \cdot h$  the group operation in  $G$ .

**DEFINITION 6.4.1.** A 1-cocyle of  $\Gamma$  with values in  $G$  is a continuous map  $\xi: \Gamma \rightarrow G$  (for the discrete topology on  $G$ ) that we denote by  $\gamma \mapsto \xi_\gamma$ , and such that

$$(6.4.a) \quad \xi_{\gamma\tau} = \xi_\gamma \cdot (\gamma\xi_\tau) \quad \text{for all } \gamma, \tau \in \Gamma.$$

The set of 1-cocycles  $\Gamma \rightarrow G$  will be denoted by  $Z^1(\Gamma, G)$ . We define an equivalence relation by declaring two 1-cocycles  $\xi, \eta$  *cohomologous* if there is  $a \in G$  such that

$$\eta_\gamma = a^{-1} \cdot \xi_\gamma \cdot (\gamma a) \quad \text{for all } \gamma \in \Gamma.$$

The set of equivalence classes is denoted by  $H^1(\Gamma, G)$ .

Assume now that  $M$  is a discrete  $\Gamma$ -module (we still use the multiplicative notation for the group operation in  $M$  even though it is commutative). Setting for  $\xi, \eta \in Z^1(\Gamma, M)$  and  $\gamma \in \Gamma$

$$(\xi \cdot \eta)_\gamma = \xi_\gamma \cdot \eta_\gamma,$$

turns  $Z^1(\Gamma, M)$  into an abelian group, compatibly with the equivalence relation defined above. Thus  $H^1(\Gamma, M)$  is naturally an abelian group.

REMARK 6.4.2. If  $\xi: \Gamma \rightarrow G$  is a 1-cocycle, note that  $\xi_1 = 1$ , and that

$$\xi_\gamma^{-1} = \gamma \xi_{\gamma^{-1}} \quad \text{for all } \gamma \in \Gamma.$$

REMARK 6.4.3. If the  $\Gamma$ -action on the discrete  $\Gamma$ -group  $G$  is trivial, a 1-cocycle  $\Gamma \rightarrow G$  is just a continuous group morphism  $\Gamma \rightarrow G$ . Two 1-cocycles are cohomologous if and only if they are conjugated by an element of  $G$ . In particular if  $M$  is a discrete  $\Gamma$ -module with trivial  $\Gamma$ -action, then  $Z^1(\Gamma, M) = H^1(\Gamma, M)$  is the group of continuous group morphisms  $\Gamma \rightarrow M$ .

Let  $\xi: \Gamma \rightarrow G$  be a 1-cocycle. Let  $X$  be a discrete  $\Gamma$ -set with a compatible left  $G$ -action (Definition 6.1.1), denoted by  $(g, x) \mapsto g \cdot x$ . For  $\gamma \in \Gamma$  and  $x \in X$ , we set

$$(6.4.b) \quad \gamma \star_\xi x = \xi_\gamma \cdot (\gamma x) \in X.$$

A straight-forward verification show that this defines a  $\Gamma$ -action on  $X$ . Any  $x \in X$  is fixed by some open subgroup  $V \subset \Gamma$  (for the original action), and the 1-cocycle  $\xi$  factors through the quotient map  $\Gamma \rightarrow \Gamma/U$  for some open subgroup  $U \subset \Gamma$  by Lemma 4.2.12. Then  $\gamma \star_\xi x = x$  for all  $\gamma \in U \cap V$ , which proves the  $\Gamma$ -action defined in (6.4.b) is continuous.

DEFINITION 6.4.4. The action defined in (6.4.b) is called the  $\Gamma$ -action *twisted* by the 1-cocycle  $\xi$ . The set  $X$  equipped with that action is a discrete  $\Gamma$ -set, that we denote by  ${}_\xi X$ .

Now let  $a \in G$ , and consider the 1-cocycle  $\xi': \Gamma \rightarrow G$  defined by

$$\xi'_\gamma = a^{-1} \cdot \xi_\gamma \cdot (\gamma a) \quad \text{for } \gamma \in \Gamma.$$

A straight-forward computation shows that the left action of  $a$  on  $X$  induces an isomorphism of discrete  $\Gamma$ -sets  ${}_\xi X \rightarrow {}_{\xi'} X$ . This shows that twisting the action by cohomologous 1-cocycles yields isomorphic discrete  $\Gamma$ -sets.

REMARK 6.4.5. The above isomorphism depends on the choice of  $a$  (and not just on the elements  $\xi, \xi'$ ), hence we cannot define a discrete  $\Gamma$ -set  ${}_\xi X$  for  $\xi \in H^1(\Gamma, G)$ .

PROPOSITION 6.4.6. *Let  $G$  be a discrete  $\Gamma$ -group. The set  $H^1(\Gamma, G)$  is naturally in bijection with the set of isomorphism classes of  $G$ -torsors.*

PROOF. This follows from (i), (ii), (iii) in the more precise Lemma 6.4.7 below.  $\square$

LEMMA 6.4.7. *Let  $G$  be a discrete  $\Gamma$ -group. We view  $G$  as a discrete  $\Gamma$ -set, with the left  $G$ -action given by the group operation in  $G$ . Then*

- (i) *Let  $\xi: \Gamma \rightarrow G$  be a 1-cocycle. Then the group operation in  $G$  induces a right  $G$ -action on  ${}_\xi G$ , and  ${}_\xi G$  is a  $G$ -torsor.*
- (ii) *Every  $G$ -torsor is isomorphic to  ${}_\xi G$  for some 1-cocycle  $\xi: \Gamma \rightarrow G$ .*

- (iii) Let  $\xi, \xi'$  be 1-cocycles  $\Gamma \rightarrow G$ . Then  ${}_{\xi}G \simeq {}_{\xi'}G$  as  $G$ -torsors if and only if  $\xi$  and  $\xi'$  are cohomologous.
- (iv) Let  $P$  be a  $G$ -torsor and  $p \in P$ . Then there is a unique map  $\xi: \Gamma \rightarrow G$  such that  $\gamma p = p \cdot \xi_{\gamma}$  for all  $\gamma \in \Gamma$ . The map  $\xi$  is a 1-cocycle such that  $P \simeq {}_{\xi}G$  as  $G$ -torsors.
- (v) Let  $X$  be a discrete  $\Gamma$ -set with a compatible left  $G$ -action. Let  $\xi: \Gamma \rightarrow G$  be a 1-cocycle, and  $P = {}_{\xi}G$ . Then  ${}_P X \simeq {}_{\xi}X$  as discrete  $\Gamma$ -sets.

PROOF. (i): We need to check that the  $G$ -action on itself given by right multiplication is compatible with the twisted  $\Gamma$ -action. Indeed, for  $g, h \in G$  and  $\gamma \in \Gamma$ , we have

$$\gamma \star_{\xi} (g \cdot h) = \xi_{\gamma} \cdot (\gamma(g \cdot h)) = \xi_{\gamma} \cdot (\gamma g) \cdot (\gamma h) = (\gamma \star_{\xi} g) \cdot \gamma(h).$$

(iv): The first statement follows from the simple transitivity of the  $G$ -action on  $P$ . If  $U$  is an open normal subgroup of  $\Gamma$  acting trivially on  $p$ , then  $\xi$  factors as  $\Gamma/U \rightarrow G$ , so that the map  $\xi$  is continuous by Lemma 4.2.12. For  $\gamma, \tau \in \Gamma$ , we have

$$\gamma \tau p = \gamma(p \cdot \xi_{\tau}) = (\gamma p) \cdot (\gamma \xi_{\tau}) = p \cdot \xi_{\gamma} \cdot (\gamma \xi_{\tau}),$$

so that  $\xi_{\gamma \tau} = \xi_{\gamma} \cdot (\gamma \xi_{\tau})$ , proving that  $\xi$  is 1-cocycle. The map  ${}_{\xi}G \rightarrow P$  given by  $g \mapsto p \cdot g$  is  $G$ -equivariant for the right  $G$ -actions. It is also  $\Gamma$ -equivariant, since for any  $\gamma \in \Gamma$  and  $g \in G$ , we have

$$p \cdot (\gamma \star_{\xi} g) = p \cdot \xi_{\gamma} \cdot (\gamma g) = (\gamma p) \cdot (\gamma g) = \gamma(p \cdot g).$$

The map  ${}_{\xi}G \rightarrow P$  is thus a morphism of  $G$ -torsors, hence an isomorphism.

(ii): Since a torsor is nonempty by definition, this follows from (iv).

The proofs of (iii) and (v) will rely on the following computation. Let  $\xi: \Gamma \rightarrow G$  be a 1-cocycle, and  $\varphi: G_{\xi} \rightarrow P$  an isomorphism of  $G$ -torsors. Set  $p = \varphi(1) \in P$ . Since  $\gamma 1 = 1$  in  $G$ , we have in  $P$

$$\gamma p = \gamma \varphi(1) = \varphi(\gamma \star_{\xi} 1) = \varphi(\xi_{\gamma} \cdot (\gamma 1)) = \varphi(\xi_{\gamma} \cdot 1) = \varphi(1 \cdot \xi_{\gamma}) = \varphi(1) \cdot \xi_{\gamma} = p \cdot \xi_{\gamma}.$$

(iii): One implication has already been observed just below Definition 6.4.4. For the converse, set  $P = G_{\xi'}$  above. We obtain  $\xi'_{\gamma} \cdot (\gamma p) = \gamma \star_{\xi'} p = p \cdot \xi_{\gamma}$ , so that  $\xi$  and  $\xi'$  are cohomologous.

(v): We use the relation  $\gamma p = p \cdot \xi_{\gamma}$  obtained above. In view of (6.1.b) and (6.1.c), we have, for any  $x \in X$  and  $\gamma \in \Gamma$ ,

$$\pi_p(\gamma \star_{\xi} x) = \pi_p(\xi_{\gamma} \cdot (\gamma x)) = \pi_{p \cdot \xi_{\gamma}}(\gamma x) = \pi_{\gamma p}(\gamma x) = \gamma \pi_p(x).$$

This proves that the map  $\pi_p: X \rightarrow {}_P X$  induces a  $\Gamma$ -equivariant bijection  ${}_{\xi}X \rightarrow {}_P X$ .  $\square$

DEFINITION 6.4.8. A *pointed set* is a set equipped with a distinguished element. We will denote by  $\{*\}$  the pointed set consisting of a single element. A morphism of pointed sets is a map sending the distinguished element to the distinguished element. The image of such a map is naturally a pointed set; the kernel of a morphism of pointed sets is the preimage of the distinguished element. We say that a sequence of pointed sets

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} \dots \xrightarrow{f_n} A_n$$

is exact if for each  $i = 1, \dots, n$  the kernel of  $f_i$  coincides with the image of  $f_{i-1}$ , as subgroups of  $A_i$ .

When  $A$  is a discrete  $\Gamma$ -group, the set  $H^1(\Gamma, A)$  is naturally pointed, the distinguished element being given by the class of the 1-cocycle  $\gamma \mapsto 1$ .

REMARK 6.4.9. Let  $A, B$  be discrete  $\Gamma$ -groups. Then the pointed set  $H^1(\Gamma, A \times B)$  is naturally isomorphic to  $H^1(\Gamma, A) \times H^1(\Gamma, B)$ .

Composing 1-cocycles  $\Gamma \rightarrow A$  with a morphism of discrete  $\Gamma$ -groups  $f: A \rightarrow B$  yields a morphism of pointed sets

$$f_*: H^1(\Gamma, A) \rightarrow H^1(\Gamma, B).$$

If  $A$  and  $B$  are  $\Gamma$ -modules, then  $f_*$  is a group morphism.

PROPOSITION 6.4.10. *Let  $B$  be a discrete  $\Gamma$ -group, and  $A \subset B$  a discrete  $\Gamma$ -subgroup. Denote by  $C = B/A$  the quotient of  $B$  by action of  $A$  given by right multiplication. Then  $C$  is a discrete  $\Gamma$ -set, and we have an exact sequence of pointed sets*

$$\{*\} \rightarrow A^\Gamma \rightarrow B^\Gamma \rightarrow C^\Gamma \xrightarrow{\delta} H^1(\Gamma, A) \rightarrow H^1(\Gamma, B).$$

For  $c \in C^\Gamma$ , the class  $\delta(c) \in H^1(\Gamma, A)$  is represented by the 1-cocycle sending  $\gamma \in \Gamma$  to  $b^{-1}(\gamma b) \in A \subset B$ , where  $b \in B$  is any preimage of  $c \in C^\Gamma$  under the map  $B \rightarrow C$  is naturally an  $A$ -torsor, whose class in  $H^1(\Gamma, A)$  is  $\delta(c)$ .

PROOF. We explain only the last statement, the rest being straight-forward. Denote by  $F \subset B$  the preimage of  $c$ . Then  $b \in F$ , and each element of  $F$  is of the form  $ba$  for a unique  $a \in A$ , so that  $F$  is an  $A$ -torsor. It follows from Lemma 6.4.7 (iv) that the corresponding element of  $H^1(\Gamma, A)$  is  $\delta(c)$ .  $\square$

COROLLARY 6.4.11. *In the situation of Proposition 6.4.10, the kernel of  $H^1(\Gamma, A) \rightarrow H^1(\Gamma, B)$  is isomorphic to the quotient of the pointed set  $C^\Gamma$  by the left action of  $B^\Gamma$ .*

PROOF. Let  $c, c' \in C^\Gamma$ , with preimages  $b, b' \in B$ . We have  $\delta(c) = \delta(c')$  if and only if the 1-cocycles  $\gamma \mapsto b^{-1}(\gamma b)$  and  $\gamma \mapsto b'^{-1}(\gamma b')$  are cohomologous, which means that there exists  $a \in A$  such that  $b'^{-1}(\gamma b') = a^{-1}b^{-1}(\gamma ba)$  for all  $\gamma \in \Gamma$ , or equivalently  $b'a^{-1}b^{-1} \in B^\Gamma$ . This is equivalent to the existence of  $\beta \in B^\Gamma$  such that  $\beta c = c'$  in  $C^\Gamma$ .  $\square$

PROPOSITION 6.4.12. *Any exact sequence of discrete  $\Gamma$ -groups*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

*induces an exact sequence of pointed sets*

$$\{*\} \rightarrow A^\Gamma \rightarrow B^\Gamma \rightarrow C^\Gamma \xrightarrow{\delta} H^1(\Gamma, A) \rightarrow H^1(\Gamma, B) \rightarrow H^1(\Gamma, C).$$

*The morphism of pointed sets  $\delta$  is the one described in Proposition 6.4.10; it is a group morphism if  $A$  is a discrete  $\Gamma$ -module.*

PROOF. This is clear.  $\square$

COROLLARY 6.4.13. *Any exact sequence of discrete  $\Gamma$ -modules*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

*induces an exact sequence of groups*

$$1 \rightarrow A^\Gamma \rightarrow B^\Gamma \rightarrow C^\Gamma \xrightarrow{\delta} H^1(\Gamma, A) \rightarrow H^1(\Gamma, B) \rightarrow H^1(\Gamma, C).$$

*The morphism  $\delta$  is the one described in Proposition 6.4.10.*



We say that a  $k$ -group  $G$  acts on a  $k$ -set  $X$  if  $G(L)$  acts on  $X(L)$  for every separable extension  $L/k$ , compatibly with the morphisms  $G(L) \rightarrow G(L')$  and  $X(L) \rightarrow X(L')$ , for every morphism  $L \rightarrow L'$  in  $\text{Sep}_k$ .

DEFINITION 6.4.14. Let  $G$  be a  $k$ -group. A  $k$ -set  $X$  with an action of  $G$  is called a  $G$ -torsor if for every separable closure  $F$  of  $k$ , the  $\text{Gal}(F/k)$ -set  $X(F)$  is a  $G(F)$ -torsor. A morphism of  $G$ -torsors is a morphism of functors between  $G$ -torsors which is compatible with the  $G$ -actions. The set of isomorphism classes of  $G$ -torsors will be denoted by  $H^1(k, G)$ .

REMARK 6.4.15. Let  $X$  be a  $k$ -set with a  $G$ -action. If  $F, F'$  are separable closures of  $k$ , there exists an isomorphism  $\varphi: F \rightarrow F'$ , which yields a bijection  $X(F) \rightarrow X(F')$  compatible with the  $G(F)$ - and  $G(F')$ -actions. Therefore  $X$  is a  $G$ -torsor as soon as  $X(k_s)$  is a  $G(k_s)$ -torsor for some separable closure  $k_s/k$ . In this case, it follows from Remark 6.2.2 and Proposition 6.4.6 that there is a canonical identification

$$H^1(k, G) = H^1(\text{Gal}(k_s/k), G(k_s)).$$

DEFINITION 6.4.16. Let  $f: H \rightarrow G$  be a morphism of  $k$ -groups. The kernel of  $f$  is the  $k$ -subgroup  $\ker f \subset G$ , defined by setting for every separable field extension  $L/k$

$$(\ker f)(L) = \ker(H(L) \rightarrow G(L)).$$

DEFINITION 6.4.17. When  $A, B, C$  are  $k$ -groups, an exact sequence

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$$

is the data of morphisms of  $k$ -groups  $A \rightarrow B$  and  $B \rightarrow C$  such that for every separable closure  $F$  of  $k$ , the sequence of groups

$$1 \rightarrow A(F) \rightarrow B(F) \rightarrow C(F) \rightarrow 1$$

is exact.

Note that in the above situation the morphism  $B(k) \rightarrow C(k)$  need not be surjective. In fact, by Proposition 6.4.12, there is an induced exact sequence of pointed sets

$$\{*\} \rightarrow A(k) \rightarrow B(k) \rightarrow C(k) \rightarrow H^1(k, A) \rightarrow H^1(k, B) \rightarrow H^1(k, C).$$

Finally, we come back to the setting of §6.2, and note the following consequence of Proposition 6.2.11 in terms of 1-cocycles:

PROPOSITION 6.4.18. Let  $F/k$  be a Galois extension, and  $\Gamma = \text{Gal}(F/k)$ . Isomorphism classes of  $F/k$ -twisted forms of  $(S, s)$  correspond to elements of  $H^1(\Gamma, \text{Aut}(S, s)(F))$ .

If  $\xi: \Gamma \rightarrow \text{Aut}(S, s)(F)$  is a 1-cocycle, the corresponding (up to isomorphism) twisted form  $(R, r)$  may be constructed by setting

$$R = \{x \in S_F \mid x = \xi_\gamma \cdot (\gamma x) \text{ for all } \gamma \in \Gamma\}$$

and  $r = s_F \in T(R) \subset T(S_F)$ .

Conversely let  $(R, r)$  be a twisted form of  $(S, s)$ . Choose an isomorphism  $\varphi: S_F \rightarrow R_F$  such that  $T(\varphi)(s_F) = r_F$ . A 1-cocycle corresponding to  $(R, r)$  is given by the map  $\Gamma \rightarrow \text{Aut}(S, s)(F)$  sending  $\gamma \in \Gamma$  to the composite

$$S_F \xrightarrow{\text{id}_S \otimes \gamma^{-1}} S_F \xrightarrow{\varphi} R_F \xrightarrow{\text{id}_R \otimes \gamma} R_F \xrightarrow{\varphi^{-1}} S_F.$$

PROOF. The first statement follows from Proposition 6.4.6 and Proposition 6.2.11. The explicit description of  $R$  follows from Lemma 6.4.7 (v), and the explicit description of the 1-cocycle follows from Lemma 6.4.7 (iv) (in view of the formula (6.2.c)).  $\square$

EXAMPLE 6.4.19. (Étales algebras.) The set of isomorphism classes of étale  $k$ -algebras of dimension  $n$  is  $H^1(k, \mathfrak{S}_n)$ , where  $\mathfrak{S}_n$  is considered as a constant  $k$ -group. In view of Remark 6.4.3, this is the set of continuous group morphisms  $\text{Gal}(k_s/k) \rightarrow \mathfrak{S}_n$  modulo conjugation by elements of  $\mathfrak{S}_n$ .

EXAMPLE 6.4.20. (Galois  $G$ -algebras.) Let  $G$  be a finite group, viewed as a constant  $k$ -group. The set of isomorphism classes of Galois  $G$ -algebras is in bijection with  $H^1(k, G)$ . Since  $\Gamma$  acts trivially on  $G$ , this is the set of continuous group morphisms  $\text{Gal}(k_s/k) \rightarrow G$  modulo conjugation by elements of  $G$  (Remark 6.4.3). In particular, if  $G$  is abelian, this is the set of continuous group morphisms  $\text{Gal}(k_s/k) \rightarrow G$ .



## CHAPTER 7

**Applications of torsors theory**

In this chapter, we apply the theory of twisted forms that we have just presented. The simplest applications are the classical Kummer and Artin–Schreier theories, which describe torsors under cyclic groups (in the presence of enough roots of unity in the base field), that is, Galois algebras under those groups. These theories are consequences of the so-called Hilbert’s Theorem 90 (and its additive counterpart), a central result which is the basis of many computations of Galois cohomology sets.

The rest of the chapter concerns central simple algebras. As we have seen, such algebras of degree  $n$  correspond to torsors under the group  $\mathrm{PGL}_n$ . Thus algebras of different degrees have classes in the first cohomology set of different groups. We first briefly explain how to relate these cohomology sets in order to understand the tensor product of central simple algebras in terms of 1-cocycles.

The next application concerns the so-called cyclic algebras. Those algebras may be thought of as higher degrees generalisations of quaternion algebras, and provide a concrete way of constructing central simple algebras. This section culminates with a computation of the relative Brauer group of a cyclic Galois extension.

The last application is a construction of the reduced norm and trace, which are twisted versions of the determinant and trace of matrices. The reduced norm may be thought of as a higher degree generalisation of the quaternion norm. We relate the image of the reduced norm to the images of the norms of splitting fields of finite degrees.

**1. Kummer theory**

Let  $V$  be a finite-dimensional  $k$ -vector space. Recall from Example 6.3.1 that  $\mathrm{GL}(V)$  denotes the  $k$ -group defined by  $\mathrm{GL}(V)(L) = \mathrm{Aut}_L(V_L)$  for any separable field extension  $L/k$ .

**PROPOSITION 7.1.1** (Hilbert’s Theorem 90). *For any Galois field extension  $F/k$ , we have  $H^1(\mathrm{Gal}(F/k), \mathrm{GL}(V)(F)) = \{*\}$ . In particular  $H^1(k, \mathrm{GL}(V)) = \{*\}$ .*

**PROOF.** This follows at once from Proposition 6.4.18, since all twisted forms of the  $k$ -vector space  $V$  have the same dimension, hence are isomorphic.  $\square$

The above statement is in fact due to Speiser. The following consequence is the original form of Hilbert’s Theorem 90.

**COROLLARY 7.1.2.** *Let  $L/k$  be a Galois field extension of finite degree such that  $\mathrm{Gal}(L/k)$  is cyclic generated by  $\sigma$ . Let  $\alpha \in L$ . Then  $N_{L/k}(\alpha) = 1$  if and only if  $\alpha = (\sigma\beta)\beta^{-1}$  for some  $\beta \in L$ .*

**PROOF.** Let  $n = [L : k]$ . Recall that, by Proposition 5.5.10,

$$N_{L/k}(\alpha) = \alpha(\sigma\alpha) \cdots (\sigma^{n-1}\alpha).$$

Certainly  $N_{L/k}((\sigma\beta)\beta^{-1}) = 1$  for all  $\beta \in L$ . Conversely, assume that  $N_{L/k}(\alpha) = 1$ . Then the map

$$\xi: \text{Gal}(L/k) \rightarrow L^\times \quad ; \quad \sigma^i \mapsto \alpha(\sigma\alpha) \cdots (\sigma^{i-1}\alpha)$$

is a 1-cocyle. By Hilbert's Theorem 90 (Proposition 7.1.1), this 1-cocyle is cohomologous to the trivial 1-cocyle. This yields an element  $\beta \in L^\times$  such that  $\xi_{\sigma^i} = (\sigma^i\beta)\beta^{-1}$  for all  $i$ , and the statement follows by taking  $i = 1$ .  $\square$

DEFINITION 7.1.3. Let  $n \in \mathbb{N} - \{0\}$ . We denote by  $\mu_n$  the kernel of the morphism of  $k$ -groups  $\mathbb{G}_m \rightarrow \mathbb{G}_m$  given by  $x \mapsto x^n$ . Thus  $\mu_n$  is a  $k$ -group such that, for any separable field extension  $L/k$ , we have

$$\mu_n(L) = \{x \in L^\times | x^n = 1\}.$$

LEMMA 7.1.4. Assume that  $n$  is not divisible by the characteristic of  $k$ . Then we have an exact sequence of  $k$ -groups

$$1 \rightarrow \mu_n \rightarrow \mathbb{G}_m \xrightarrow{x \mapsto x^n} \mathbb{G}_m \rightarrow 1.$$

PROOF. We only need to prove surjectivity of the last morphism. If  $a \in k_s^\times$ , then the polynomial  $X^n - a$  is separable (its derivative  $nX^{n-1}$  is nonzero by the assumption), hence has a root in  $b \in k_s^\times$ . The element  $b$  is the required preimage of  $a$ .  $\square$

PROPOSITION 7.1.5 (Kummer's theory). Assume that  $n$  is not divisible by the characteristic of  $k$ . Then there is a natural group isomorphism

$$k^\times / k^{\times n} \simeq H^1(k, \mu_n),$$

mapping  $a \in k^\times$  to the class of the 1-cocyle  $\gamma \mapsto (\gamma\alpha)\alpha^{-1}$ , where  $\alpha \in k_s$  is any element such that  $\alpha^n = a$ .

Every  $\mu_n(k_s)$ -torsor is isomorphic to  $\{x \in k_s | x^n = a\}$ , where  $\omega \in \mu_n(k_s)$  acts by  $x \mapsto \omega x$ , for a uniquely determined element  $a \in k^\times / k^{\times n}$ .

PROOF. By Proposition 6.4.12, the exact sequence of  $k$ -groups of Lemma 7.1.4 yields an exact sequence of groups (Corollary 6.4.13)

$$1 \rightarrow \mu_n(k) \rightarrow k^\times \xrightarrow{x \mapsto x^n} k^\times \xrightarrow{\delta} H^1(k, \mu_n) \rightarrow H^1(k, \mathbb{G}_m).$$

The group on the right is trivial by Hilbert's Theorem 90 (Proposition 7.1.1), so the required isomorphism is induced by  $\delta$ . The remaining statements follow from the explicit descriptions of  $\delta$  provided in Proposition 6.4.10.  $\square$

COROLLARY 7.1.6. Assume that  $k$  contains a root of unity  $\omega$  of order  $n$ . Then

$$H^1(k, \mathbb{Z}/n) \simeq k^\times / k^{\times n}.$$

The class of an element  $a \in k^\times$  corresponds to the isomorphism class of the Galois  $\mathbb{Z}/n$ -algebra  $R_a = k[X]/(X^n - a)$ , with the action of  $i \in \mathbb{Z}/n$  given by  $X \mapsto \omega^i X$ .

PROOF. The assumption implies that  $n$  is not divisible by the characteristic of  $k$ , and yields an isomorphism of  $\text{Gal}(k_s/k)$ -groups  $\mathbb{Z}/n \rightarrow \mu_n(k_s)$  given by  $i \mapsto \omega^i$ . Sending  $f \in \mathbf{X}(R_a)$  to  $f(X) \in k_s$  induces an isomorphism of  $\mathbb{Z}/n$ -torsors  $\mathbf{X}(R_a) \simeq \{x \in k_s | x^n = a\}$ , where  $i \in \mathbb{Z}/n$  acts by  $x \mapsto \omega^i x$ . Since  $\dim_k R_a = n$ , this implies that  $R_a$  is the Galois  $\mathbb{Z}/n$ -algebra (unique up to isomorphism) corresponding to the  $\mu_n(k_s)$ -torsor  $\{x \in k_s | x^n = a\}$ , where  $\omega$  acts by  $x \mapsto \omega x$ . Thus the statement follows from Proposition 7.1.5.  $\square$

## 2. Artin–Schreier theory

Proposition 7.1.1 has the following “additive” counterpart. The proof given here relies in the interpretation of  $H^1(k, \mathbb{G}_a)$  as the set of isomorphism classes of twisted forms of a particular object. A different, purely cohomological proof will be given later.

PROPOSITION 7.2.1. *We have  $H^1(k, \mathbb{G}_a) = \{*\}$ .*

PROOF. For a vector space  $V$  over a field  $K$ , we set

$$T(V) = V \oplus \operatorname{Hom}_K(V, K).$$

Consider the  $k$ -vector space  $S = k^2$ . The element  $s = (1, 0) \in S$  and the map  $\sigma \in \operatorname{Hom}_k(S, k)$  given by  $\sigma(x, y) = y$  for all  $x, y \in k$  define an element  $(s, \sigma) \in T(S)$ . We will abuse the notation and denote the pair  $(S, (s, \sigma))$  by  $(S, s, \sigma)$ . Let  $F/k$  be a Galois extension and  $\Gamma = \operatorname{Gal}(F/k)$ . Any element  $\varphi \in \operatorname{Aut}(S, s, \sigma)(F)$  is given by a matrix

$$\begin{pmatrix} a_\varphi & b_\varphi \\ c_\varphi & d_\varphi \end{pmatrix} \in M_2(F).$$

The condition  $\varphi(s_F) = s_F$  means that  $a_\varphi = 1$  and  $c_\varphi = 0$ . The condition  $\sigma_F \circ \varphi = \sigma_F$  means that  $d_\varphi = 1$  and  $c_\varphi = 0$ . The remaining coefficient  $b_\varphi$  may be freely chosen in  $F$  (observe that the matrix will always be invertible), and we have, for any  $x, y \in F$ ,

$$\varphi(x, y) = (x + b_\varphi y, y).$$

If  $\psi$  is another automorphism of  $(S_F, s_F, \sigma_F)$ , we have  $b_{\varphi \circ \psi} = b_\varphi + b_\psi$ . This proves that  $\operatorname{Aut}(S, s, \sigma)(F)$  is the group  $F$ . Moreover if  $\gamma \in \operatorname{Gal}(F/k)$ , and  $\psi = (\operatorname{id} \otimes \gamma) \circ \varphi \circ (\operatorname{id} \otimes \gamma^{-1})$ , we have for any  $x, y \in F$

$$\psi(x, y) = (\operatorname{id} \otimes \gamma) \circ \varphi(\gamma^{-1}x, \gamma^{-1}y) = (\operatorname{id} \otimes \gamma)(\gamma^{-1}x + b_\varphi \gamma^{-1}y, \gamma^{-1}y) = (x + (\gamma b_\varphi)y, y),$$

so that  $b_\psi = \gamma b_\varphi$ . We have proved that the discrete  $\Gamma$ -group  $\operatorname{Aut}(S, s, \sigma)(F)$  is isomorphic to  $\mathbb{G}_a(F)$ .

Let now  $(R, r, \rho)$  be a twisted form of  $(S, s, \sigma)$  over  $k$ . Note that the elements  $r$  and  $\rho$  are nonzero, since they are so after extending scalars to  $F$ . Also  $\rho(r) = 0$ , since  $\sigma(s) = 0$ . Let  $e \in R$  be such that  $\rho(e) = 1$ , and  $f \in S$  such that  $\sigma(f) = 1$ . Then the family  $(r, e)$ , resp.  $(s, f)$ , is a  $k$ -basis of  $R$ , resp.  $S$ . The  $k$ -linear map  $S \rightarrow R$  given by  $s \mapsto r$  and  $f \mapsto e$  is then an isomorphism of twisted forms  $(S, s, \sigma) \rightarrow (R, r, \rho)$ . We have proved that all twisted forms of  $(S, s, \sigma)$  are isomorphic. Therefore by Proposition 6.4.18 we have

$$H^1(\operatorname{Gal}(k_s/k), \operatorname{Aut}(S, s, \sigma)(k_s)) = H^1(k, \mathbb{G}_a) = \{*\}. \quad \square$$

LEMMA 7.2.2. *If  $k$  has characteristic  $p > 0$ , we have an exact sequence of  $k$ -groups*

$$1 \rightarrow \mathbb{Z}/p \rightarrow \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \rightarrow 1,$$

where, for every separable field extension  $L/k$ ,

$$\wp: L \rightarrow L \quad ; \quad x \mapsto x^p - x.$$

PROOF. Note that  $\wp$  defines a morphism of  $k$ -groups, and that  $\ker \wp: L \rightarrow L$  coincides with the prime field  $\mathbb{F}_p \subset L$  for every separable field extension  $L/k$ . Thus  $\ker \wp$  is isomorphic to the constant group  $\mathbb{Z}/p$ . The morphism  $\wp: k_s \rightarrow k_s$  is surjective because for any  $a \in k_s$  the polynomial  $X^p - X - a \in k_s[X]$  is separable (its derivative is the constant nonzero polynomial  $-1$ ), so that if  $b \in k_s$  is a root of that polynomial, we have  $\wp(b) = a$ .  $\square$

PROPOSITION 7.2.3 (Artin–Schreier’s theory). *Assume that  $k$  has characteristic  $p > 0$ . Then there is a natural group isomorphism*

$$k/\wp(k) \simeq H^1(k, \mathbb{Z}/p),$$

*mapping  $a \in k$  to the class of the 1-cocycle  $\gamma \mapsto \gamma\alpha - \alpha$ , where  $\alpha \in k_s$  is any element such that  $\alpha^p - \alpha = a$ .*

*Every  $\mathbb{Z}/p$ -torsor is isomorphic to  $\{x \in k_s \mid x^p - x = a\}$ , where  $i \in \mathbb{Z}/p$  acts by  $x \mapsto x + i$ , for a uniquely determined  $a \in k/\wp(k)$ .*

PROOF. By Proposition 6.4.12, the exact sequence of  $k$ -groups of Lemma 7.2.2 yields an exact sequence of groups (Corollary 6.4.13)

$$1 \rightarrow \mathbb{Z}/p \rightarrow k \xrightarrow{\wp} k \xrightarrow{\delta} H^1(k, \mathbb{Z}/p) \rightarrow H^1(k, \mathbb{G}_a).$$

The group on the right is trivial by Proposition 7.2.1, so the required isomorphism is induced by  $\delta$ . The remaining statements follow from the explicit descriptions of  $\delta$  provided in Proposition 6.4.10.  $\square$

COROLLARY 7.2.4. *Assume that  $k$  has characteristic  $p > 0$ . Every Galois  $\mathbb{Z}/p$ -algebra is isomorphic to  $T_a = k[X]/(X^p - X - a)$  for a uniquely determined  $a \in k/\wp(k)$ , where the action of  $i \in \mathbb{Z}/p$  given by  $X \mapsto X + i$ .*

PROOF. Sending  $f \in \mathbf{X}(T_a)$  to  $f(X) \in k_s$  induces an isomorphism of  $\mathbb{Z}/p$ -torsors  $\mathbf{X}(T_a) \simeq \{x \in k_s \mid x^p - x = a\}$ , where  $i \in \mathbb{Z}/p$  acts by  $x \mapsto x + i$ . Since  $\dim_k T_a = p$ , this implies that  $T_a$  is the Galois  $\mathbb{Z}/p$ -algebra (unique up to isomorphism) corresponding to the  $\mathbb{Z}/p$ -torsor  $\{x \in k_s \mid x^p - x = a\}$ . Thus the statement follows from Proposition 7.2.3.  $\square$

## Bibliography

- [Dra83] Peter K. Draxl. *Skew fields*, volume 81 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.
- [GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017.
- [Ker07] Ina Kersten. *Brauergruppen*. Universitätsverlag Göttingen, Göttingen, 2007. <https://univerlag.uni-goettingen.de/bitstream/handle/3/isbn-978-3-938616-89-5/brauergruppen.pdf>.
- [KMRT98] Max-Albert Knus, Alexander S. Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions. With a preface by J. Tits*. Providence, RI: American Mathematical Society, 1998.
- [Lam05] Tsi-Yuen Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.
- [Pie82] Richard S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982. Studies in the History of Modern Science, 9.
- [Ser62] Jean-Pierre Serre. *Corps locaux*. Publications de l’Institut de Mathématique de l’Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.
- [Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.
- [Sta] The Stacks Project Authors. Stacks Project. <http://stacks.math.columbia.edu>.