Brauer Groups of fields

Olivier Haution

Ludwig-Maximilians-Universität München

Winter semester 2020/2021

Contents

Note on the literature

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

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

Part 1

Noncommutative Algebra

CHAPTER 1

Quaternion algebras

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

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

1. The norm form

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

We fix a base field k. A k-algebra is a ring A equipped with a structure of k-vector space such that the multiplication map $A \times A \to A$ is k-bilinear. A morphism of k-algebras is a ring morphism which is k-linear. Observe that the bilinearity of the multiplication map implies that for any $\lambda \in k$ and $a \in A$

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

If A is nonzero, the ring morphism $k \to A$ given by $\lambda \mapsto \lambda 1$ is injective, and we will view k as a subring of A.

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

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

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

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

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

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

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

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

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

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

(i) $(a, b) \simeq (b, a)$,

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

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

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

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

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

PROOF. The matrices

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

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

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

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

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

PROOF. This follows from the computation

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

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. □

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

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

Definition 1.1.8. We define the *(quaternion) norm map* $N \colon Q \to k$ by $q \mapsto q\overline{q} = \overline{q}q$.

Observe that the norm map is multiplicative:

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

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

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

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

Proof. If $N(q) \neq 0$, then q is a two-sided inverse of $N(q)^{-1}\overline{q}$. Conversely, if $p \in Q$ is such that $pq = 1$, then $N(p)N(q) = 1$, hence $N(q) \neq 0$. □

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

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

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

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

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

It follows from the multiplicativity of the determinant that

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

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

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

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

$$\mathrm{N}_{k(\sqrt{a})/k}(x + y\alpha) = x^2 - ay^2. \tag{1.1.d}$$

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

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

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

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

is not invertible.

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

(iii) $\Rightarrow$ (iv) : We may assume that a is not a square in k, and choose $\alpha \in k(\sqrt{a})$ such that $\alpha^2 = a$. Let $q = x + yi + zj + wij$ be a nontrivial zero of the norm map, where $x, y, z, w \in k$. Then by the formula (1.1.c)

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

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

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

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

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

Then

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

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

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

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

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

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

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

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

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

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

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

Let us record another useful consequence of Lemma 1.1.14.

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

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

PROPOSITION 1.1.20. *Let Q, Q' be quaternion algebras, with respective pure quaternion subspaces Q_0, Q'_0. Then $Q \simeq Q'$ if and only if there is a k-linear map $\varphi \colon Q_0 \to Q'_0$ such that $\varphi(q)^2 = q^2 \in k$ for all $q \in Q_0$.*

PROOF. Let $\psi \colon Q \to Q'$ be an isomorphism of k-algebras. If $q \in Q_0$, then

$$\psi(q)^2 = \psi(q^2) = q^2 \in k, \quad \text{and } \psi(q) \notin \psi(k^\times) = k^\times,$$

so that $\psi(q) \in Q'_0$. So we may take for φ the restriction of ψ.

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

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

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

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

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

PROOF. Let Q be a quaternion algebra and $N\colon Q \to k$ its norm form. Note that $N(q) = -q^2$ for all $q \in Q_0$. The subspaces k and Q_0 are orthogonal in Q with respect to the norm form N, and $N|_k = \langle 1 \rangle$. So we have a decomposition $N \simeq \langle 1 \rangle \perp (N|_{Q_0})$. This quadratic form is nondegenerate (e.g. by (1.1.c)), hence a morphism φ as in Proposition 1.1.20 is automatically an isometry. The corollary follows, by Witt's cancellation Theorem (see for instance [**Lam05**, Theorem 4.2]). $\square$

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 $k(\sqrt{a}) = k[X]/(X^2 - a) \to (a, b)$ given by $X \mapsto i$ is injective (because its source is a field, and its target is nonzero).

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

PROOF. Let $L \subset D$ be a subalgebra isomorphic to $k(\sqrt{a})$, and $\alpha \in L$ such that $\alpha^2 = a$. Since α does not lie in the center of D, there is $x \in D$ such that $x\alpha \neq \alpha x$. Then $\beta = \alpha^{-1}x\alpha - x$ is nonzero. Using the fact that $\alpha^2 = a$ is in the center of D, we see that

$$\beta\alpha = \alpha^{-1}x\alpha^2 - x\alpha = \alpha x - x\alpha = -\alpha\beta.$$

Multiplying with β on the left, resp. right, we obtain $\beta^2\alpha = -\beta\alpha\beta$, resp. $\beta\alpha\beta = -\alpha\beta^2$. It follows that β^2 commutes with α. Since β does not commute with α, we have $\beta \notin L$. Therefore the L-subspace of D generated by $1, \beta$ has dimension 2 over L, hence dimension 4 over k, and thus coincides with D by dimensional reasons. In particular the k-algebra D is generated by α, β. Since β^2 commutes with α and β, it lies in center of D, so that $b = \beta^2 \in k^\times$. It follows from Lemma 1.1.2 (applied with $i = \alpha, j = \beta$) that $D \simeq (a, b)$. $\square$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note that $N(q) \neq 0$, for otherwise $N(p) = -aN(q) = 0$, and thus $q = p = 0$ (by Lemma 1.1.9, as Q is division), contradicting the choice of p, q. The element $s = N(q)^{-1}r \in Q$ satisfies $s^2 = a$. Mapping X to s yields a morphism of k-algebras $k[X]/(X^2 - a) \to Q$, and (iii) follows.

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

3. Biquaternion algebras

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

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

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

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

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

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

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

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

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

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

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

Assume that $q_1q_2 = q_2q_1$. Let K be the k-subalgebra of Q generated by q_1, q_2. We claim that if $K \neq k$, then K is a quadratic field extension of k. Indeed, this is true by Lemma 1.2.5 if $q_1 \in k$, so we will assume that $q_1 \notin k$. Then the k-subalgebra K_1 of Q generated by q_1 is a quadratic field extension of k, by the same lemma. If $q_2 \notin K_1$, then $1, q_2$ is a K_1-basis of Q, so that $K = Q$. This is not possible since q_1 and q_2 commute (as

Q is central). Thus $q_2 \in K_1$, and $K = K_1$ is as required, proving the claim. If $K \neq k$, then Proposition 1.2.9 thus implies that Q splits over K, and since (ii) does not hold, by the same proposition $K \otimes_k Q'$ must remain division. This conclusion also holds if $K = k$. Thus in any case $x \in K \otimes_k Q'$ admits a left inverse.

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

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

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

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

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

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

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

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

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

There are isomorphisms of k-algebras

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $M_4(k)$.

Exercises

Exercise 1.1. Let $a \in k^\times$. Show that:

(i) $(a, -a)$ splits.
(ii) If $a \neq 1$, then $(a, 1-a)$ splits.
(iii) $(a, a) \simeq (a, -1)$.
(iv) $(a, -1)$ splits if and only if a is a sum of two squares in k.

Exercise 1.2. (Chain Lemma.) Let $a, b, c, d \in k^\times$ be such that $(a, b) \simeq (c, d)$. We are going to prove that there is $e \in k^\times$ such that

$$(a, b) \simeq (e, b) \simeq (e, d) \simeq (c, d).$$

So we let Q be such that $(a, b) \simeq Q \simeq (c, d)$.

(i) Let i, j, resp. i', j', be the images in Q of the standard generators of (a, b), resp. (c, d). Show that $i, j, i', j' \in Q_0$.
(ii) Let V be the k-subspace of Q_0 generated by j, j'. Show that the morphism $\varphi \colon Q_0 \to \mathrm{Hom}_k(V, k)$ sending $q \in Q_0$ to the map $v \mapsto qv + vq$ is not injective.
(iii) Deduce that there is a nonzero $\varepsilon \in Q_0$ such that $\varepsilon j = -j\varepsilon$ and $\varepsilon j' = -j'\varepsilon$.
(iv) Show that $e = \varepsilon^2 \in k$, and conclude.

Exercise 1.3. Let L/k be a field extension of odd degree and Q a quaternion k-algebra. Show that Q splits if and only if $Q \otimes_k L$ splits over L. (Hint : use the splitting criterion involving the norm of quadratic field extensions, and the properties of field norms.)

Exercise 1.4. Show that every quaternion algebra can be realised as a subalgebra of $M_4(k)$.

Exercise 1.5. Let $k = \mathbb{Q}$, and consider that quaternion algebra $Q = (-1, -1)$ over k. Let $\xi \in \mathbb{C}$ be a primitive 5-th root of 1, and $K \subset \mathbb{C}$ be the field extension generated by ξ.

(i) Show that Q_K splits.
(ii) Determine the subfields of K.
(iii) Deduce that K contains no quadratic extension splitting Q.

Exercise 1.6. Show that every element of a quaternion k-algebra satisfies a quadratic equation over k.

Exercise 1.7. Let D be a division k-algebra. We assume that for every $d \in D$, there is a nonzero polynomial $P \in k[X]$ of degree ≤ 2 such that $P(d) = 0$. We are going to prove that one of the following must happen (in particular, the k-algebra D must be finite-dimensional!):

— $D = k$,
— D is a quadratic field extension of k,
— D is a quaternion k-algebra.

Let us assume that $D \neq k$.

(i) Show that there is $i \in D - k$ and $a \in k$ such that $i^2 = a$.
(ii) Let K be the k-subalgebra of D generated by i. Show that K is a field and that $[K : k] = 2$.
(iii) Let $\varphi\colon D \to D$ be the map $d \mapsto i^{-1}di$. Show that $\varphi^2 = \mathrm{id}$, and that $D = D_+ \oplus D_-$ as K-vector spaces, where $D_+ = \ker(\varphi - \mathrm{id}), D_- = \ker(\varphi + \mathrm{id})$.
(iv) Show that D_+ is a K-subalgebra of D.
(v) Let $\alpha \in D_+$ and F the K-subalgebra of D_+ generated by α. Show that F is a field.
(vi) Show that $\alpha \in K$.
(vii) Deduce that $D_+ = K$.
(viii) Let now $\beta, \beta' \in D_-$. Show that $\beta\beta' \in D_+$, and deduce that $\dim_K D_- \in \{0, 1\}$.
(ix) Assume that $\dim_K D_- = 1$, and let j be a nonzero element of D_-. Let $A \in k[X]$ be a nonzero polynomial of degree ≤ 2 such that $A(j) = 0$. Show that $A(-j) = 0$, and deduce that $j^2 \in k$.
(x) Conclude.

CHAPTER 2

Simple algebras

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

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

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

1. Wedderburn's Theorem

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

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

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

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

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

Definition 2.1.3. Let R be a ring. The *opposite ring* R^{op} is the ring equal to R as an abelian group, where multiplication is defined by mapping (x, y) to yx (instead of xy for the multiplication in R). Note that if R is a k-algebra, then R^{op} is naturally a k-algebra.

Observe that:

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

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

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

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

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

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

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

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

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

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

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

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

and

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

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

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

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

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

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

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

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

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

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

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

DEFINITION 2.1.9. A ring 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 $1 \in Sa_1 + \cdots + Sa_p$. We have thus a surjective morphism of A-modules $S^{\oplus p} \to A$ given by $(s_1, \dots, s_p) \mapsto s_1a_1 + \cdots + s_pa_p$.

Let now M be a finitely generated A-module. Then M is a quotient of $A^{\oplus q}$ for some integer q, hence a quotient of $S^{\oplus n}$ for some integer n (namely $n = pq$). Choose n minimal with this property, and denote by N the kernel of the surjective morphism $S^{\oplus n} \to M$. For $i = 1, \ldots, n$, denote by $\pi_i \colon S^{\oplus n} \to S$ the projection onto the i-th factor. If $N \neq 0$, there is i such that $\pi_i(N) \neq 0$. Since S is simple, this implies that $\pi_i(N) = S$. Let now $m \in M$, and $s \in S^{\oplus n}$ a preimage of m. Then there is $z \in N$ such that $\pi_i(z) = \pi_i(s)$. The element $s - z$ is mapped to m in M, and belongs to $\ker \pi_i \simeq S^{\oplus n-1}$. This yields a surjective morphism $S^{\oplus n-1} \to M$, contradicting the minimality of n. So we must have $N = 0$, and $S^{\oplus n} \simeq M$. This proves the second statement.

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

THEOREM 2.1.13 (Wedderburn). *Let A be an artinian simple ring (resp. a finite-dimensional simple k-algebra). Then A is isomorphic to $M_n(D)$ for some integer n and division ring (resp. finite-dimensional division k-algebra) D. Such a ring (resp. k-algebra) D is unique up to isomorphism, and the centers of A and D are isomorphic.*

PROOF. Recall that in any case A is artinian (Example 2.1.10). Let S be a simple A-module, which exists by Proposition 2.1.12. Then the ring $E = \operatorname{End}_A(S)$ 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

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

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

2. The commutant

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We can now summarise our results as follows:

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

PROOF. Combine Proposition 2.2.6, Proposition 2.2.4 and Proposition 2.2.5. □

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

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

PROOF. The map φ is a nonzero morphism of k-algebras (because $\mathrm{End}_k(A) \neq 0$, as A is simple), and its kernel is a two-sided ideal in the ring $A \otimes_k A^{\mathrm{op}}$, which is simple by Proposition 2.2.6. Thus φ is injective, and bijective for dimensional reasons. □

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

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

PROOF. Consider the isomorphism $\varphi\colon A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ of Proposition 2.2.9, and let $C = \varphi(B \otimes_k k)$ (recall that A is nonzero, being simple). A morphism in $\mathrm{End}_k(A)$ commutes with C if and only if it is B-linear (for the left action on A induced by multiplication). Thus

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

To conclude, note that $\mathcal{Z}_{A\otimes_k A^{\mathrm{op}}}(B \otimes_k k) = \mathcal{Z}_A(B) \otimes_k A^{\mathrm{op}}$ by Lemma 2.2.3. □

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

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

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

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

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

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

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

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

(ii): Let $a = \dim_k A, b = \dim_k B, c = \dim_k C, d = \dim_k D, s = \dim_k S$. Taking the dimensions in (2.2.b) and (2.2.c) yields $ac = n^2 d$ and $b = r^2 d$. Since $B \simeq S^{\oplus r}$ and $A \simeq S^{\oplus n}$, we have $b = rs$ and $a = ns$, and therefore $ar = bn$. Thus

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

hence $a = bc$.

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

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

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

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

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

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

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

3. Skolem–Noether's Theorem

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

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

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

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

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

Proof. Let $\varphi\colon A^f \to A^g$ be an isomorphism of $B \otimes_k A^{\mathrm{op}}$-modules. Set $u = \varphi(1) \in A$. For any $b \in B$, we have

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

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

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

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

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

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

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

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

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

Exercises

Exercise 2.1. Prove the following converse of Wedderburn's Theorem: If D is a division ring and $n \geq 1$ an integer, then the ring $M_n(D)$ is artinian simple.

Exercise 2.2. In Proposition 1.3.4, we proved the following statement : if Q, Q' are quaternion algebras over a field k (of characteristic $\neq 2$), then

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

The proof of "$\Longleftarrow$" was easy, while the proof of "$\Longrightarrow$" was comparatively difficult (in particular used Albert's Theorem). Give a new (short) proof of "$\Longrightarrow$", using "$\Longleftarrow$" and the results of §2.1 in the lecture notes.

Exercise 2.3. (i) Show that every nonzero ring admits a simple module.

(ii) Let R be a ring, and M a nonzero R-module. Show that there is a submodule N of M and a quotient S of N such that S is simple.

Exercise 2.4. Let D be a finite-dimensional central division k-algebra, and n an integer. Show that $M_n(k)$ contains a k-subalgebra isomorphic to D if and only if $\dim_k D \mid n$.

Exercise 2.5. Let R be a ring and M an R-module. We are going to prove that the following conditions are equivalent:

(a) The module M is generated by its simple submodules.
(b) The module M is a direct sum of simple R-modules.
(c) Every submodule of M is a direct summand.

The R-module M will be called *semisimple* if it satisfies the above conditions.

(i) Let $S_i \to M$ for $i \in I$ be a collection of morphisms of R-modules, where each S_i is a simple module. When $K \subset I$, let us write $S_K = \bigoplus_{i \in K} S_i$, and denote by N_K the kernel of $S_K \to M$. Using Zorn's lemma, show that there is a maximal subset $K \subset I$ such that $N_K = 0$.
(ii) In the situation of (i), show that $S_I \to M$ and $S_K \to M$ have the same image.
(iii) Prove that (a) $\Longrightarrow$ (b).
(iv) Prove that (b) $\Longrightarrow$ (c). (Hint: use (i) and (ii) for an appropriate collection of morphisms $S_i \to Q$.)

For the rest of the exercise, we assume that (c) holds, and prove (a). So we let M' be the submodule of M generated by the simple submodules of M, and choose a submodule M'' such that $M' \oplus M'' = M$. We assume that $M'' \neq 0$ and come to a contradiction. By Exercise 2.3, we know that there are submodules $P \subset N \subset M''$ such that N/P is simple.

(v) Show that N/P is isomorphic to a submodule of N.
(vi) Conclude that (c) $\Longrightarrow$ (a).

Exercise 2.6. A ring is called *semisimple* if it is semisimple as a module over itself (see the previous exercise). Prove the following assertions:

(i) Every semisimple ring is a finite direct sum of simple modules.
(ii) Every semisimple ring is artinian.

(iii) Every artinian simple ring is semisimple.
(iv) Every semisimple ring is isomorphic to a product $M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, where $D_1, \ldots, D_r$ are division rings and $n_1, \ldots, n_r$ are integers.
(v) The product of two semisimple rings is semisimple.
(vi) A ring is semisimple if and only if it is a finite product of artinian simple rings.

Exercise 2.7. Let D be a division ring of positive characteristic (i.e. there is a prime number p such that $pD = 0$.) Show that every finite subgroup of $D^\times$ is cyclic. (Hint: you may use the fact that every subgroup of $k^\times$ is cyclic when k is a finite field).

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 $B \to B$ given by left multiplication by b is injective, because if $x \in B$ is such that $bx = 0$, then $0 = b^{-1}bx = x$ in D, hence $x = 0$ in B. By dimensional reasons, this map is surjective. Thus the element $1 \in B$ lies in its image, so there is $b' \in B$ such that $bb' = 1$. Multiplying by b^{-1} on the left, we deduce that $b^{-1} = b' \in B$. $\square$

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 $\overline{k}$ be an algebraic closure of k. The $\overline{k}$-algebra $A_{\overline{k}}$ is finite-dimensional central simple by Lemma 3.1.1, hence isomorphic to $M_n(\overline{k})$ for some integer n by Corollary 3.1.4. Then $\dim_k A = \dim_{\overline{k}} A_{\overline{k}} = n^2$. $\square$

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 $\mathrm{ind}(A)$.

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

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

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

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

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

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

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

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

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

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

so that B is Brauer-equivalent to A. □

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

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

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

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

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

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

from which the statement follows. □

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

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

PROOF. The first assertion follows from Lemma 3.1.2.

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

(iv) $\Rightarrow$ (iii) : Since $[L : k] \mid \mathrm{ind}(D)$ 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 $(D^{\mathrm{op}})_L \simeq \mathrm{End}_L(D)$ by Lemma 2.2.10. Thus L splits D^{op}, hence also D. □

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

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

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

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

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

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

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 $[E:L] = \operatorname{ind}(A_L)$. Then E is a splitting field for the k-algebra A, and it follows from Corollary 3.2.3 that

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

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

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

which implies that D_L is division. □

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

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

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

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

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

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

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

COROLLARY 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

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

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

3. Separable splitting fields

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

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

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

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

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

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

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

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

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

Corollary 3.3.2. *Assume that k is separably closed (i.e. admits no nontrivial separable extension). Then every finite-dimensional division k-algebra is commutative. In particular, every finite-dimensional central simple k-algebra splits.*

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

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

Proof. Let D be a finite-dimensional central division k-algebra. Recall that every commutative subalgebra of D is a field by Lemma 3.1.2. Let L be a commutative subalgebra of D, which is maximal among those which are separable as a field extension of k. Let $E = \mathcal{Z}_D(L)$. As L is commutative, we have $L \subset E$. The L-algebra E is division by Lemma 3.1.2. If E is not commutative, using Proposition 3.3.1 we find a separable extension L'/L such that $L \subsetneq L' \subset E$. The field extension L'/k is then separable (being a composite of separable extensions), contradicting the maximality of L. Thus E is commutative. Therefore $E \subset \mathcal{Z}_D(E) = L$ by Proposition 2.2.11 (iii). We have proved that $L = E = \mathcal{Z}_D(L)$, so that L is a maximal subfield. □

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

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

4. Finite division rings, real division algebras

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

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

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

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

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

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

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

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

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

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

by Proposition 3.1.3. So we may assume that $k = \mathbb{R}$. Then D splits over the degree two extension $\mathbb{C}/\mathbb{R}$ (by Corollary 3.1.4) hence $\operatorname{ind}(D) \in \{1, 2\}$ by Corollary 3.2.3. If $\operatorname{ind}(D) = 1$, then $D = \mathbb{R}$. Otherwise D is a quaternion $\mathbb{R}$-algebra by Corollary 1.2.6; such an algebra is division if and only if it is isomorphic to $(-1, -1)$ by Example 1.1.18. □

5. The Brauer group, I

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

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

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

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:

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

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

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

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 $\operatorname{Br}(k)$. Then $\operatorname{ind}(B) \mid \operatorname{ind}(A)$.*

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 $\operatorname{ind}(A^{\otimes i}) = \operatorname{ind}(B)$. By Corollary 3.2.7, we may find an extension L/k of degree $\operatorname{ind}(A)$ 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

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

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

Definition 3.5.6. If L/k is a field extension, we denote by $\operatorname{Br}(L/k)$ the subgroup of $\operatorname{Br}(k)$ consisting of those classes of algebras split by L.

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

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

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

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

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

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

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

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

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

PROOF. We show that every finite-dimensional central division k-algebra D splitting over L splits over a finitely generated subextension of L, proceeding by induction on the degree of D (for all fields k simultaneously). We may assume that $D \neq k$. Then $D \otimes_k L$ contains an element $x \neq 0$ such that $x^2 = 0$ (Remark 3.5.8). Writing $x = d_1 \otimes \lambda_1 + \cdots + d_n \otimes \lambda_n$, where $d_1, \ldots, d_n \in D$ and $\lambda_1, \ldots, \lambda_n \in L$, we see that x belongs to $D \otimes_k K'$, where K' is the subextension of L generated by $\lambda_1, \ldots, \lambda_n$. Then $D \otimes_k K'$ is not division (as it contains the nonzero noninvertible element x), hence is Brauer-equivalent to a central division algebra of strictly smaller degree, by Wedderburn's Theorem 2.1.13. So by induction it splits over a finitely generated extension K of K'. Then K is a finitely generated extension of k splitting D. □

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

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

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

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

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

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

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

Exercises

Exercise 3.1. The purpose of this exercise is to describe another proof of the fact that every finite-dimensional central division k-algebra contains a maximal subfield which is separable over k (Theorem 3.3.3).

(i) Let $P = p_n X^n + \cdots + p_0$ and $Q = q_m X^m + \cdots + q_0$ be polynomials in $k[X]$. Construct a matrix $S \in M_{m+n}(k)$ having the following property. If $A = a_{m-1}X^{m-1} + \cdots + a_0$ and $B = b_{n-1}X^{n-1} + \cdots + b_0$ are polynomials in $k[X]$, writing

$$S \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} u_{m+n-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ u_0 \end{pmatrix}$$

we have

$$PA + QB = u_{m+n-1}X^{m+n-1} + \cdots + u_0 \in k[X].$$

(ii) Assume that $p_n \neq 0$ and $q_m \neq 0$. Show that P and Q admit a nontrivial common factor if and only if $\det S = 0$. (The value $\det S$ is called the *resultant* of P and Q.)

(iii) Fix an integer d. Show that there exists a polynomial $\delta \in k[X_0, \ldots, X_d]$ such that $\delta(a_0, \ldots, a_d) \neq 0$ if and only if the polynomial $a_d X^d + \cdots + a_0$ is separable. (Hint: a polynomial is separable if and only if it is prime to its derivative.)

Let A be a finite-dimensional k-algebra and $a \in A$. The kernel of the k-algebra morphism $k[X] \to A$ is a principal ideal. Recall that the *minimal polynomial* of a is the unique generator of that ideal having leading coefficient 1.

(iv) Let L/k be a field extension. If $P \in k[X]$ is the minimal polynomial of a in the k-algebra A, show that its image $P \in L[X]$ is the minimal polynomial of $a \otimes 1$ in the L-algebra $A \otimes_k L$.

(v) Let $M \in M_n(k)$ and $\chi \in k[X]$ its characteristic polynomial. Show that if χ is separable, then χ is the minimal polynomial of M.

(vi) Fix an integer n. Show that there exists a polynomial $\pi \in k[X_{i,j}, 1 \leq i, j \leq n]$ having the following property: if M is a matrix in $M_n(k)$ having coefficients $m_{i,j} \in k$ for $1 \leq i, j \leq n$, then $\pi(m_{1,1}, \ldots, m_{n,n}) \neq 0$ if and only if the minimal polynomial of $M \in M_n(k)$ is separable of degree n. (Hint : use (iii) of the previous exercise.)

Let now D be a central division k-algebra of degree n, and F an algebraic closure of k.

(vii) Let $e_1, \ldots, e_{n^2}$ be a k-basis of D. Show that there exists a polynomial $\rho \in F[X_1, \ldots, X_{n^2}]$ having the following property: if $x \in D$ has coefficients $x_1, \ldots, x_{n^2}$ in the basis $e_1, \ldots, e_{n^2}$, then $\rho(x_1, \ldots, x_{n^2}) \neq 0$ if and only if the minimal polynomial of x in the k-algebra D is separable of degree n.

(viii) Assume that k is infinite. Let L/k be a field extension and d an integer. Let $P \in L[X_1, \ldots, X_d]$ be a polynomial. Assume that there exist $y_1, \ldots, y_d \in L$ such that $P(y_1, \ldots, y_d) \neq 0$. Show that there exist $x_1, \ldots, x_d \in k$ such that $P(x_1, \ldots, x_d) \neq 0$.

(Hint: find $x_1, \dots, x_m \in k$ by induction on m so that $P(x_1, \dots, x_m, y_{m+1}, \dots, y_d) \neq 0$.)

(ix) Conclude that D contains a separable extension of k of degree n. (Hint: observe that the case when k is finite is easy.)

Part 2

Torsors

CHAPTER 4

Infinite Galois theory

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

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

1. Profinite sets

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

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

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

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

These data must satisfy the following conditions:

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

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

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

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

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

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

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

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

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

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

Lemma 4.1.7. *Every closed subset of a profinite set is profinite.*

Proof. Let $F \subset E$ be a closed subset. For each $\alpha \in \mathcal{A}$, let $F_\alpha = \pi_\alpha(F)$, and set $F' = \varprojlim F_\alpha$. We may F' as a subset of E; as such it contains F. Conversely, let $f \in F'$. For each $\alpha \in \mathcal{A}$, let $f_\alpha = \pi_\alpha(f) \in F_\alpha$. If U is an open neighborhood of f in E, it contains $\pi_\alpha^{-1}\{f_\alpha\}$ for some $\alpha \in \mathcal{A}$ by Lemma 4.1.6. Then $\pi_\alpha^{-1}\{f_\alpha\} \cap F \neq \varnothing$ as $F \to F_\alpha$ is surjective. Thus F meets every neighborhood of every element of F'. Since F is closed in E, this implies that $F = F'$. The topology induced on the subset $F \subset E$ is generated by the open subsets $\pi_\alpha^{-1}\{x\} \cap F$ where $x \in E_\alpha$ and $\alpha \in \mathcal{A}$. Such a subset is empty if $x \notin F_\alpha$, and coincides with the preimage of x under the projection map $F' \to F_\alpha$ when $x \in F_\alpha$. It follows that the induced topology on F coincides with the profinite topology on F'. □

Lemma 4.1.8. *The inverse limit of an inverse system of nonempty finite sets is nonempty.*

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

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

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

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

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

Proposition 4.1.9. *Every profinite set is compact.*

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

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

Assume that $F_\alpha = \varnothing$ for some $\alpha \in \mathcal{A}$. Then E_α is covered by subsets of the form $V_i = f_{\alpha\alpha_i}^{-1}\{x_i\}$. As E_α is finite, it is covered by finitely many such subsets, and thus $E = \pi_\alpha^{-1}E_\alpha$ is covered by finitely many subsets of the form $\pi_\alpha^{-1}V_i = U_i$. Thus we are done in this case.

Therefore we may assume that $F_\alpha \neq \varnothing$ for each $\alpha \in \mathcal{A}$. Then $\varprojlim F_\alpha$ contains an element by Lemma 4.1.8. Its image in $y \in E$ satisfies $\pi_\alpha(y) \in F_\alpha \subset E_\alpha$ for all $\alpha \in \mathcal{A}$, and in particular y belongs to no U_i. This contradicts the fact that the subsets U_i for $i \in I$ cover E. □

Remark 4.1.10. Proposition 4.1.9 and Lemma 4.1.8 may also be viewed as consequences of Tikhonov's Theorem, asserting that a product of compact topological spaces is compact.

Remark 4.1.11. The sets $F_\alpha = \operatorname{im}\pi_\alpha \subset E_\alpha$ for an inverse system. Let F be its inverse limit. The natural map $F \to E$ is continuous, open, and bijective, and is therefore a homeomorphism. Thus (replacing E_α with F_α) we can always represent a profinite set as an inverse limit of finite sets in such a way that the projection maps are surjective. Note that this implies that the transition maps are also surjective.

Conversely:

Lemma 4.1.12. *Assume that each E_α is finite, and that the transition maps $E_\beta \to E_\alpha$ for $\alpha \leq \beta$ are surjective. Then the projection maps $\pi_\alpha \colon E \to E_\alpha$ are surjective.*

Proof. Fix $\gamma \in \mathcal{A}$ and $x \in E_\gamma$. Define an inverse system by

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

Then each F_α is nonempty and finite, hence $\varprojlim F_\alpha$ contains an element by Lemma 4.1.8. Its image in $y \in E$ satisfies $\pi_\gamma(y) = x$. □

2. Profinite groups

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

DEFINITION 4.2.1. When each E_α appearing in Definition 4.1.2 is a group and the transition maps $f_{\beta\alpha}$ are group morphisms, we say that E_α is an *inverse system of groups*. Its inverse limit is naturally a group, and the projections maps π_α are group morphisms. When each E_α is finite, the topological group E is called a *profinite group*.

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

EXAMPLE 4.2.3. Let p be a prime number. The groups $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$, together with the maps $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for $m \leq n$ given by $(1 \mod p^n) \mapsto (1 \mod p^m)$ yield an inverse system of groups, whose limit is the profinite group denoted by $\mathbb{Z}_p$.

EXAMPLE 4.2.4. The groups $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$, together with the maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$ given by $(1 \mod n) \mapsto (1 \mod m)$ yield an inverse system of groups, whose limit is the profinite group denoted by $\widehat{\mathbb{Z}}$.

Let us fix a profinite group Γ. We choose a directed set $\mathcal{A}$ and an inverse system of finite groups Γ_α for $\alpha \in \mathcal{A}$ such that $\Gamma = \varprojlim \Gamma_\alpha$, and denote by $\pi_\alpha \colon \Gamma \to \Gamma_\alpha$ the projections. We also define the subgroups $U_\alpha = \ker \pi_\alpha$. By Remark 4.1.11, we can assume that each projection morphism π_α is surjective, and thus identify each Γ_α with Γ/U_α.

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

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

(iii) If a subgroup of Γ contains an open subgroup, it is open.

PROOF. (i) : By Lemma 4.1.6 there exist $\alpha \in \mathcal{A}$ and $x \in E_\alpha$ such that $\pi_\alpha^{-1}\{x\}$ is contained in U and contains u. Then $uU_\alpha \subset \pi_\alpha^{-1}\{x\}$.

(ii) : Let $U \subset \Gamma$ be an open subgroup, and S its complement in Γ. Then S is the union of the subsets γU for $\gamma \in S$. Such subsets are images of U under a self-homeomorphism of Γ (namely, left multiplication by γ), hence are open, so that S is open, proving that U is closed. By (i) (with $u = 1$) the subgroup U contains U_α for some $\alpha \in \mathcal{A}$. Certainly U_α has finite index in Γ (as $\Gamma/U_\alpha \simeq \Gamma_\alpha$), so that U has finite index in Γ.

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

(iii) : Let $H \subset \Gamma$ be a subgroup containing an open subgroup U. Then $H = HU$ is the union of the subsets hU for $h \in H$. Such subsets are images of U under a self-homeomorphism of Γ, hence are open, so that H is open. $\square$

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

Definition 4.2.7. Let p be a prime number. Recall that a finite group is called a *p-group* if its cardinality is a power of p. A profinite group is called a *pro-p-group* if the index of every open subgroup is a power of p.

Lemma 4.2.8. *The profinite group Γ is a pro-p-group if and only if each Γ_α is a p-group.*

Proof. If Γ is a pro-p-group, then $|\Gamma_\alpha| = |\Gamma/U_\alpha|$ is a power of p. Conversely assume that each Γ_α is a p-group. Let U be an open subgroup of Γ. By Lemma 4.2.5 (i) with $u = 1$, we find an index α such that $U_\alpha \subset U$. Let $V_\alpha = U/U_\alpha$. Then the index of U in Γ coincides with the index of V_α in Γ_α, hence is a power of p, since Γ_α is a p-group. $\square$

Definition 4.2.9. A subgroup P of Γ is called a *pro-p-Sylow subgroup* if all the following conditions are satisfied:

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

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

Proposition 4.2.10. *The profinite group Γ admits a pro-p-Sylow subgroup.*

Proof. For each $\alpha \in \mathcal{A}$, let S_α be the set of p-Sylow subgroups of $\Gamma_\alpha = \Gamma/U_\alpha$, which is finite and nonempty by Sylow's Theorem. If $\alpha \leq \beta$ in $\mathcal{A}$, the map $\Gamma_\beta \to \Gamma_\alpha$ sends elements of S_β to elements of S_α, because the image of a p-Sylow subgroup under a surjective morphism of finite groups is a p-Sylow subgroup (exercise). Thus the sets S_α form an inverse system indexed by $\mathcal{A}$, whose inverse limit S is nonempty by Lemma 4.1.8. Any element of S is represented by a collection of p-Sylow subgroups $P_\alpha \subset \Gamma_\alpha$ for $\alpha \in \mathcal{A}$, such that for any $\alpha \leq \beta$ in $\mathcal{A}$ the morphism $\Gamma_\beta \to \Gamma_\alpha$ maps P_β onto P_α. The group $P = \varprojlim P_\alpha$ is naturally a subgroup of Γ, and is a pro-p-group. The subset $P \subset \Gamma$ is closed, being the intersection of the preimages of $P_\alpha \subset \Gamma_\alpha$ for $\alpha \in \mathcal{A}$ (by construction of the inverse limit). It follows from Lemma 4.1.12 (applied to the system P_α for $\alpha \in \mathcal{A}$) that for each $\alpha \in \mathcal{A}$ the image of P in Γ_α is the p-Sylow subgroup P_α. Now any an open subgroup U of Γ contains U_α for some $\alpha \in \mathcal{A}$, and the image of P in Γ/U coincides with the image of P_α under the surjective morphism $\Gamma_\alpha = \Gamma/U_\alpha \to \Gamma/U$, and in particular has index prime to p (exercise). $\square$

Lemma 4.2.11. *Let X be a set with an action of the profinite group Γ. The following conditions are equivalent:*

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

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

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

Definition 4.2.12. When the conditions of Lemma 4.2.11 are fulfilled, we say that Γ acts *continuously* on X, or that X is a *discrete* Γ*-set*. A discrete Γ-set equipped with a Γ-equivariant group structure will be called a discrete Γ*-group*. A discrete Γ-group whose underlying group is abelian will be called a discrete Γ*-module*. We define a morphism of discrete Γ-groups, resp. Γ-modules, as a Γ-equivariant group morphism.

Lemma 4.2.13. *Let X be a discrete Γ-set, and F a finite subset of X. Then there exists an open subgroup of Γ fixing each element of F.*

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

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

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

Let now $f\colon \Gamma^n \to X$ be a continuous map, and $Y \subset X$ its image. Since Γ^n is profinite set (the limit of the inverse system $(\Gamma_\alpha)^n$), it is compact by Proposition 4.1.9. Therefore Y is compact. Being also discrete, the set Y is finite. Since X is a discrete Γ-set, there is an open subgroup U' in Γ fixing all the elements of Y (Lemma 4.2.13). Shrinking U', we may assume that it is normal in Γ (by Lemma 4.2.5 (i) with $u = 1$). We have achieved $f(\Gamma^n) \subset X^{U'}$.

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

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

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

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

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

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

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

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

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

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

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

φ is injective, so that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

THEOREM 4.3.11 (Krull). *The associations*

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

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

(i) the subgroup $\mathrm{Gal}(F/E)$ is open if and only if E/k is finite, in which case

$$[\mathrm{Gal}(F/k) : \mathrm{Gal}(F/E)] = [E : k].$$

(ii) the subgroup $\mathrm{Gal}(F/E)$ is normal if and only if E/k is Galois, in which case

$$\mathrm{Gal}(F/k)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/k).$$

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

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

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

Let now E/k be a subextension of F/k, and consider the set $X = \mathrm{Hom}_{k-\mathrm{alg}}(E, F)$. Let $\overline{F}$ be an algebraic closure of F, and $Y = \mathrm{Hom}_{k-\mathrm{alg}}(E, \overline{F})$. By Lemma 4.3.1 (i), every element $g \in Y$ may be extended to a morphism of k-algebras $h\colon F \to \overline{F}$. The image of h coincides with $F \subset \overline{F}$ by Lemma 4.3.3, hence h is induced by an element $\sigma \in \mathrm{Gal}(F/k)$ such that g is the composite $E \subset F \xrightarrow{\sigma} F \subset \overline{F}$. This implies that the map $X \to Y$ induced by the inclusion $F \subset \overline{F}$ is bijective, and that the natural action of $\mathrm{Gal}(F/k)$ on X is transitive. Since the stabilisator of the inclusion $E \subset F$ (viewed as an element of X) is $\mathrm{Gal}(F/E)$, we deduce that X is in bijection with the quotient $\mathrm{Gal}(F/k)/\mathrm{Gal}(F/E)$. Now $|Y| = [E : k]$ by Lemma 4.3.1 (iii), and we conclude that $[\mathrm{Gal}(F/k) : \mathrm{Gal}(F/E)] = [E : k]$.

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

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

proving that $\sigma(x) \in E$. Thus the subfield $E \subset F$ is stable under the action of $\mathrm{Gal}(F/k)$, so that $E^{\mathrm{Aut}_{k-\mathrm{alg}}(E)} \subset F^{\mathrm{Gal}(F/k)} = k$. It follows that the extension E/k is Galois (Proposition 4.3.4). The isomorphism $\mathrm{Gal}(F/k)/\,\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/k)$ is a consequence of Lemma 4.3.7. $\square$

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

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

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

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 $K \to F$ mapping x to y. As F is separable over K, this morphism extends to a morphism of k-algebras $\sigma\colon F \to F$ by Lemma 4.3.12 (i), which is an isomorphism by Lemma 4.3.12 (ii). We have thus constructed $\sigma \in \mathrm{Aut}_{k-\mathrm{alg}}(F)$ such that $\sigma(x) \neq x$, proving that F is Galois (Proposition 4.3.4). $\square$

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 $\mathrm{Gal}(F_n/k)$ is cyclic of order n, generated by the automorphism $x \mapsto x^q$. We deduce that (see Example 4.2.4)

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

Finally, the existence of pro-p-Sylow subgroups has the following consequence:

Lemma 4.3.16. *Let p be a prime number. Then there exists a separable extension E/k having the following properties:*

(i) The degree of every finite separable extension of E is a power of p.
(ii) The degree of every finite subextension of E/k is prime to p.

Proof. Let k_s be a separable closure of k, and P a pro-p-Sylow subgroup of $\mathrm{Gal}(k_s/k)$. We set $E = (k_s)^P$.

(i): Let D/E be a finite separable extension. By Lemma 4.3.12 (i) we may assume that $D \subset k_s$. By Theorem 4.3.11, the integer $[D : E]$ coincides with the index of the open subgroup $\mathrm{Gal}(k_s/D)$ in the pro-p-group $P = \mathrm{Gal}(k_s/E)$, hence is a power of p.

(ii): Let L/k be a finite subextension of E/k. Then we may find a Galois subextension F/k of k_s/k containing L. Let Q be the image of P under the morphism $\mathrm{Gal}(k_s/k) \to \mathrm{Gal}(F/k)$, and set $K = F^Q$. Since by Proposition 4.3.2 we have $|\mathrm{Gal}(F/k)| = [F : k] = [F : K] \cdot [K : k]$ and $|Q| = |\mathrm{Gal}(F/K)| = [F : K]$, it follows that $[K : k]$ is the index of Q in $\mathrm{Gal}(F/k)$, hence is prime to p (as P is pro-p-Sylow subgroup). Now $K = (k_s)^P \cap F = E \cap F$ contains L, hence $[L : k]$ is also prime to p. □

4. Galois descent

Let us fix a Galois extension F/k and denote by Γ the profinite group $\mathrm{Gal}(F/k)$. 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 Γ-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 $e_i^* \colon W \to k$ be the linear map sending an element of W to its i-th coordinate in the above basis, and consider the k-linear map

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

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

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

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 ϵ_i is G-equivariant, it maps $(W \otimes_k U)^G$ into U^G, and the statement follows from (4.4.a). □

Definition 4.4.2. Let V be an F-vector space. A Γ-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 Γ-action. Then $V \oplus V'$ and $V \otimes_F V'$ inherit a semilinear Γ-action. So does $\mathrm{Hom}_F(V, V')$, by setting, for $f \in \mathrm{Hom}_F(V, V')$ and $\gamma \in \Gamma$

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

LEMMA 4.4.3. *Let W be a k-vector space. Then the Γ-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 $w_1, \ldots, w_n \in W$ and $\lambda_1, \ldots, \lambda_n \in F$. By Lemma 4.3.8, the elements $\lambda_1, \ldots, \lambda_n$ are contained in some finite Galois subextension L of F/k. Then the subgroup $\mathrm{Gal}(F/L) \subset \Gamma$ is open (Theorem 4.3.11) and fixes w, proving the continuity (see Lemma 4.2.11). □

LEMMA 4.4.4 (Dedekind). *Let A be a k-algebra and K/k a field extension. Let $\sigma_1, \ldots, \sigma_n$ be pairwise distinct morphisms of k-algebras $A \to K$. Then the elements*

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

are linearly independent over K. In particular $n \leq \dim_k A$.

PROOF. Assume that

$$a_1\sigma_1 + \cdots + a_m\sigma_m = 0. \tag{4.4.c}$$

where $a_1, \ldots, a_m \in K$ are not all zero. Pick such a relation, where $m \in \{1, \ldots, n\}$ is minimal. In particular $a_m \neq 0$, and $m > 1$. As $\sigma_m \neq 0$, there exists $i \in \{1, \ldots, m-1\}$ 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 $\sigma_1, \ldots, \sigma_m$ are multiplicative, it follows from (4.4.c) that

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

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 $\dim_K \mathrm{Hom}_k(A, K) = \dim_K A_K = \dim_k A$. □

PROPOSITION 4.4.5 (Galois descent). *Let V be an F-vector space. If Γ acts continuously on V by semilinear automorphisms, then the natural morphism $V^\Gamma \otimes_k F \to V$ is bijective.*

PROOF. Denote by φ the morphism $V^\Gamma \otimes_k F \to V$. The proof of the injectivity of φ is a recast of the proof of Proposition 4.3.2. Namely, assume that the kernel of φ 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 $i = 1, \ldots, r$. Choose r minimal with this property. Then $v_1, \ldots, v_r$ are linearly independent over k. Replacing v with $\lambda_1^{-1}v$, we may assume that $\lambda_1 = 1$. Since the elements $v_1, \ldots, v_r$ are linearly independent over k and $0 = \varphi(v) = \lambda_1 v_1 + \cdots + \lambda_r v_r$, there exists $j \in \{2, \ldots, r\}$ such that λ_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 Γ-action on V, the morphism φ is Γ-equivariant, hence γv lies in the kernel of φ. 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 φ. 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 φ is injective.

Conversely let $v \in V$. By continuity of the Γ-action on V, we may find a finite Galois subextension L of F/k such that v is fixed by $\mathrm{Gal}(F/L)$ (see Lemma 4.2.11 and Theorem 4.3.11). Let $e_1, \dots, e_n$ be a basis of the k-vector space L. The group $\mathrm{Gal}(L/k)$ 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 $\mathrm{Gal}(L/k)$. Consider the elements

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

Let $\gamma \in \Gamma$. Since Γ is the disjoint union of the subsets $\gamma_1 \mathrm{Gal}(F/L), \dots, \gamma_n \mathrm{Gal}(F/L)$, 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 $\mathrm{Gal}(F/L)$. 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 φ (as each w_j belongs to V^Γ). There is $i \in \{1, \dots, n\}$ such that γ_i is the preimage of $1 \in \mathrm{Gal}(L/k)$, hence belongs to $\mathrm{Gal}(F/L)$ and thus fixes v. Then $v = \gamma_i v$ belongs to the image of φ. □

Remark 4.4.6. Let A be an F-algebra. Assume that Γ acts continuously by semilinear automorphisms on the F-vector space A, and that the multiplication map of A is compatible with the Γ-action, in the sense that

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

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

Exercises

Exercise 4.1. Let p be a prime number and Γ a pro-p-group. The purpose of this exercise is to prove that the index of every subgroup of Γ is a power of p, if it is finite.

Let $n \in \mathbb{N}$, and write $n = p^r m$, where m is prime to p and $r \in \mathbb{N}$.

(i) Consider the subset $C_n = \{g^n | g \in \Gamma\}$. Show that C_n is closed in Γ.

Let now $g \in \Gamma$. Let U be an open normal subgroup of Γ.

(ii) Show that $g^{p^s} \in U$ for some $s \geq r$.
(iii) Show that $g^{p^r} \in C_n U$. (Hint: Write $p^r = ap^s + bn$, with $a, b \in \mathbb{Z}$.)
(iv) Deduce that $g^{p^r} \in C_n$.
(v) Let $H \subset \Gamma$ be a normal subgroup of index n. Show that $C_n \subset H$, and deduce that Γ/H is a finite p-group.
(vi) Conclude.

Exercise 4.2. Let F/k be a Galois field extension. Let $H \subset \mathrm{Gal}(F/k)$ be a subgroup, and $\overline{H}$ its closure. Show that $\overline{H}$ is a subgroup, and that $F^H = F^{\overline{H}}$.

Exercise 4.3. Recall that a topological space is called *Hausdorff* if any two distinct points are contained in disjoint opens subsets.

(i) Let Γ be a profinite group. We have seen that Γ is compact. Show that Γ is Hausdorff and that every open subset of Γ containing 1 contains an open normal subgroup.

Let now G be a compact and Hausdorff topological group. We assume that every open subset of G containing 1 contains an open normal subgroup. We are going to show that G is profinite. Let $\mathcal{U}$ be the set of open normal subgroups of G, ordered by setting $U \leq V$ when $V \subset U$.

(ii) Show that the groups G/U for $U \in \mathcal{U}$ form an inverse system, that the group $H = \varprojlim G/U$ is profinite and that the natural morphism $f \colon G \to H$ is continuous.
(iii) Show that f is injective.
(iv) Show that the image of f is dense (i.e. meets every nonempty open subset of H).
(v) Show that f is closed (i.e. $f(Z)$ is closed in H whenever Z is closed in G).
(vi) Conclude that $f \colon G \to H$ is a homeomorphism.

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 begin 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 $\mathrm{Hom}_{\mathcal{C}}(A,B)$,
(iii) a specified element $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$ for every $A \in \mathrm{Ob}(\mathcal{C})$,
(iv) a map (called *composition law*) $\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \to \mathrm{Hom}_{\mathcal{C}}(A,C)$ denoted by $(f,g) \mapsto g \circ f$, for every objects A, B, C.

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

(a) $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$ for every $f \colon A \to B$,
(b) $h \circ (g \circ f) = (h \circ g) \circ f$ for every $f \colon A \to B, g \colon B \to C, h \colon C \to D$.

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

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

(a) $\mathcal{F}(\mathrm{id}_B) = \mathrm{id}_{\mathcal{F}(B)}$ for every $B \in \mathcal{B}$,
(b) $\mathcal{F}(g) \circ \mathcal{F}(f) = \mathcal{F}(g \circ f)$ for every $f\colon B \to B'$ and $g\colon B' \to B''$ 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 $\mathrm{id}_{\mathcal{B}}\colon \mathcal{B} \to \mathcal{B}$.

If $\mathcal{F}, \mathcal{G}\colon \mathcal{B} \to \mathcal{C}$ are functors, a *morphism of functors* (or natural transformation) $\varphi\colon \mathcal{F} \to \mathcal{G}$ is the data of a morphism $\varphi_B\colon \mathcal{F}(B) \to \mathcal{G}(B)$ in $\mathcal{C}$ for every $B \in \mathcal{B}$ such that for every morphism $f\colon B \to B'$ in $\mathcal{B}$, the following diagram commutes

$$\begin{tikzcd}
\mathcal{F}(B) \arrow[r, "\varphi_B"] \arrow[d, "\mathcal{F}(f)"'] & \mathcal{G}(B) \arrow[d, "\mathcal{G}(f)"] \\
\mathcal{F}(B') \arrow[r, "\varphi_{B'}"] & \mathcal{G}(B')
\end{tikzcd}$$

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

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

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

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

A *contravariant functor* $\mathcal{B} \to \mathcal{C}$ is a functor $\mathcal{B}^{\mathrm{op}} \to \mathcal{C}$. 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

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

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. □

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 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 $\mathbf{X}(K) \neq \varnothing$, 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 $K \to F$ by Lemma 4.3.1 (iii). Let $f \colon K \to F$ 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 $\mathbf{X}(K)$. □

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 $\sigma \colon k_s \to L_s$. Denote by $\mu \colon k_s \otimes_k L \to L_s$ 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 $f \colon A \to k_s$ induces a morphism of L-algebras

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

which fits into the commutative diagram

$$\begin{tikzcd} A_L \arrow[r, "\widetilde{f}"] & L_s \\ A \arrow[u, "a \mapsto a\otimes 1"] \arrow[r, "f"] & k_s \arrow[u, "\sigma"'] \end{tikzcd}$$

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

Proposition 5.2.6. *Assume that $k = k_s$, and let A be an étale k-algebra. Let M be the set of maps $\mathbf{X}(A) \to k$, with its k-algebra structure given by pointwise operations. Then the morphism of k-algebras $A \to M$ 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 $\mathrm{Hom}_k(A, k)$. In particular the intersection of their kernels is zero. Thus the morphism of the statement is injective, hence bijective by dimensional reasons. □

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 $A \to k_s$ maps x to zero, hence factors uniquely through the quotient morphism $A \to A/xA$. In other words, the natural map $\mathbf{X}(A/xA) \to \mathbf{X}(A)$ 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. □

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 $A \times B \to A$ and $A \times B \to B$ 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. □

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[1] 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

$$\psi \colon A \to \prod_{\mathfrak{m} \in M} A/\mathfrak{m}.$$

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 $e_{\mathfrak{m},\mathfrak{m}'} = 1 \mod \mathfrak{m}$. 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 ψ is A-linear, we conclude that ψ is surjective.

[1] 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 ψ. □

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. □

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 $\overline{k}$ is an algebraic closure of k, then the ring $A_{\overline{k}}$ is reduced.
(v) If L/k is a field extension, then the ring A_L is reduced.

PROOF. (i) ⇒ (ii) : This follows from Lemma 5.2.5 and Corollary 5.2.7.
(ii) ⇒ (i) : The projections $(k_s)^n \to k_s$ yield n distinct elements of $\mathbf{X}(A)$.
(iii) ⇒ (i) : This follows from Lemma 5.2.10 (ii) and Lemma 5.2.4.
(i) ⇒ (v) : This follows from Lemma 5.2.5 and Lemma 5.2.9.
(v) ⇒ (iv) : Clear.
(iv) ⇒ (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 $\overline{k}[X]/P \simeq B_{\overline{k}}$ is reduced, being contained in $K_{\overline{k}}$, which is reduced because $A_{\overline{k}}$ is so (in view of Remark 5.2.8). This implies that $P \in k[X]$ is separable : indeed if $P = (X-a)Q \in \overline{k}[X]$ where $Q \in \overline{k}[X]$ and $a \in \overline{k}$ are such that $Q(a) = 0$, then $P \mid Q^2$, hence Q defines a nonzero nilpotent element of $\overline{k}[X]/P$. □

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 $\overline{k}$ be an algebraic closure of k, and $\overline{L}$ an algebraic closure of L. By Lemma 4.3.12 (i), we may view $\overline{k}$ as a subfield of $\overline{L}$. The ring $A_{\overline{L}}$ is reduced by assumption (and the criterion (v) in Proposition 5.2.13), hence so is its subring $A_{\overline{k}}$. This proves that A is étale by the criterion (iv) in Proposition 5.2.13. □

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

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

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

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

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

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

For any $a \in A$, we have $\mathrm{N}_{A/k}(a) = \det(l_a)$. The properties of the determinant imply that, for any $a, b \in A$

$$\mathrm{N}_{A/k}(ab) = \mathrm{N}_{A/k}(a)\,\mathrm{N}_{A/k}(b) \quad ; \quad \mathrm{N}_{A/k}(1) = 1. \tag{5.3.a}$$

LEMMA 5.3.2. *Let A be a finite-dimensional k-algebra, and $a \in A$. Then $a \in A^\times$ if and only if $\mathrm{N}_{A/k}(a) \neq 0$.*

PROOF. It follows from (5.3.a) that $\mathrm{N}_{A/k}(a) \in k^\times$ when $a \in A^\times$. Conversely if $\mathrm{N}_{A/k}(a) \neq 0$, the k-linear map $l_a \colon A \to A$ is bijective. Its surjectivity yields an element $b \in A$ such that $ab = 1$, and we conclude using Remark 1.1.11. □

In particular the norm map induces a group morphism $\mathrm{N}_{A/k} \colon A^\times \to k^\times$.

PROPOSITION 5.3.3. *Let A be an étale k-algebra. Then for any $a \in A$, we have*

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

In particular

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

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. □

COROLLARY 5.3.4. *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*

$$\mathrm{N}_{K/k} \circ \mathrm{N}_{A/K} = \mathrm{N}_{A/k} \quad \textit{and} \quad \mathrm{Tr}_{K/k} \circ \mathrm{Tr}_{A/K} = \mathrm{Tr}_{A/k}.$$

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

$$\alpha\colon \mathbf{X}(K) \times \mathbf{X}(A/K) \to \mathbf{X}(A) \quad ; \quad (f,g) \mapsto \widetilde{f} \circ g.$$

If $f, f' \in \mathbf{X}(K)$ and $g, g' \in \mathbf{X}(A/K)$ are such that $\widetilde{f} \circ g = \widetilde{f'} \circ g' \colon A \to k_s$, composing with the unique morphism of K-algebras $K \to A$ we see that $f = f'$. Therefore $\widetilde{f} = \widetilde{f'}$, hence $g = g'$ (by injectivity of $\widetilde{f}$), proving that α 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 $h\colon A \to k_s$ is a morphism of K-algebras, and $\widetilde{f}\colon K_s \to k_s$ is an isomorphism of K-algebras by Lemma 4.3.12 (ii). So we may set $g = \widetilde{f}^{-1} \circ h \in \mathbf{X}(A/K)$. Then $\widetilde{f} \circ g = h$, proving that α 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 $\widetilde{f} \circ g \in \mathbf{X}(A)$ for $f \in \mathbf{X}(K)$ and $g \in \mathbf{X}(A/K)$. If $a \in A$ then, in view of Proposition 5.3.3

$$\begin{aligned}
\mathrm{N}_{K/k} \circ \mathrm{N}_{A/K}(a) &= \prod_{f \in \mathbf{X}(K)} f\Big(\prod_{g \in \mathbf{X}(A/K)} g(a) \Big) \\
&= \prod_{f \in \mathbf{X}(K)} \prod_{g \in \mathbf{X}(A/K)} \widetilde{f} \circ g(a) \\
&= \prod_{h \in \mathbf{X}(A)} h(a) \\
&= \mathrm{N}_{A/k}(a),
\end{aligned}$$

and similarly

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

□

Remark 5.3.5. Corollary 5.3.4 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 Γ on the set $\mathbf{X}(A)$.

Lemma 5.4.1. *Let A be a finite-dimensional k-algebra. Then the Γ-action on $\mathbf{X}(A)$ is continuous (Definition 4.2.12).*

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 4.2.11. □

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

Let now X be a finite discrete Γ-set of cardinality n. The set

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

is naturally a commutative k_s-algebra (via pointwise operations), which is isomorphic to $(k_s)^n$. The Γ-actions on k_s and X induce a left Γ-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 Γ-equivariant maps $X \to k_s$.

Lemma 5.4.2. *If X is a finite discrete Γ-set, the Γ-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 Γ-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 Γ 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 Γ fixing f. □

We deduce from Proposition 4.4.5 that the natural morphism of k_s-algebras

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

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 Γ-sets $\alpha\colon X \to Y$ corresponds a morphism of étale k-algebras $\mathbf{M}(Y)^\Gamma \to \mathbf{M}(X)^\Gamma$ given by $f \mapsto f \circ \alpha$, and one sees easily that $\mathbf{M}^\Gamma\colon X \mapsto \mathbf{M}(X)^\Gamma$ defines a contravariant functor $\mathsf{Fsets}_\Gamma \to \mathsf{Et}_k$.

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

$$\Phi_A\colon A \to \mathbf{M}^\Gamma(\mathbf{X}(A)).$$

Lemma 5.4.3. *Let A be a finite-dimensional k-algebra. Then A is étale if and only if Φ_A is an isomorphism.*

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

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

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 Φ_A (exercise). □

We can now establish our first interesting equivalence of categories.

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

Proof. Let X be a finite discrete Γ-set. Consider the map

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

mapping $x \in X$ to the morphism of k-algebras $\mathbf{M}(X)^\Gamma \to k_s$ 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 Ψ_X is Γ-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 Ψ_X have the same finite number of elements, the map Ψ_X is bijective.

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

To conclude note that Ψ and Φ in fact define functors. □

The theorem implies that operations on étale algebras correspond bijectively to operations on finite discrete Γ-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 Γ-sets, there are natural Γ-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 Γ-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 Γ 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 Γ acts trivially on the finite set X. Then $\mathbf{M}^\Gamma(X)$ may be identified with the k-algebra consisting of the maps $X \to k$. 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 $\Gamma = \mathrm{Gal}(k_s/k)$.

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 Γ-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 Γ-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 Γ-set $Y = X/G$. Since a map $Y \to k_s$ is the same thing as a map $X \to k_s$ 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). □

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) $\dim_k A \geq |G|$.

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.

LEMMA 5.5.4. *Let A be a Galois G-algebra. Then* $\dim_k A = |G|$.

PROOF. Since $A^G = k$, the group G acts transitively on $\mathbf{X}(A)$ (Proposition 5.5.2). Thus, as A is étale, we have $\dim_k A = |\mathbf{X}(A)| \leq |G|$. □

LEMMA 5.5.5. *Let A be an étale G-algebra. Then the following conditions are equivalent:*
(a) The G-algebra A is Galois.
(b) We have $\mathbf{X}(A) \neq \varnothing$ and the G-action on $\mathbf{X}(A)$ is simply transitive.

PROOF. 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 $|G|$. □

LEMMA 5.5.6. *Let A be a Galois G-algebra. Then the natural morphism $G \to \mathrm{Aut}_{k-\mathrm{alg}}(A)$ is injective.*

PROOF. If $g \in G$ acts trivially on A, then g acts trivially on $\mathbf{X}(A)$. Since the G-action on $\mathbf{X}(A)$ is simply transitive (Lemma 5.5.5), we must have $g = 1$. □

EXAMPLE 5.5.7. 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 $\mathrm{Gal}(L/k)$-algebra over k. Conversely, if L is a G-algebra, then L/k is a Galois field extension, and the morphism $G \to \mathrm{Gal}(L/k)$ is bijective.

Example 5.5.8. Consider the set S consisting of all maps $G \to k$, with the k-algebra structure given by pointwise operations. The group G naturally acts on S: if f is a map $G \to k$ and $g \in G$, then $g \cdot f$ is the map $G \to k$ 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 $G \to k$, which coincides with $k \subset S$. Therefore S is a Galois G-algebra. We have $\mathbf{X}(S) = G$ with the trivial Γ-action (see Remark 5.4.7), and the G-action given by right multiplication.

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

Proposition 5.5.9. *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 Γ-sets with a simply transitive G-action.*

Proof. This follows from Lemma 5.5.5 and Theorem 5.4.4. □

Corollary 5.5.10. *Every morphism of Galois G-algebras is an isomorphism.*

Proof. This is so in the category of nonempty finite discrete Γ-sets with a simply transitive G-action. □

Definition 5.5.11. We say that a Galois G-algebra A is *split* if Γ acts trivially on the set $\mathbf{X}(A)$.

It follows from Proposition 5.5.9 that a Galois G-algebra is split if and only if it is isomorphic to the algebra S of Example 5.5.8.

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 5.5.12. *Let A be a Galois G-algebra, and consider the split G-algebra S of Example 5.5.8. 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 $\alpha \colon G \times X \to X \times X$ given by $(g, x) \mapsto (x \cdot g, x)$ is bijective. It is Γ-equivariant, if we let Γ act trivially on G. Under the equivalence of Theorem 5.4.4, this yields an isomorphism of k-algebras $\beta \colon A \otimes_k A \to S \otimes_k A$. Since α is G-equivariant for the right G-actions via the first factors, it follows that β is G-equivariant for the left G-actions via the first factors.

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

Proposition 5.5.12 will be exploited via the next corollary.

Corollary 5.5.13. *Let A be a Galois G-algebra, and $A \to K$ a morphism of k-algebras, where K is a field. Then the Galois G-algebra A_K over K is split.*

PROOF. Let $f\colon A \to K$ 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 $\beta\colon A \otimes_k A \to S \otimes_k A$ of Proposition 5.5.12 induces an isomorphism of K-vector spaces $\beta'\colon A \otimes_k K \to S \otimes_k K$, and it follows from Proposition 5.5.12 that β' is a morphism of G-algebras over K. □

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 5.5.14. *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,

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

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 5.3.3. □

DEFINITION 5.5.15. Let $H \subset G$ be a subgroup and B a H-algebra over k. Consider the set

$$\mathrm{Ind}_H^G(B) = \{\text{maps } f\colon G \to B \text{ such that } f(h \cdot g) = h \cdot f(g) \text{ for all } g \in G, h \in H\},$$

viewed as a k-algebra, via pointwise operations on B. If $f \in \mathrm{Ind}_H^G(B)$ and $g \in G$, we define an element $g \cdot f \in \mathrm{Ind}_H^G B$ by mapping a $x \in G$ to $f(x \cdot g)$. This gives $\mathrm{Ind}_H^G(B)$ the structure of a G-algebra.

REMARK 5.5.16. The G-algebra S considered in Example 5.5.8 coincides with $\mathrm{Ind}_1^G(k)$.

There are morphisms of H-algebras

$$\pi\colon \mathrm{Ind}_H^G(B) \to B \quad ; \quad f \mapsto f(1), \tag{5.5.a}$$

and

$$\nu\colon B \to \mathrm{Ind}_H^G(B) \quad ; \quad \nu(b)(g) = \begin{cases} g \cdot b & \text{if } g \in H \\ 0 & \text{if } g \notin H \end{cases} \quad \text{for } b \in B \text{ and } g \in G. \tag{5.5.b}$$

Note that $\pi \circ \nu = \mathrm{id}_B$.

LEMMA 5.5.17. *Let H be a subgroup of G, and B an H-algebra over k. Then the H-algebra B is Galois if and only if the G-algebra $\mathrm{Ind}_H^G(B)$ is Galois.*

PROOF. Let $A = \mathrm{Ind}_H^G(B)$. Observe that the choice of a set of representatives of G/H yields an isomorphism of k-algebras $A \simeq B^{|G/H|}$. It thus follows from Lemma 5.2.10 (ii) that B is étale if and only if A is so. Moreover

$$\dim_k A = \dim_k B^{|G/H|} = |G/H| \dim_k B,$$

so that $\dim_k B = |H|$ if and only if $\dim_k A = |G|$. The morphism $\pi\colon A \to B$ of (5.5.a) induces an isomorphism $A^G \simeq B^H$, so that $A^G = k$ if and only if $B^H = k$. □

Proposition 5.5.18. *Let A be a Galois G-algebra over k.*

(i) There exists a morphism of k-algebras $f\colon A \to k_s$, and its image L does not depend on the choice of f.

(ii) The k-algebra L is a Galois field extension of k.

(iii) There exists a subgroup H of G isomorphic to $\mathrm{Gal}(L/k)$, and such that $A \simeq \mathrm{Ind}_H^G(L)$ (where L is viewed as an H-algebra via the isomorphism $\mathrm{Gal}(L/k) \simeq H$).

Proof. Let $X = \mathbf{X}(A)$. By Lemma 5.5.5, we may find an element $f \in X$, and $\mathbf{X}(A) = \{f \circ g | g \in G\}$. For $g \in G$, the morphisms f and $f \circ g$ have the same image (as $g\colon A \to A$ is surjective), proving (i).

The finite-dimensional k-algebra L is a field (Lemma 3.1.2), and the surjective morphism of k-algebras $\varphi\colon A \to L$ (induced by f) identifies $\mathbf{X}(L)$ with the Γ-orbit $Y \subset X$ of f (see Remark 5.4.6). Let $H \subset G$ be the subgroup of elements mapping Y to itself. Then the morphism φ is H-equivariant. Let $y, z \in Y$. Since G acts transitively on X, we may find $g \in G$ such that $z = y \cdot g$. Then every element of Y is of the form γy for some $\gamma \in \Gamma$, and we have $(\gamma y) \cdot g = \gamma(y \cdot g) = \gamma z \in Y$, proving that $g \in H$. Therefore the H-action on Y is transitive, and in fact simply transitive (because G acts simply transitively on X). It follows from Proposition 5.5.9 that L is a Galois H-algebra over k. By Example 5.5.7, the extension L/k is Galois and the H-action on L induces an isomorphism $H \simeq \mathrm{Gal}(L/k)$ by Example 5.5.7. We have proved (ii).

We define a morphism of k-algebras $\psi\colon A \to \mathrm{Ind}_H^G(L)$ by mapping $a \in A$ to the map $g \mapsto \varphi(g \cdot a)$ (which is H-equivariant because φ is so). The morphism ψ is G-equivariant, since for $g \in G$ and $a \in A$, we have

$$(g \cdot \psi(a))(x) = \psi(a)(x \cdot g) = \varphi(x \cdot g \cdot a) = \psi(g \cdot a)(x) \quad \text{for all } x \in G,$$

so that $g \cdot \psi(a) = \psi(g \cdot a)$. Since both A and $\mathrm{Ind}_H^G(A)$ are Galois G-algebras, the morphism ψ has to be an isomorphism (Corollary 5.5.10). This concludes the proof of (iii). □

Lemma 5.5.19. *In the situation of Proposition 5.5.18, the norm maps $\mathrm{N}_{L/k}$ and $\mathrm{N}_{A/k}$ have the same image.*

Proof. We use the morphisms π and ν of (5.5.a) and (5.5.b). Let $x \in L$, and $f = \nu(x) \in A$. Then, in view of Proposition 5.5.14

$$\mathrm{N}_{A/k}(f) = \pi \circ \mathrm{N}_{A/k}(f) = \sum_{g \in G} \pi(g \cdot f) = \sum_{g \in G} f(g) = \sum_{h \in H} h \cdot x = \mathrm{N}_{L/k}(x).$$

This proves that $\mathrm{N}_{L/k}(L) \subset \mathrm{N}_{A/k}(A)$. Now the morphism $\nu\colon L \to A$ allows us the view A as an L-algebra, and using transitivity of the norms (Corollary 5.3.4), we have $\mathrm{N}_{A/k} = \mathrm{N}_{L/k} \circ \mathrm{N}_{A/L}$, so that in particular $\mathrm{N}_{A/k}(A) \subset \mathrm{N}_{L/k}(L)$. □

Exercises

Exercise 5.1. Let A be a k-algebra. Recall that $\mathbf{X}(A)$ denotes the set k-algebra morphisms $A \to k_s$, where k_s is a separable closure of k.

We assume that A is étale.

(i) Let B be a quotient algebra of A. Show that B is étale and that the map $\mathbf{X}(B) \to \mathbf{X}(A)$ is injective.
(ii) Let B be a subalgebra of A. Show that B is étale and that the map $\mathbf{X}(A) \to \mathbf{X}(B)$ is surjective. (Hint: assuming that the map is not surjective, produce an element of the kernel of $\mathbf{M}(\mathbf{X}(B)) \to \mathbf{M}(\mathbf{X}(A))$.)
(iii) Show that A has only finitely many subalgebras and quotient algebras.
(iv) Assume that k is infinite. Show that there exists a separable polynomial P such that $A \simeq k[X]/P$. (Hint: to show that A is generated by a single element as a k-algebra, observe that no k-vector space is a finite union of proper subspaces.)

Exercise 5.2. Let A be a finite-dimensional k-algebra. For an element $a \in A$ recall that $\mathrm{Tr}_{A/k}(a) \in k$ is the trace of the k-linear map $A \to A$ given by $x \mapsto ax$.

(i) Show that a finite-dimensional commutative k-algebra A is étale if and only if for every nonzero $a \in A$ there exists $b \in A$ such that $\mathrm{Tr}_{A/k}(ab) \neq 0$.
(ii) Show that a finite field extension L/k is separable if and only if the map $\mathrm{Tr}_{L/k} \colon L \to k$ is nonzero.

Exercise 5.3. Let K/k be a field extension. We have seen in Example 5.5.7 that there is at most one group G (up to isomorphism) such that K is a Galois G-algebra (namely K/k must be Galois, and $G = \mathrm{Gal}(K/k)$). We give here an example of an algebra A (which is not field) admitting G-Galois structures for two nonisomorphic groups G.

Let K be a separable quadratic extension of k, and $A = K \times K$.

(i) Define a $\mathbb{Z}/4$-Galois algebra structure on A.
(ii) Define a $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$-Galois algebra structure on A.

Exercise 5.4. Let k_s be a separable closure of k, and $\Gamma = \mathrm{Gal}(k_s/k)$. Let A be an étale k-algebra of dimension n. Consider the associated discrete Γ-set $X = \mathrm{Hom}_{k-\mathrm{alg}}(A, k_s)$. Let $Y \subset X^n$ be the set of those $(x_1, \ldots, x_n)$ such that $x_i \neq x_j$ when $i \neq j$, with the Γ-action given by

$$\gamma(x_1, \ldots, x_n) = (\gamma x_1, \ldots, \gamma x_n) \quad \text{for } \gamma \in \Gamma, \text{ and } x_1, \ldots, x_n \in X.$$

The symmetric group $\mathfrak{S}_n$ acts on Y by

$$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

where $\sigma \in \mathfrak{S}_n$ and $x_1, \ldots, x_n$ are pairwise distinct elements of X. Denote by Z the quotient of Y be the action of the subgroup $\mathfrak{A}_n$ of even permutations (the kernel of the signature morphism $\mathfrak{S}_n \to \mathbb{Z}/2$).

(i) Show that Z is a discrete Γ-set having two elements.

We denote by Δ the corresponding étale k-algebra of dimension two; it is called the *discriminant algebra* of A.

Assume now that k has characteristic $\neq 2$. Let $e_1, \ldots, e_n$ be a k-basis of A, let $f_1, \ldots, f_n$ be the elements of X, and consider the matrix $M = (f_i(e_j)) \in M_n(k_s)$. Set

$$u = \det M \in k_s.$$

Let Γ_0 be the subgroup of Γ consisting of those elements acting by even permutations on the set X.

(ii) Let $\gamma \in \Gamma$. Show that $\gamma u = u$ if $\gamma \in \Gamma_0$ and $\gamma u = -u$ otherwise.

Let d be the determinant of the matrix $(\mathrm{Tr}_{A/k}(e_i e_j)) \in M_n(k)$.

(iii) Show that $d = u^2$. (Hint: compute the product $M^t \cdot M$.)

(iv) Conclude that $\Delta \simeq k[X]/(X^2 - d)$.

CHAPTER 6

Torsors, cocyles, 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-cocyles. 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-cocyles 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-cocyles; this is only true "up to isomorphism", and therefore some care is required when working with twisted forms and 1-cocyles. 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 Γ is a profinite group, and G a discrete Γ-group (Definition 4.2.12). We will denote Γ-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 Γ-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 Γ-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 Γ-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 Γ- 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 Γ- and G-equivariant. Thus all morphisms of G-torsors are isomorphisms.

EXAMPLE 6.1.3. Let $\Gamma = \mathrm{Gal}(k_s/k)$, and G a finite group considered as a discrete Γ-group with trivial Γ-action. We have seen in Proposition 5.5.9 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 Γ-set with a compatible left G-action, and let P be a G-torsor. We now describe a procedure that yields another discrete Γ-set ${}_PX$, 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 ${}_PX$.

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

LEMMA 6.1.5. *The Γ-action on ${}_PX$ is continuous.*

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

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

$$\pi_p \colon X \to {}_PX \quad , \quad x \mapsto (p, x). \tag{6.1.a}$$

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

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

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

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

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

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

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

LEMMA 6.1.6. *The map $P \to \mathrm{Hom}_F(V, {}_PV)$ given by $p \mapsto \pi_p$ is Γ- and G-equivariant.*

PROOF. This follows from (6.1.b) and (6.1.c). □

2. Twisted forms

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

[1]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 $K \to L$ in Sep_k with L/K Galois, the $\mathrm{Gal}(L/K)$-action on the set $\mathcal{F}(L)$ is continuous, and the map

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

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 Γ-set. Conversely let X be a discrete Γ-set. For $L \in \mathsf{Sep}_k$ and $\varphi \in \mathrm{Hom}_{k-\mathrm{alg}}(L, k_s)$, let us set $X_\varphi = X^{\mathrm{Gal}(k_s/\varphi(L))}$. Let $L \to L'$ be a morphism in Sep_k. By Lemma 4.3.12, there exist $\varphi \in \mathrm{Hom}_{k-\mathrm{alg}}(L, k_s)$ and $\varphi' \in \mathrm{Hom}_{k-\mathrm{alg}}(L', k_s)$, 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 α on X induces a map $X_\varphi \to X_{\varphi'}$. Any other choice for α is of the form $\alpha \circ \gamma$ where $\gamma \in \mathrm{Gal}(k_s/\varphi(L))$, hence induces the same map $X_\varphi \to X_{\varphi'}$. It follows that, when $L \in \mathsf{Sep}_k$ is fixed, the sets X_φ for $\varphi \in \mathrm{Hom}_{k-\mathrm{alg}}(L, k_s)$ form a inverse system (here the set $\mathrm{Hom}_{k-\mathrm{alg}}(L, k_s)$ is directed by letting $\varphi' \leq \varphi$ for every φ, φ'). We denote by $\mathcal{F}(L)$ its inverse limit. Observe that the projections $\mathcal{F}(L) \to X_\varphi$ are bijections (all maps $X_\varphi \to X_{\varphi'}$ are bijections)[2]; 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 Γ-equivariant map $\mathcal{F}(k_s) \to \mathcal{G}(k_s)$ is induced by a unique morphism of k-sets $\mathcal{F} \to \mathcal{G}$ (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 $E \to L$ in Sep_k induces a group morphism $V_E \to V_L$, so that we may define a functor $\mathsf{Sep}_k \to \mathsf{Groups}$ 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 $m_1, \ldots, m_n, m'_1, \ldots, m'_n \in \mathbb{N}$. 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 $\varphi \colon V \to W$ is an isomorphism of K-vector spaces, we will write

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

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

$$T(\varphi) \circ T(\psi) = T(\varphi \circ \psi). \tag{6.2.a}$$

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

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 $T(V) \to T(V_L)$, 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 $T(V)_L \to T(V_L)$ 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 $\Gamma = \mathrm{Gal}(F/k)$.

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

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

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

Proof. Let U_1, U_1', U_2, U_2' be F-vector spaces with a semilinear Γ-action, and $\varphi\colon U_1 \to U_2$, $\varphi'\colon U_1' \to U_2'$ 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

$$\psi = \mathrm{Hom}_F(\varphi^{-1}, \varphi')\colon \mathrm{Hom}_F(U_1, U_1') \to \mathrm{Hom}_F(U_2, U_2').$$

For $f \in \mathrm{Hom}_F(U_1, U_1')$, 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 $\gamma\psi = \mathrm{Hom}_F((\gamma\varphi)^{-1}, \gamma\varphi')$. In view of the construction of the functor T, this proves the statement. □

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

Proof. Let U, U' be k-vector spaces. From the Γ-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 Γ-action on U_F' induces a Γ-action on $\mathrm{Hom}_k(U, U_F')$, and the identification $\mathrm{Hom}_F(U_F, U_F') = \mathrm{Hom}_k(U, U_F')$ given by $f \mapsto f|_U$ is Γ-equivariant. Thus

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

and the statement follows as above from the construction of T. □

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 $\Gamma = \mathrm{Gal}(F/k)$.

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 $\varphi\colon S_F \to R_F$ such that $T(\varphi)(s_F) = r_F$. A morphism $(R, r) \to (R', r')$ of twisted forms of (S, s) is an isomorphism of k-vector spaces $\psi\colon R \to R'$ such that $T(\psi)(r) = r'$. This defines a category of twisted forms of (S, s).

Remark 6.2.9. The isomorphism φ 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

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

When $f\colon E \to L$ is a morphism in Sep_k and $\varphi \in \mathcal{I}(E)$, the map $\mathcal{I}(f)(\varphi) = \varphi \otimes_E \mathrm{id}_L$ fits into the commutative diagram

$$\begin{tikzcd} S_E \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}_S \otimes_k f"'] & R_E \arrow[d, "\mathrm{id}_R \otimes_k f"] \\ S_L \arrow[r, "\mathcal{I}(f)(\varphi)"] & R_L \end{tikzcd} \tag{6.2.b}$$

We have thus defined a functor $\mathcal{I}\colon \mathsf{Sep}_k \to \mathsf{Sets}$. 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 $\gamma \in \mathrm{Aut}_{k-\mathrm{alg}}(L)$ on $\varphi \in \mathcal{I}(L)$ is given by

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

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

We will make the following assumption:

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

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 $f\colon K \to L$ be a morphism in Sep_k so that L/K is Galois, and $\varphi \in \mathcal{I}(L)$. Since $\mathrm{Gal}(L/K)$ acts continuously on R_L (by Lemma 4.4.3), we may find an open normal subgroup U of $\mathrm{Gal}(L/K)$ 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)

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

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

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

$$\psi = \varphi^{\mathrm{Gal}(L/K)}\colon S_K \to R_K,$$

which is an isomorphism (with inverse $(\varphi^{-1})^{\mathrm{Gal}(L/K)}$). 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 $T(R_K) \to T(R_L)$ 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 $\operatorname{Aut}(S,s)$. Thus for every separable extension L/k

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

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

We now start with an $\operatorname{Aut}(S,s)(F)$-torsor P and construct a twisted form (R,r) of (S,s). Consider the discrete Γ-set ${}_PS_F$ introduced in Definition 6.1.4. The element $s_F \in T(S_F)$ is $\operatorname{Aut}(S,s)(F)$-invariant (by definition of $\operatorname{Aut}(S,s)$). It thus follows from (6.1.c) that its image $r' = T(\pi_p)(s_F) \in T({}_PS_F)$ does not depend on the choice of $p \in P$. The element r' is Γ-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 $R = ({}_PS_F)^\Gamma$, we have a Γ-equivariant identification of F-vector spaces $R_F = {}_PS_F$ by Proposition 4.4.5. The element r' lies in $T({}_PS_F)^\Gamma = T(R_F)^\Gamma$. 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 $\varphi\colon S_F \xrightarrow{\pi_p} {}_PS_F = R_F$ 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*

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

induce an equivalence between the categories of $\operatorname{Aut}(S,s)(F)$*-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

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

does not depend on the choice of $\varphi \in P$, since for $g \in \operatorname{Aut}(S,s)(F)$, 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 Γ-equivariant, since for $\gamma \in \Gamma$ we have by (6.2.c) and (6.1.b)

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

where we used the independence of u in the choice of φ for the last step. In view of Lemma 4.4.3, the isomorphism u induces an isomorphism $u^\Gamma\colon R \to R(P)$ of K-vector spaces such that $T(u^\Gamma)(r) = r(P)$. Therefore u^Γ induces an isomorphism of twisted forms $(R,r) \simeq (R(P), r(P))$.

Conversely, let P be a $\mathrm{Aut}(S,s)(F)$-torsor, and write $(R,r) = (R(P), r(P))$. It follows from Lemma 6.1.6 that the map $v\colon P \to \mathcal{I}_{(R,r)}(F)$ sending $p \in P$ to the map $S_F \xrightarrow{\pi_p} {}_P S_F = R_F$ is an isomorphism of $\mathrm{Aut}(S,s)(F)$-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 $\mathrm{GL}(W)$, which satisfies for any separable field extension L/k.

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

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

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 $S \otimes_k A \to S$. After choosing a k-basis of A, we may set $T(V) = \mathrm{Hom}_k(V \otimes_k A, V)$. Then

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

defines a k-group. When $S = A^{\oplus n}$, we denote this k-group by $\mathrm{GL}_n(A)$. In particular we have $\mathrm{GL}_1(A)(L) = (A_L)^\times$ 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 $T(V) = \mathrm{Hom}_k(V \otimes_k V, V)$. The multiplication in S defines an element $s \in T(S)$, and the condition (6.2.d) is satisfied. Therefore

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

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 $\mathrm{Hom}_k(A \otimes_k A, A)$, define a twisted form of (S,s). Conversely, let (R,r) be a twisted form of (S,s). Then r defines a product $R \otimes_k R \to R$. The induced product on R_F defines a F-algebra structure (isomorphic to S_F). Since $R \to R_F$ 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 γ 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 $r_F\colon (R \otimes_k R)_F \simeq R_F \otimes_F R_F \to R_F$ is Γ-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 $\mathrm{Aut}(S,s)(F)$-torsor P under the correspondence of Proposition 6.2.11, then the k-algebra R may be identified with ${}_PS_F$, with its natural product. We have thus proved:

PROPOSITION 6.3.3. *Let S be a finitely generated k-algebra. There is an equivalence between the category whose objects are the k-algebras A such that $A_F \simeq S_F$ as F-algebras, and morphisms are isomorphisms of k-algebras, and the category of* $\mathrm{Aut}_{F-\mathrm{alg}}(S_F)$*-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 Γ 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 $\mathrm{Aut}_{k_s-\mathrm{alg}}((k_s)^n)$ 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 $\mathrm{Gal}(k_s/k)$-action).

EXAMPLE 6.3.5. (Galois G-algebras) Let G be a finite group, viewed as a discrete Γ-group with the trivial $\mathrm{Gal}(k_s/k)$-action. Consider the split Galois G-algebra S described in Example 5.5.8. 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 5.5.9.

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 $(x_1,\ldots,x_n) \mapsto x_1^2 + \cdots + x_n^2$. For each separable field extension L/k, let $\mathrm{O}_n(L)$ be the group of isometries of the quadratic form q_L. Then O_n defines a k-group by Proposition 6.2.10, and $\mathrm{O}_n(k_s)$-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

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

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 $\mathrm{PGL}_n(k_s)$-torsors.

4. 1-cocyles

In this section we fix a profinite group Γ. Let G be a discrete Γ-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 Γ with values in G is a continuous map $\xi\colon \Gamma \to G$ (for the discrete topology on G) that we denote by $\gamma \mapsto \xi_\gamma$, and such that

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

The set of 1-cocyles $\Gamma \to G$ will be denoted by $Z^1(\Gamma, G)$. We define an equivalence relation by declaring two 1-cocyles ξ,η *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 Γ-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 $\xi \colon \Gamma \to G$ is a 1-cocyle, 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 Γ-action on the discrete Γ-group G is trivial, a 1-cocyle $\Gamma \to G$ is just a continuous group morphism $\Gamma \to G$. Two 1-cocyles are cohomologous if and only if they are conjugated by an element of G. In particular if M is a discrete Γ-module with trivial Γ-action, then $Z^1(\Gamma, M) = H^1(\Gamma, M)$ is the group of continuous group morphisms $\Gamma \to M$.

Let $\xi \colon \Gamma \to G$ be a 1-cocyle. Let X be a discrete Γ-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

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

A straight-forward verification show that this defines a Γ-action on X. Any $x \in X$ is fixed by some open subgroup $V \subset \Gamma$ (for the original action), and the 1-cocyle ξ factors through the quotient map $\Gamma \to \Gamma/U$ for some open subgroup $U \subset \Gamma$ by Lemma 4.2.14. Then $\gamma \star_\xi x = x$ for all $\gamma \in U \cap V$, which proves the Γ-action defined in (6.4.b) is continuous.

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

Now let $a \in G$, and consider the 1-cococycle $\xi' \colon \Gamma \to G$ 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 Γ-sets ${}_\xi X \to {}_{\xi'} X$. This shows that twisting the action by cohomologous 1-cocyles yields isomorphic discrete Γ-sets.

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

PROPOSITION 6.4.6. *Let G be a discrete Γ-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. □

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

(i) Let $\xi \colon \Gamma \to G$ be a 1-cocyle. 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 $\xi \colon \Gamma \to G$.

(iii) *Let ξ, ξ' be 1-cocycles $\Gamma \to G$. Then ${}_\xi G \simeq {}_{\xi'} G$ as G-torsors if and only if ξ and ξ' are cohomologuous.*

(iv) *Let P be a G-torsor and $p \in P$. Then there is a unique map $\xi \colon \Gamma \to G$ such that $\gamma p = p \cdot \xi_\gamma$ for all $\gamma \in \Gamma$. The map ξ is a 1-cocycle such that $P \simeq {}_\xi G$ as G-torsors.*

(v) *Let X be a discrete Γ-set with a compatible left G-action. Let $\xi \colon \Gamma \to G$ be a 1-cocyle, and $P = {}_\xi G$. Then ${}_P X \simeq {}_\xi X$ as discrete Γ-sets.*

PROOF. (i): We need to check that the G-action on itself given by right multiplication is compatible with the twisted Γ-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 Γ acting trivially on p, then ξ factors as $\Gamma/U \to G$, so that the map ξ is continuous by Lemma 4.2.14. 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 ξ is 1-cocyle. The map ${}_\xi G \to P$ given by $g \mapsto p \cdot g$ is G-equivariant for the right G-actions. It is also Γ-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 ${}_\xi G \to P$ is thus a morphism of G-torsors, hence an isomorphism.

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

The proofs of (iii) and (v) will rely on the following computation. Let $\xi \colon \Gamma \to G$ be a 1-cocyle, and $\varphi \colon G_\xi \to P$ 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 ξ and ξ' 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 $\pi_p \colon X \to {}_P X$ induces a Γ-equivariant bijection ${}_\xi X \to {}_P X$. $\square$

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

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

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

When A is a discrete Γ-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 Γ-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-cocyles $\Gamma \to A$ with a morphism of discrete Γ-groups $f\colon A \to B$ yields a morphism of pointed sets

$$f_*\colon H^1(\Gamma, A) \to H^1(\Gamma, B).$$

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

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

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

For $c \in C^\Gamma$, the class $\delta(c) \in H^1(\Gamma, A)$ is represented by the 1-cocyle sending $\gamma \in \Gamma$ to $b^{-1}(\gamma b) \in A \subset B$, where $b \in B$ is any preimage of c. The preimage of $c \in C^\Gamma$ under the map $B \to C$ 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 $H^1(\Gamma, A) \to H^1(\Gamma, B)$ is isomorphic to the quotient of the pointed set C^Γ by the left action of B^Γ.*

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-cocyles $\gamma \mapsto b^{-1}(\gamma b)$ and $\gamma \mapsto b'^{-1}(\gamma b')$ are cohomologuous, 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^Γ. $\square$

PROPOSITION 6.4.12. *Any exact sequence of discrete Γ-groups*

$$1 \to A \to B \to C \to 1$$

induces an exact sequence of pointed sets

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

The morphism of pointed sets δ is the one described in Proposition 6.4.10; it is a group morphism if A is a discrete Γ-module.

PROOF. This is clear. $\square$

COROLLARY 6.4.13. *Any exact sequence of discrete Γ-modules*

$$1 \to A \to B \to C \to 1$$

induces an exact sequence of groups

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

The morphism δ 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 $G(L) \to G(L')$ and $X(L) \to X(L')$, for every morphism $L \to L'$ in 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 $\mathrm{Gal}(F/k)$-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 $\varphi \colon F \to F'$, which yields a bijection $X(F) \to X(F')$ 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

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

Definition 6.4.16. Let $f \colon H \to G$ 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

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

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

$$1 \to A \to B \to C \to 1$$

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

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

is exact.

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

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

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

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

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

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

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 $\varphi \colon S_F \to R_F$ such that $T(\varphi)(s_F) = r_F$. A 1-cocyle corresponding to (R, r) is given by the map $\Gamma \to \mathrm{Aut}(S, s)(F)$ sending $\gamma \in \Gamma$ to the composite

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

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-cocyle 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 $\mathrm{Gal}(k_s/k) \to \mathfrak{S}_n$ 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 Γ acts trivially on G, this is the set of continuous group morphisms $\mathrm{Gal}(k_s/k) \to G$ modulo conjugation by elements of G (Remark 6.4.3). In particular, if G is abelian, this is the set of continuous group morphisms $\mathrm{Gal}(k_s/k) \to G$.

Exercises

Exercise 6.1. Let Γ be a profinite group, and $f\colon A \to B$ be a morphism of Γ-groups. Composing 1-cocyles with f yields a map $f_*\colon H^1(\Gamma, A) \to H^1(\Gamma, B)$. Describe this map in terms of torsors.

Exercise 6.2. (i) Let V be a k-vector space of finite dimension n, and $f\colon V \times V \to k$ be a k-bilinear form. We assume that $f(x,x) = 0$ for all $x \in V$ (i.e. f is alternated) and that the k-linear map $V \to \mathrm{Hom}_k(V,k)$ sending x to the map $y \mapsto f(x,y)$ is bijective (i.e. f is nondegenerate). Show that n is even, and that V admits a k-basis $e_1, \dots, e_n$ such that $f(e_{2r+1}, e_{2r+2}) = 1$ and $f(e_{2r+2}, e_{2r+1}) = -1$ for all $0 \le r < n/2$, and $f(e_i, e_j) = 0$ for all other values of i, j.

(ii) Let $r \in \mathbb{N} - 0$ and consider the matrix (where blank entries are zero)

$$J = \begin{pmatrix} 0 & 1 & & & & & \\ -1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & -1 & 0 \end{pmatrix} \in M_{2r}(k).$$

Show that letting, for every separable field extension L/k,

$$\mathrm{Sp}_{2r}(L) = \{M \in M_{2r}(L) | M^t J M = J\},$$

where M^t denotes the transpose of M, defines a k-group Sp_{2r} such that $H^1(k, \mathrm{Sp}_{2r}) = \{*\}$.

Exercise 6.3. For every separable extension L/k denote by $L[X]$ the polynomial algebra in one variable over L, and set

$$G(L) = \mathrm{Aut}_{L-\mathrm{alg}}(L[X]).$$

Extension of scalars yields a map $G(L) \to G(L')$ for every morphism $L \to L'$ of separable extensions of k.

(i) Show that G defines a k-group.
(ii) Show that every element of $G(L)$ is of the form $X \mapsto aX + b$, where $a \in L^\times$ and $b \in L$.
(iii) Show that we have an exact sequence of k-groups

$$1 \to \mathbb{G}_a \to G \to \mathbb{G}_m \to 1.$$

(iv) Show that $H^1(k, G) = \{*\}$.
(v) Let A be a k-algebra such that $A_L \simeq L[X]$ as L-algebra, for some separable extension L/k. Show that $A \simeq k[X]$ as k-algebra.

We have thus proved that the k-algebra $k[X]$ admits no nontrivial twisted forms. We now give an example a nontrivial "inseparable twisted form" of $k[X]$, that is a k-algebra B such that $B \not\simeq k[X]$ and $B_K \simeq K[X]$ for some nonseparable extension K/k.

Let us assume that k has positive characteristic p, and that $a \in k$ is such that $a \neq b^p$ for all $b \in k$. We consider the k-algebra $B = k[U,V]/(U^p - aV^p - V)$.

(vi) Show that there exists an algebraic field extension K/k such that $B_K \simeq K[X]$ as K-algebra.

(vii) Show that B is not isomorphic to $k[X]$ as k-algebra.

(viii) For every prime p, give an example of a field k of characteristic p, together with an element $a \in k$ such that $a \neq b^p$ for all $b \in k$.

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 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-cocyles.

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. □

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 σ. Let $\alpha \in L$. Then $\mathrm{N}_{L/k}(\alpha) = 1$ if and only if $\alpha = (\sigma\beta)\beta^{-1}$ for some $\beta \in L$.*

PROOF. Let $n = [L : k]$. Recall that, by Proposition 5.5.14,

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

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

$$\xi\colon \operatorname{Gal}(L/k) \to L^\times \quad ; \quad \sigma^i \mapsto \alpha(\sigma\alpha)\cdots(\sigma^{i-1}\alpha)$$

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 μ_n the kernel of the morphism of k-groups $\mathbb{G}_m \to \mathbb{G}_m$ given by $x \mapsto x^n$. Thus μ_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*

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

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)

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

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

COROLLARY 7.1.6. *Assume that k contains a root of unity ω 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 $\operatorname{Gal}(k_s/k)$-groups $\mathbb{Z}/n \to \mu_n(k_s)$ 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 ω 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 isomorphisms 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,σ). 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_φ 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 ψ is another automorphism of (S_F,s_F,σ_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 Γ-group $\operatorname{Aut}(S,s,\sigma)(F)$ is isomorphic to $\mathbb{G}_a(F)$.

Let now (R,r,ρ) be a twisted forms of (S,s,σ) over k. Note that the elements r and ρ 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 $S\to R$ given by $s\mapsto r$ and $f\mapsto e$ is then an isomorphism of twisted forms $(S,s,\sigma)\to(R,r,\rho)$. We have proved that all twisted forms of (S,s,σ) are isomorphic. Therefore by Proposition 6.4.18 we have

$$H^1(\operatorname{Gal}(k_s/k),\operatorname{Aut}(S,s,\sigma)(k_s))=H^1(k,\mathbb{G}_a)=\{*\}.$$ □

Lemma 7.2.2. *If k has characteristic $p>0$, we have an exact sequence of k-groups*

$$1\to\mathbb{Z}/p\to\mathbb{G}_a\xrightarrow{\wp}\mathbb{G}_a\to 1,$$

where, for every separable field extension L/k,

$$\wp\colon L\to L\quad;\quad x\mapsto x^p-x.$$

Proof. Note that $\wp$ defines a morphism of k-groups, and that $\ker\wp\colon L\to L$ 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 $\wp\colon k_s\to k_s$ 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 $\wp(b)=a$. □

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-cocyle $\gamma \mapsto \gamma\alpha - \alpha$, where $\alpha \in k_s$ is any element such that $\alpha^p - \alpha = a$.

Every $\mathbb{Z}/p$-torsor is isomorphic to $\{x \in k_s | x^p - x = a\}$, 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)

$$1 \to \mathbb{Z}/p \to k \xrightarrow{\wp} k \xrightarrow{\delta} H^1(k, \mathbb{Z}/p) \to H^1(k, \mathbb{G}_a).$$

The group on the right is trivial by Proposition 7.2.1, so the required isomorphism is induced by δ. The remaining statements follow from the explicit descriptions of δ provided in Proposition 6.4.10. □

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 $\mathbf{X}(T_a) \simeq \{x \in k_s | x^p - x = a\}$, 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 $\{x \in k_s | x^p - x = a\}$. Thus the statement follows from Proposition 7.2.3. □

3. Tensor product and 1-cocyles

In this short section, we explain how the tensor product of central simple algebras can be expressed in terms of 1-cocycles.

Let $n \in \mathbb{N}$ and L/k be a separable extension. Recall that we have defined $\mathrm{PGL}_n(L) = \mathrm{Aut}_{L-\mathrm{alg}}(M_n(L))$. Since every automorphism of $M_n(L)$ is inner by Skolem–Noether's Theorem 2.3.3, and the center of $M_n(L)$ is L, we have an exact sequence of groups

(7.3.a) $$1 \to L^\times \to \mathrm{GL}_n(L) \to \mathrm{PGL}_n(L) \to 1,$$

where the map $\mathrm{GL}_n(L) \to \mathrm{PGL}_n(L)$ sends an invertible matrix A to the automorphism of $M_n(L)$ given by $M \mapsto AMA^{-1}$. This yields an exact sequence of k-groups

(7.3.b) $$1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1.$$

Let $m, n \in \mathbb{N} - 0$ and consider the k-vector spaces $V = k^n$ and $W = k^m$. For any separable extension L/k, we may define a group morphism

$$\mathrm{GL}(V)(L) \times \mathrm{GL}(W)(L) \to \mathrm{GL}(V \otimes_k W)(L) \quad ; \quad (\varphi, \psi) \mapsto \varphi \otimes \psi.$$

This yields a morphism of k-groups $\mathrm{GL}_m \times \mathrm{GL}_n \to \mathrm{GL}_{mn}$ fitting into a commutative diagram of k-groups, having exact rows

(7.3.c)
$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_m \times \mathbb{G}_m \arrow[r] \arrow[d] & \mathrm{GL}_m \times \mathrm{GL}_n \arrow[r] \arrow[d] & \mathrm{PGL}_m \times \mathrm{PGL}_n \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathrm{GL}_{mn} \arrow[r] & \mathrm{PGL}_{mn} \arrow[r] & 1
\end{tikzcd}$$

where the vertical map on the left is the group operation in $\mathbb{G}_m$.

Let us denote by $[A] \in H^1(k, \mathrm{PGL}_n)$ the class of a finite-dimensional central simple k-algebra of degree n.

PROPOSITION 7.3.1. *Let A, B be a finite-dimensional central simple k-algebras, and $m = \deg(A), n = \deg(B)$. Then $([A],[B])$ is mapped to $[A \otimes_k B]$ under the composite*

$$H^1(k, \mathrm{PGL}_m) \times H^1(k, \mathrm{PGL}_n) \to H^1(k, \mathrm{PGL}_m \times \mathrm{PGL}_n) \to H^1(k, \mathrm{PGL}_{mn}).$$

PROOF. We use the explicit description given at the end of Proposition 6.4.18: if $\varphi\colon M_m(k_s) \to A_{k_s}$ is any isomorphism of k_s-algebras, the class $[A] \in H^1(k, \mathrm{PGL}_m)$ is represented by the 1-cocyle

$$\alpha\colon \operatorname{Gal}(k_s/k) \to \operatorname{Aut}_{k_s-\mathrm{alg}}(M_m(k_s)) \quad ; \quad \gamma \mapsto \alpha_\gamma = \varphi^{-1} \circ \gamma \circ \varphi \circ \gamma^{-1}.$$

Similarly if $\psi\colon M_n(k_s) \to A_{k_s}$ is any isomorphism of k_s-algebras, the class $[B] \in H^1(k, \mathrm{PGL}_n)$ is represented by the 1-cocyle $\beta_\gamma = \psi^{-1} \circ \gamma \circ \psi \circ \gamma^{-1}$. The image of $([A],[B])$ in $H^1(k, \mathrm{PGL}_{mn})$ under the composite of the statement is thus represented by 1-cocyle $\alpha_\gamma \otimes \beta_\gamma$. Now, the isomorphisms φ and ψ induce an isomorphism of k_s-algebras

$$M_{mn}(k_s) = M_m(k_s) \otimes_{k_s} M_n(k_s) \xrightarrow{\varphi \otimes \psi} A_{k_s} \otimes_{k_s} B_{k_s} = (A \otimes_k B)_{k_s},$$

so that the $[A \otimes_k B] \in H^1(k, \mathrm{PGL}_{mn})$ is represented by the 1-cocycle $\pi_\gamma = (\varphi \otimes \psi)^{-1} \circ \gamma \circ (\varphi \otimes \psi) \circ \gamma^{-1}$. Since $\pi_\gamma = \alpha_\gamma \otimes \beta_\gamma$ for all $\gamma \in \operatorname{Gal}(k_s/k)$, the statement follows. □

4. Cyclic algebras

We are now in position to define and study higher-dimensional analogs of quaternion algebras, called cyclic algebras.

Let $n \in \mathbb{N} - 0$. When L is a Galois $\mathbb{Z}/n$-algebra over k, we will denote by $\rho\colon L \to L$ the action of $1 \in \mathbb{Z}/n$.

DEFINITION 7.4.1. Let L be a Galois $\mathbb{Z}/n$-algebra over k, and $a \in k^\times$. We define the k-algebra

$$(L, a) = \bigoplus_{i=0}^{n-1} L z^i$$

where the element z, that we call the *standard element*, is subject to the relations

$$z^n = a \quad \text{and} \quad zl = \rho(l) z \text{ for all } l \in L.$$

Algebras of the form (L, a) for L and a as above are called *cyclic algebras*.

Observe that $\dim_k(L, a) = n^2$, and that if K/k is a field extension we have $(L_K, a) \simeq (L, a)_K$.

LEMMA 7.4.2. *Let A be a k-algebra containing L as a subalgebra and $\alpha \in A$ such that*

$$\alpha^n = a \quad \text{and} \quad \alpha l = \rho(l) \alpha \text{ for all } l \in L.$$

Then there exists a unique morphism of k-algebras $(L, a) \to A$ mapping z to α, whose restriction on L is the inclusion $L \subset A$.

PROOF. This is clear from the definition of (L, a). □

The next statement asserts that the isomorphism class of the k-algebra (L, a) depends only on the class of a in $k^\times / k^{\times n}$:

LEMMA 7.4.3. *Let L be a Galois $\mathbb{Z}/n$-algebra over k and $a \in k^\times$. For any $b \in k^\times$, we have $(L,a) \simeq (L, ab^n)$ as k-algebras.*

PROOF. Let z, resp. y, be the standard element of (L,a), resp. (L,ab^n). In view of Lemma 7.4.2, we may define mutually inverse isomorphisms $(L,a) \simeq (L,ab^n)$ by $z \mapsto b^{-1}y$ and $y \mapsto bz$. □

For $a \in k^\times$, consider the matrix (blank entries are zero)

$$Z_a = \begin{pmatrix} 0 & \cdots & 0 & a \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix} \in M_n(k).$$

Using the notation diag for the diagonal matrices, observe that

$$(Z_a)^n = \mathrm{diag}(a, \dots, a) \tag{7.4.a}$$

and that, if $x_1, \dots, x_n \in k$, then

$$Z_a \cdot \mathrm{diag}(x_1, \dots, x_n) \cdot Z_a^{-1} = \mathrm{diag}(x_n, x_1, \dots, x_{n-1}). \tag{7.4.b}$$

PROPOSITION 7.4.4. *Let L be a Galois $\mathbb{Z}/n$-algebra over k and $a \in k^\times$.*

(i) The k-algebra (L,a) is central and simple.
(ii) If the Galois $\mathbb{Z}/n$-algebra L is split, then $(L,a) \simeq M_n(k)$.
(iii) If $a \in k^{\times n}$, then $(L,a) \simeq M_n(k)$.
(iv) Let $\Gamma = \mathrm{Gal}(k_s/k)$ and $\lambda \colon \Gamma \to \mathbb{Z}/n$ be a 1-cocyle whose class in $H^1(\Gamma, \mathbb{Z}/n)$ is the class of the Galois $\mathbb{Z}/n$-algebra L. Then the class of the finite-dimensional central simple k-algebra (L,a) in $H^1(\Gamma, \mathrm{PGL}_n(k_s))$ is given by the 1-cocycle $z_a \circ \lambda$, where $z_a \colon \mathbb{Z}/n \to \mathrm{PGL}_n(k_s)$ is the group morphism mapping $1 \in \mathbb{Z}/n$ to the automorphism of $M_n(k_s)$ given by $M \mapsto Z_a M Z_a^{-1}$.

PROOF. Consider the k-algebra $B = k^n$ with the $\mathbb{Z}/n$-action given by

$$\rho(x_1, \dots, x_n) = (x_n, x_1, \dots, x_{n-1}) \quad \text{for } x_1, \dots, x_n \in k.$$

Then B is a split Galois $\mathbb{Z}/n$-algebra. By Lemma 7.4.2, in view of (7.4.b) and (7.4.a) we may define a morphism of k-algebras $\varphi \colon (B,a) \to M_n(k)$ by

$$(x_1, \dots, x_n) \in L \mapsto \mathrm{diag}(x_1, \dots, x_n) \quad \text{and} \quad z \mapsto Z_a.$$

Let $j \in \{1, \dots, n\}$ and $u_j = (\delta_{1,j}, \dots, \delta_{n,j}) \in B$ (where $\delta_{i,j}$ is the Kronecker delta). For $i \in \{1, \dots, n\}$, we have

$$\varphi(u_j z^i) = \begin{cases} e_{j,j-i} & \text{if } j > i, \\ a e_{j,n+j-i} & \text{if } j \leq i, \end{cases}$$

where $e_{u,v}$ denotes the matrix in $M_n(k)$ whose only nonzero entry is in position (u,v) and has value 1. It follows that φ is surjective, hence bijective by dimensional reasons. We have proved that the k-algebra (B,a) is isomorphic to $M_n(k)$.

(ii): Since all split Galois $\mathbb{Z}/n$-algebras are isomorphic to one another, this follows from the above observation.

(i): This follows from (ii) by extending scalars to k_s (in view of Lemma 3.1.1).

(iii): Sending $l \in L$ to the endomorphism of L given by $x \mapsto lx$ induces a morphism of k-algebras $\tau \colon L \to \mathrm{End}_k(L)$. This morphism is injective, since $\tau(l)(1) = l$. We may thus view L as a subalgebra of $\operatorname{End}_k(L)$. We may apply Lemma 7.4.2 with $A = \operatorname{End}_k(L)$ and $\alpha = \rho$, since $\alpha^n = \rho^n = \mathrm{id}$, and for any $l \in L$

$$\alpha \circ \tau(l)(x) = \rho(lx) = \rho(l)\rho(x) = \tau(\rho(l)) \circ \alpha(x) \quad \text{for all } x \in L,$$

so that $\alpha \circ (\tau(l)) = \tau(\rho(l)) \circ \alpha$. We obtain a morphism of k-algebras $(L,1) \to \operatorname{End}_k(L)$, which is injective by simplicity of $(L,1)$ (obtained in (i)), and bijective by dimensional reasons. We conclude using Lemma 7.4.3, and choosing an isomorphism $\operatorname{End}_k(L) \simeq M_n(k)$ (corresponding to a k-basis of L).

(iv): Upon replacing L with an isomorphic Galois $\mathbb{Z}/n$-algebra, we may assume that $L_{k_s} = B_{k_s}$ as k_s-algebras, with the Γ-action given by twisting the action on B_{k_s} by the 1-cocyle λ. Consider the isomorphism of k_s-algebras

$$\phi\colon (B_{k_s}, a) = (B,a)_{k_s} \xrightarrow{\varphi_{k_s}} M_n(k_s).$$

Let $\gamma \in \Gamma$. Then γ acts trivially on $z \in (B,a) \subset (B,a)_{k_s}$ and on $\phi(z) = Z_a \in M_n(k) \subset M_n(k_s)$. Moreover $\xi_\gamma(M) = Z_a^{\lambda_\gamma} \cdot M \cdot Z_a^{-\lambda_\gamma}$ for every $M \in M_n(k_s)$. Therefore, twisting the Γ-action on $M_n(k_s)$ by the 1-cocyle $\xi = z_a \circ \lambda\colon \Gamma \to \mathrm{PGL}_n(k_s)$, we have

$$\gamma \star_\xi \phi(z) = Z_a^{\lambda_\gamma} \cdot (\gamma\phi(z)) \cdot Z_a^{-\lambda_\gamma} = Z_a^{\lambda_\gamma} \cdot Z_a \cdot Z_a^{-\lambda_\gamma} = Z_a = \phi(z) = \phi(\gamma z).$$

If $x = (x_1, \dots, x_n) \in B_{k_s} = (k_s)^n$, we have for any $\gamma \in \Gamma$

$$\gamma \star_\lambda x = \rho^{\lambda_\gamma}(\gamma x_1, \dots, \gamma x_n) = \rho^{\lambda_\gamma}(\gamma x).$$

We also have $\phi(\gamma x) = \gamma\phi(x)$, and, in view of (7.4.b)

$$\gamma \star_\xi \phi(x) = Z_a^{\lambda_\gamma} \cdot (\phi(\gamma x)) \cdot Z_a^{-\lambda_\gamma} = \phi(\rho^{\lambda_\gamma}(\gamma x)) = \phi(\gamma \star_\lambda x).$$

We have proved that the composite

$$(L,a)_{k_s} = (L_{k_s}, a) = (B_{k_s}, a) \xrightarrow{\phi} {}_\xi M_n(k_s)$$

is Γ-equivariant, hence induces an isomorphism of k-algebras $(L,a) \simeq ({}_\xi(M_n(k_s)))^\Gamma$, as required. $\square$

Remark 7.4.5. If $\omega \in k^\times$ is a root of unity of order n, then Galois $\mathbb{Z}/n$-algebras are classified by elements of $k^\times/k^{\times n}$ by Corollary 7.1.6, hence we may associate a cyclic algebra to each pair $(a,b) \in (k^\times/k^{\times n})^2$ (which depends on the choice of ω). When $n=2$ and k has characteristic different from two (thus $\omega = -1$), this is of course the quaternion algebra (a,b) of Definition 1.1.1. This suggests how to define quaternion algebras when k has characteristic two: in this case Artin–Schreier theory (Proposition 7.2.3) asserts that Galois $\mathbb{Z}/2$-algebras are classified by $k/\wp(k)$, so that one may associate a cyclic algebra of degree 2 to each pair in $(k/\wp(k)) \times (k^\times/k^{\times 2})$.

Proposition 7.4.6. *Let K be a Galois $\mathbb{Z}/m$-algebra over k, and $r \in \mathbb{N} - 0$. Set $n = rm$, and consider the Galois $\mathbb{Z}/n$-algebra $L = \operatorname{Ind}_{\mathbb{Z}/m}^{\mathbb{Z}/n}(K)$ over k (see Lemma 5.5.17). Then for any $a \in k^\times$*

$$(L,a) \simeq M_r(A) \quad \textit{where } A = (K,a).$$

Proof. Recall that L is the k-algebra of those maps $f\colon \mathbb{Z}/n \to K$ such that $f(i+r) = \tau(f(i))$, where $\tau\colon K \to K$ is the action of $1 \in \mathbb{Z}/m$. We define a morphism of k-algebras $L \to M_r(A)$ by sending a map $f \in L$ to the matrix $\operatorname{diag}(f(0), \dots, f(1-r))$. This morphism is visibly injective. Letting $z \in A = (K, a)$ be the standard element, we consider the matrix (blank entries are zero)

$$Z = \begin{pmatrix} 0 & \cdots & 0 & z \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix} \in M_r(A).$$

Then $Z^r = \operatorname{diag}(z, \ldots, z) \in M_r(A)$ coincides with $z \in A \subset M_r(A)$, hence $Z^n = Z^{rm} = a$. Now for $x_0, \ldots, x_{r-1} \in A$, we have

$$Z \cdot \operatorname{diag}(x_0, \ldots, x_{r-1}) = \operatorname{diag}(\tau(x_{r-1}), x_0, \ldots, x_{r-2}) \cdot Z.$$

The image of $f \in L$ under the action of $1 \in \mathbb{Z}/n$ is the map $g \in L$ given by $g(i) = f(i+1)$ for $i \in \mathbb{Z}/n$. Setting $x_i = f(-i)$ for $i = 0, \ldots, r-1$, and noting that $\tau(f(1-r)) = f(1) = g(0)$

$$Z \cdot \operatorname{diag}(f(0), \ldots, f(r-1)) = \operatorname{diag}(g(0), \ldots, g(1-r)) \cdot Z.$$

Therefore by Lemma 7.4.2 there exists a morphism of k-algebras $(L, a) \to M_r(A)$ sending the standard element to Z, and restricting to $f \mapsto \operatorname{diag}(f(0), \ldots, f(1-r))$ on L. This morphism is injective (as (L, a) is simple and $M_r(A)$ is nonzero), hence bijective by dimensional reasons. □

LEMMA 7.4.7. *Let $a, b \in k^\times$. Then there exists an invertible element $U \in M_n(k) \otimes_k M_n(k)$ such that*

$$Z_a \otimes Z_b = U^{-1}(Z_1 \otimes Z_{ab})U \in M_n(k) \otimes_k M_n(k).$$

PROOF. Let $e_1, \ldots, e_n$ be a k-basis of $V = k^n$. Letting U correspond to the endomorphism of $V \otimes_k V$ given by

$$e_i \otimes e_j \mapsto \begin{cases} e_i \otimes e_j & \text{if } i \geq j, \\ a^{-1} e_i \otimes e_j & \text{if } i < j, \end{cases}$$

one verifies that $Z_a \otimes Z_b$ and $U^{-1}(Z_1 \otimes Z_{ab})U$ both correspond to the endomorphism of $V \otimes_k V$ given by

$$e_i \otimes e_j \mapsto \begin{cases} e_{i+1} \otimes e_{j+1} & \text{if } i < n \text{ and } j < n, \\ a e_1 \otimes e_{j+1} & \text{if } j < i = n, \\ b e_{i+1} \otimes e_1 & \text{if } i < j = n, \\ ab e_1 \otimes e_1 & \text{if } i = j = n. \end{cases}$$ □

PROPOSITION 7.4.8. *Let L be a Galois $\mathbb{Z}/n$-algebra over k and $a, b \in k^\times$. Then*

$$(L, a) \otimes_k (L, b) \simeq M_n(k) \otimes_k (L, ab).$$

PROOF. As usual, we identify $M_n(k) \otimes_k M_n(k)$ with $M_{n^2}(k)$, which yields a group morphism

$$\mathrm{PGL}_n(k_s) \times \mathrm{PGL}_n(k_s) \to \mathrm{PGL}_{n^2}(k_s) \quad ; \quad (f, g) \mapsto f \otimes g.$$

Let $U \in M_{n^2}(k)$ be as in Lemma 7.4.7, and $u \in \mathrm{PGL}_{n^2}(k) \subset \mathrm{PGL}_{n^2}(k_s)$ be the automorphism given by $M \mapsto U^{-1}MU$. Then for every $M \in M_{n^2}(k)$ and $i \in \mathbb{Z}/n$,

$$(Z_1 \otimes Z_{ab})^i M (Z_1 \otimes Z_{ab})^{-i} = U(Z_a \otimes Z_b)^i U^{-1} M U (Z_a \otimes Z_b)^{-i} U^{-1}.$$

We now apply Proposition 7.4.4 and use its notation. The above formula implies that, for all $i \in \mathbb{Z}/n$, we have in $\mathrm{PGL}_{n^2}(k_s)$

$$(z_1 \otimes z_{ab})(i) = u^{-1} \cdot (z_a(i) \otimes z_b(i)) \cdot u. \tag{7.4.c}$$

Since U is defined over k, the automorphism u is Γ-invariant, so that (7.4.c) shows that the 1-cocyles $(z_a \otimes z_b) \circ \lambda$ and $(z_1 \otimes z_{ab}) \circ \lambda$ in $Z^1(\Gamma, \mathrm{PGL}_{n^2}(k_s))$ are cohomologous, hence represent isomorphic k-algebras. Since $(L,1) \simeq M_n(k)$ (Proposition 7.4.4 (iii)), the statement follows from Proposition 7.3.1. □

Remark 7.4.9. It follows from Proposition 7.4.8 and Proposition 7.4.4 (iii) that the finite-dimensional central simple algebra $(L,a)^{\otimes n}$ splits.

Lemma 7.4.10. *Let L be a Galois $\mathbb{Z}/n$-algebra and $a \in k^\times$. Assume that L is a field. Consider the cyclic algebra (L,a) and its standard element $z \in (L,a)$. Let $i \in \{0,\dots,n-1\}$. Any element $x \in (L,a)$ such that $\rho^i(l)x = xl$ for all $l \in L$ is of the form uz^i for some $u \in L$.*

Proof. Write $x = x_0 + x_1 z + \cdots + x_{n-1}z^{n-1}$ with $x_j \in L$ for all $j = 0,\dots,n-1$. The condition $\rho^i(l)x = xl$ implies that

$$\sum_{j=0}^{n-1} \rho^i(l)x_j z^j = \sum_{j=0}^{n-1} x_j z^j l = \sum_{j=0}^{n-1} x_j \rho^j(l) z^j = \sum_{j=0}^{n-1} \rho^j(l) x_j z^j,$$

so that $\rho^i(l)x_j = \rho^j(l)x_j$ for all $j = 0,\dots,n-1$. Let $j \in \{0,\dots,n-1\}$ be such that $x_j \neq 0$. Then $x_j \in L^\times$, and thus $\rho^i(l) = \rho^j(l)$ for all $l \in L$. Therefore $\rho^{i-j} = \mathrm{id}_L$, which implies that $i = j$ in view of Lemma 5.5.6. □

Proposition 7.4.11. *Let L be a Galois $\mathbb{Z}/n$-algebra over k and $a,b \in k^\times$. Then the k-algebras (L,a) and (L,b) are isomorphic if and only if $ab^{-1} \in \mathrm{N}_{L/k}(L^\times)$.*

Proof. By Proposition 5.5.18, Proposition 7.4.6 and Lemma 5.5.19 we may assume that L is a field (recall that Brauer-equivalent central simple k-algebras of the same finite dimension are isomorphic, by Wedderburn's Theorem 2.1.13). Let y and z be the respective standard elements of (L,a) and (L,b). For any $u \in L$, we have $(uz)^n = u\rho(u)\cdots\rho^{n-1}(u)z^n$, so that by Proposition 5.5.14

$$(uz)^n = b\,\mathrm{N}_{L/k}(u). \tag{7.4.d}$$

Now assume that $u \in L^\times$ is such that $a = b\,\mathrm{N}_{L/k}(u)$. Then $(uz)^n = a$ by (7.4.d), so that by Lemma 7.4.2 we may define a morphism of k-algebras $\varphi\colon (L,a) \to (L,b)$ satisfying $\varphi(y) = uz$ and $\varphi(l) = l$ for all $l \in L$. This morphism is injective by simplicity of (L,a), and an isomorphism by dimensional reasons.

Conversely, assume given an isomorphism of k-algebras $\varphi\colon (L,a) \to (L,b)$. The ring L is simple by Remark 2.1.6. Applying Skolem–Noether's Theorem 2.3.3 to the inclusion $L \subset (L,b)$ and the composite $L \subset (L,a) \xrightarrow{\varphi} (L,b)$ we obtain an element $v \in (L,b)$ such that $v\varphi(l)v^{-1} = l$ for all $l \in L$. Replacing φ by the isomorphism $x \mapsto v\varphi(x)v^{-1}$, we may assume that $\varphi(l) = l$ for all $l \in L$. Then for all $l \in L$

$$\varphi(y)l = \varphi(yl) = \varphi(\rho(l)y) = \rho(l)\varphi(y),$$

so that by Lemma 7.4.10 (with $i = 1$) we have $\varphi(y) = uz$ for some $u \in L$. Then, by (7.4.d),

$$a = \varphi(y^n) = \varphi(y)^n = (uz)^n = b\,\mathrm{N}_{L/k}(u). \qquad \square$$

PROPOSITION 7.4.12. *Let L be a Galois $\mathbb{Z}/n$-algebra over k and A a finite-dimensional central simple k-algebra of degree n containing L as a subalgebra. Assume that L is a field. Then there exists $a \in k^\times$ such that $A \simeq (L, a)$.*

PROOF. The ring L being simple (Remark 2.1.6), by Skolem–Noether's Theorem 2.3.3 applied the morphisms $L \subset A$ and $L \xrightarrow{\rho} L \subset A$, we find $\alpha \in A^\times$ such that $\alpha l \alpha^{-1} = \rho(l)$ for all $l \in L$. Let $a = \alpha^n$. Then $a \in \mathcal{Z}_A(L)$ (as $\rho^n = \mathrm{id}_L$). Since $L = \mathcal{Z}_A(L)$ by Lemma 3.2.4, it follows that $a \in L$. We have

$$\rho(a) = \alpha^{-1} a \alpha = \alpha^{-1} \alpha^n \alpha = \alpha^n = a,$$

hence $a \in L^{\mathbb{Z}/n} = k$. By Lemma 7.4.2, we may define a morphism of k-algebras $\varphi \colon (L, a) \to A$ satisfying $\varphi(z) = \alpha$ and $\varphi(l) = l$ for $l \in L$. This morphism is injective by simplicity of (L, a), and bijective by dimensional reasons. □

THEOREM 7.4.13. *Let L be a Galois $\mathbb{Z}/n$-algebra. Assume that L is a field. Then mapping $a \in k^\times$ to the cyclic algebra (L, a) yields a group isomorphism*

$$k^\times / \mathrm{N}_{L/k}(L^\times) \simeq \mathrm{Br}(L/k).$$

PROOF. Mapping a to (L, a) induces a group morphism $k^\times \to \mathrm{Br}(k)$ by Proposition 7.4.8. The image of this morphism is contained in $\mathrm{Br}(L/k)$ by Corollary 5.5.13 and Proposition 7.4.4 (ii). This morphism induces an injective morphism $k^\times / \mathrm{N}_{L/k}(L^\times) \to \mathrm{Br}(L/k)$ by Proposition 7.4.11. Its surjectivity is obtained by combining Proposition 3.2.2 with Proposition 7.4.12. □

COROLLARY 7.4.14. *If L/k is a finite Galois extension such that* $\mathrm{Gal}(L/k)$ *is cyclic, then*

$$\mathrm{Br}(L/k) \simeq k^\times / \mathrm{N}_{L/k}(L^\times).$$

PROOF. Choosing a generator of $\mathrm{Gal}(L/k)$ makes L a Galois $\mathbb{Z}/n$-algebra over k, where $n = [L : k]$ (Example 5.5.7), and we may apply Theorem 7.4.13. □

5. The reduced characteristic polynomial

When L is a field and n an integer, we denote by

$$\chi_L \colon M_n(L) \to L[X] \quad ; \quad M \mapsto \det(X I_n - M)$$

the map sending a matrix to its characteristic polynomial (where $I_n \in M_n(k)$ is the unit matrix). Observe that, for any field extension E/L the following diagram commutes

$$\begin{array}{ccc} M_n(L) & \xrightarrow{\chi_L} & L \\ \downarrow & & \downarrow \\ M_n(E) & \xrightarrow{\chi_E} & E \end{array} \tag{7.5.a}$$

DEFINITION 7.5.1. Let A be a k-algebra, and M an A-module of finite dimension over k. The *characteristic polynomial* of an element $a \in A$ is the polynomial

$$\mathrm{Cp}_{M/k}(a) = \det(X \,\mathrm{id}_M - l_a) \in k[X],$$

where $l_a \colon M \to M$ is the map given by $x \mapsto ax$ (viewed as a k-linear map).

Observe that if $f\colon M \to N$ is an isomorphism of A-modules, then $l_a = f \circ l_a \circ f^{-1}$ for any $a \in A$, so that

$$\mathrm{Cp}_{M/k}(a) = \mathrm{Cp}_{N/k}(a). \tag{7.5.b}$$

If M, N are A-modules of finite dimensions over k, then for any $a \in A$

$$\mathrm{Cp}_{M\oplus N/k}(a) = \mathrm{Cp}_{M/k}(a)\,\mathrm{Cp}_{N/k}(a). \tag{7.5.c}$$

Finally, if $\varphi\colon B \to A$ is a morphism of k-algebras, and M an A-module of finite dimension over k, we may view M as a B-module using φ, and we have $l_b = l_{\varphi(b)}$ for any $b \in B$, so that

$$\mathrm{Cp}_{M/k}(b) = \mathrm{Cp}_{M/k}(\varphi(b)). \tag{7.5.d}$$

LEMMA 7.5.2. *For any $M \in M_n(k)$, we have $\chi_k(M)^n = \mathrm{Cp}_{M_n(k)/k}(M)$.*

PROOF. For $1 \leq i,j \leq n$, let us set $x_{i+(n-1)j} = e_{i,j} \in M_n(k)$ (the matrix whose only nonzero entry is 1, in the position (i,j)). The elements $x_1, \dots, x_{n^2}$ form a k-basis of $M_n(k)$. If $M \in M_n(k)$ has coefficients $m_{i,j} \in k$, we have

$$Mx_{k+(n-1)l} = Me_{k,l} = \sum_{i,j=1}^{n} m_{i,j}e_{i,j}e_{k,l} = \sum_{i=1}^{n} m_{i,k}e_{i,l} = \sum_{i=1}^{n} m_{i,k}x_{i+(n-1)l},$$

showing that, in the basis $x_1, \dots, x_{n^2}$, the matrix of the map $M_n(k) \to M_n(k)$ given by $x \mapsto Mx$ is

$$\begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & M \end{pmatrix}.$$

Its characteristic polynomial is $\chi_k(M)^n$. $\square$

LEMMA 7.5.3. *Let A be a finite-dimensional simple k-algebra. If $f, g\colon A \to M_n(k)$ are morphisms of k-algebras, then $\chi_k \circ f = \chi_k \circ g\colon A \to k[X]$.*

PROOF. By Skolem–Noether's Theorem 2.3.3 there exists $b \in M_n(k)$ such that $f(a) = b^{-1}g(a)b$ for all $a \in A$, so that the matrices $f(a)$ and $g(a)$ have the same characteristic polynomial. $\square$

LEMMA 7.5.4. *Let A be a finite-dimensional central simple k-algebra, and F/k a Galois extension. Let $f\colon A_F \to M_n(F)$ be a morphism of F-algebras. Then the composite*

$$A \to A_F \xrightarrow{f} M_n(F) \xrightarrow{\chi_F} F[X]$$

has image contained in $k[X]$.

PROOF. Let $\Gamma = \mathrm{Gal}(F/k)$. In view of the diagram (7.5.a) when $E = L$ and $\gamma \in \Gamma$, the map $\chi_F\colon M_n(F) \to F$ is Γ-equivariant. If $\gamma \in \Gamma$, the map $g\colon A_F \to M_n(F)$ given by $x \mapsto \gamma^{-1}f(\gamma x)$ is a morphism of F-algebras, hence by Lemma 7.5.3 we have for any $x \in A_F$,

$$\chi_F \circ f(x) = \chi_F \circ g(x) = \chi_F(\gamma^{-1}f(\gamma x)) = \gamma^{-1}(\chi_F \circ f(\gamma x)).$$

Thus the morphism $\chi_F \circ f$ is Γ-equivariant, hence maps $A = (A_F)^\Gamma$ to $k[X] = (F[X])^\Gamma$ (see Lemma 4.4.3). $\square$

Let now A be a finite-dimensional central simple k-algebra of degree n. Choose a Galois extension F/k and a morphism of F-algebras $f\colon A_F \to M_n(F)$ (this is possible, since $A_{k_s} \simeq M_n(k_s)$). Let $a \in A$. The polynomial $\chi_F \circ f(a \otimes 1) \in F[X]$ belongs to $k[X]$ by Lemma 7.5.4. Let now F'/k be a Galois extension and $f'\colon A_{F'} \to M_n(F')$ a morphism of F'-algebras. Let E be a separable closure of F'. Then F can be embedded into E by Lemma 4.3.12, and using Lemma 7.5.3 and the commutativity of the diagram (7.5.a), we have in $k[X] \subset E[X]$

$$\chi_F \circ f(a \otimes 1) = \chi_E \circ f_E(a \otimes 1) = \chi_E \circ f'_E(a \otimes 1) = \chi_{F'} \circ f'(a \otimes 1).$$

This proves that the map

$$A \to k[X] \quad ; \quad a \mapsto \chi_F \circ f(a \otimes 1) \tag{7.5.e}$$

does not depend on the choices of the Galois extension F/k and the morphism $f\colon A_F \to M_n(F)$.

DEFINITION 7.5.5. The map (7.5.e) is called the *reduced characteristic polynomial* and denoted by

$$\mathrm{Cprd}_A\colon A \to k[X].$$

Writing this map as $a_nX^n + \cdots + a_0$ where $a_0, \ldots, a_n$ are maps $A \to k$ and $n = \deg(A)$, we define the *reduced norm* and *reduced trace* as

$$\mathrm{Nrd}_A = (-1)^n a_0 \quad \text{and} \quad \mathrm{Trd}_A = -a_{n-1}.$$

By construction, when $A = M_n(k)$, the reduced characteristic polynomial (resp. reduced trace, reduced norm) coincides with the characteristic polynomial (resp. trace, norm) of matrices.

If L/k is a separable field extension, it also follows from the construction that the following diagram commutes

$$\begin{tikzcd} A \arrow[r, "\mathrm{Cprd}_A"] \arrow[d] & k[X] \arrow[d] \\ A_L \arrow[r, "\mathrm{Cprd}_{A_L}"] & L[X] \end{tikzcd} \tag{7.5.f}$$

PROPOSITION 7.5.6. *Let A be a finite-dimensional central simple k-algebra of degree n.*

(i) For any $a \in A$, we have $\mathrm{Cp}_{A/k}(a) = \mathrm{Cprd}_A(a)^n$. In particular

$$\mathrm{N}_{A/k}(a) = \mathrm{Nrd}_A(a)^n \quad \textit{and} \quad \mathrm{Tr}_{A/k}(a) = n\,\mathrm{Trd}_A(a).$$

(ii) Let L be a subalgebra of A, and assume that L is a field. Then $n = r[L : k]$ for some integer r, and for any $l \in L$ we have $\mathrm{Cprd}_A(l) = \mathrm{Cp}_{L/k}(l)^r$. In particular

$$\mathrm{Nrd}_A(l) = \mathrm{N}_{L/k}(l)^r \quad \textit{and} \quad \mathrm{Trd}_A(l) = r\,\mathrm{Tr}_{L/k}(l).$$

PROOF. (i) : Let $f\colon A_F \to M_n(F)$ be an isomorphism of F-algebras, where F/k is a Galois extension. Then $\mathrm{Cp}_{A/k}(a) \in k[X]$ maps to $\mathrm{Cp}_{A_F/F}(a \otimes 1) \in F[X]$. By (7.5.b), (7.5.d) and Lemma 7.5.2, we have in $k[X] \subset F[X]$

$$\mathrm{Cp}_{A_F/F}(a \otimes 1) = \mathrm{Cp}_{M_n(F)/F} \circ f(a \otimes 1) = (\chi_F \circ f(a \otimes 1))^n = \mathrm{Cprd}(a)^n.$$

(ii) : The first statement follows from Lemma 3.2.4. Let $d = [L : k]$. Since $n^2 = \dim_k A = d{\cdot}\dim_L A$, we have $\dim_L A = r^2 d = nr$. Thus the L-vector space A is isomorphic to $L^{\oplus nr}$, and it follows from (7.5.b), (7.5.c) and (7.5.d) that $\mathrm{Cp}_{A/k}(l) = \mathrm{Cp}_{L/k}(l)^{nr}$. By (i), we deduce that $\mathrm{Cprd}_A(l)^n = \mathrm{Cp}_{L/k}(l)^{nr}$. We conclude using Lemma 7.5.7 below. ☐

LEMMA 7.5.7. *Let $P, Q \in k[X]$ be monic polynomials, and $s \in \mathbb{N} - \{0\}$ such that $P^s = Q^s$. Then $P = Q$.*

PROOF. Let $\mathcal{R}$ be the set of monic irreducible polynomials in $k[X]$. Since $k[X]$ is factorial, there are uniquely determined integers p_R, q_R for each $R \in \mathcal{R}$ such that

$$P = \prod_{R\in\mathcal{R}} R^{p_R} \quad ; \quad Q = \prod_{R\in\mathcal{R}} R^{q_R}.$$

For each $R \in \mathcal{R}$, we have $sp_R = sq_R$, hence $p_R = q_R$, and $P = Q$. ☐

We will be mostly interested in the reduced norm. Let us first collect some of its elementary properties.

LEMMA 7.5.8. *Let A be a finite-dimensional central simple k-algebra.*

(i) For any $a, b \in A$, we have $\mathrm{Nrd}_A(ab) = \mathrm{Nrd}_A(a)\,\mathrm{Nrd}_A(b)$.
(ii) We have $\mathrm{Nrd}_A(1) = 1$.

PROOF. Extending scalars, we may assume that $A \simeq M_n(k)$. Since the map $\mathrm{Nrd}_{M_n(k)}$ sends a matrix to its determinant, the lemma follows from the properties of the determinant. ☐

PROPOSITION 7.5.9. *Let A be a finite-dimensional central simple k-algebra, and $a \in A$. Then $a \in A^\times$ if and only if* $\mathrm{Nrd}_A(a) \neq 0$.

PROOF. If $a \in A^\times$, then $\mathrm{Nrd}_A(a)$ must be nonzero by Lemma 7.5.8. Conversely assume that $\mathrm{Nrd}_A(a) \neq 0$. Then $\mathrm{N}_{A/k}(a) \neq 0$ by Proposition 7.5.6 (i), hence left multiplication by a is an isomorphism $A \to A$. In particular 1 lies in its image, showing that a admits a right inverse, which is also a left inverse by Remark 1.1.11. ☐

Let A be a finite-dimensional central simple k-algebra. Recall from Example 6.3.2 that the k-group $\mathrm{GL}_1(A)$ is defined by setting $\mathrm{GL}_1(A)(L) = (A_L)^\times$ for every separable field extension L/k. The reduced norms induce group morphisms $\mathrm{Nrd}_{A_L} \colon (A_L)^\times \to L^\times$ by Lemma 7.5.8, and thus, by the commutativity of the diagram (7.5.f), a morphism of k-groups

$$\mathrm{Nrd}_A \colon \mathrm{GL}_1(A) \to \mathbb{G}_m.$$

DEFINITION 7.5.10. We define the k-group $\mathrm{SL}_1(A)$ as the kernel of the morphism $\mathrm{Nrd}_A \colon \mathrm{GL}_1(A) \to \mathbb{G}_m$.

LEMMA 7.5.11. *We have an exact sequence of k-groups*

$$1 \to \mathrm{SL}_1(A) \to \mathrm{GL}_1(A) \xrightarrow{\mathrm{Nrd}_A} \mathbb{G}_m \to 1.$$

PROOF. There exists an isomorphism of k_s-algebras $M_n(k_s) \simeq A_{k_s}$ for some n. The composite $\mathrm{GL}_n(k_s) \simeq (A_{k_s})^\times \xrightarrow{\mathrm{Nrd}_{A_{k_s}}} k_s^\times$ sends a matrix to its determinant, and is therefore surjective. ☐

PROPOSITION 7.5.12. *Let A be a finite-dimensional central simple k-algebra. Then*

$$H^1(k, \mathrm{GL}_1(A)) = \{*\}.$$

Proof. If M is an A-module such that the A_{k_s}-module M_{k_s} is isomorphic to A_{k_s}, then $\dim_k M = \dim_k A$, so that the A-module M is isomorphic to A by Lemma 2.3.1. Therefore all twisted forms of the A-module A are isomorphic, and the statement follows from Proposition 6.4.18 □

Corollary 7.5.13. *Let A be a finite-dimensional central simple k-algebra. There is a natural isomorphism of pointed sets*

$$H^1(k, \mathrm{SL}_1(A)) \simeq k^\times / \mathrm{Nrd}_A(A^\times).$$

Proof. In view of the sequence of Lemma 7.5.11, this follows by combining Proposition 7.5.12 with Corollary 6.4.11. □

Lemma 7.5.14. *The subset $\mathrm{Nrd}_A(A^\times) \subset k^\times$ depends only on the Brauer-equivalence class of the finite-dimensional central simple k-algebra A.*

Proof. When R is a ring and r an integer, a matrix $P \in M_r(R)$ is called *permutation* if there exists a permutation $\sigma \in \mathfrak{S}_r$ such that the (i,j)-th coefficient of P is equal to 1 if $j = \sigma(i)$ and zero otherwise. Such σ is then unique, and we define the *signature* ε of P in $\{-1, 1\}$ as the signature of the permutation σ. If R is a field, then $\det(P) = \varepsilon$.

In order to prove the statement, by Wedderburn's Theorem 2.1.13, we may assume that $A = M_n(D)$ for some finite-dimensional central simple division k-algebra D and integer n. It will suffice to prove that $\mathrm{Nrd}_D(D^\times) = \mathrm{Nrd}_A(A^\times)$. The same proof as over fields shows that every matrix in $M_n(D) = A$ can be made upper triangular by elementary rows operations. Any invertible upper triangular matrix can then be made diagonal by elementary rows operations. This implies that the group $A^\times$ is generated by elementary matrices (those matrices whose diagonal coefficients are equal to 1, and having a unique nonzero coefficient off the diagonal), diagonal matrices, and permutation matrices.

Let now F/k be a Galois extension and $\varphi\colon D_F \to M_d(F)$ and isomorphism of F-algebras. Consider the isomorphism of F-algebras $f\colon M_n(M_d(F)) \to M_{nd}(F)$ given by viewing a matrix with coefficients in $M_d(F)$ as a block matrix with coefficients in F. If $B_1, \ldots, B_n \in M_d(F)$, then $\det(f(\mathrm{diag}(B_1, \ldots, B_n)) = \det(B_1) \cdots \det(B_n)$. If $E \in M_n(M_d(F))$ is an elementary matrix, then $f(E)$ is an upper or lower triangular matrix whose diagonal coefficients are equal to 1, so that $\det(f(E)) = 1$. If $P \in M_n(M_d(F))$ is a permutation matrix with signature $\varepsilon \in \{-1, 1\}$, then $f(P) \in M_{dn}(F)$ is a permutation matrix with signature ε^d, so that $\det(f(P)) = \varepsilon^d = \det(\varepsilon I_d)$ (where $I_d = 1 \in M_d(F)$ is the unit matrix). We deduce that the composite

$$A^\times = M_n(D)^\times \subset M_n(D_F) \xrightarrow{M_n(\varphi)} M_n(M_d(F)) \xrightarrow{f} M_{nd}(F) \xrightarrow{\det} F$$

(being multiplicative) has the same image as the composite

$$D^\times \subset D_F \xrightarrow{\varphi} M_d(F) \xrightarrow{\det} F$$

(observe that $\varepsilon I_d \in M_d(F)$ is the image of $\varepsilon \in k^\times \subset D^\times$ under φ), as required. □

Proposition 7.5.15. *Let A be a finite-dimensional central simple k-algebra. Then*

$$\mathrm{Nrd}_A(A^\times) = \bigcup_L \mathrm{N}_{L/k}(L^\times) \subset k^\times$$

where L/k runs over the extensions of finite degree splitting A.

PROOF. $\subset$: By Lemma 7.5.14, we may assume that A is division. Let $a \in A$. Then any $a \in A$ is contained in some maximal subfield L of A, and $\mathrm{Nrd}_A(a) = \mathrm{N}_{L/k}(a)$ by Proposition 7.5.6 (ii).

$\supset$: Let L/k be a splitting field of A. By Proposition 3.2.2 and Lemma 7.5.14, we may assume that $L \subset A$ and that $\deg(A) = [L : k]$. It then follows from Proposition 7.5.6 (ii) that $\mathrm{N}_{L/k}(L^\times) \subset \mathrm{Nrd}_A(A^\times)$ in $k^\times$. $\square$

Exercises

Exercise 7.1. We have seen in Corollary 1.2.6 that central simple k-algebra of degree 2 are cyclic (in fact quaternion algebras) when k has characteristic $\neq 2$. In this exercise, we consider the case when the characteristic of k is arbitrary.

(i) Let D be a finite-dimensional central division k-algebra of degree 2. Show that D contains a Galois $\mathbb{Z}/2$-algebra as a k-subalgebra, and deduce that D is cyclic.
(ii) Conclude that every finite-dimensional central simple k-algebra of degree 2 is cyclic.

Exercise 7.2. Let A be a finite-dimensional central simple k-algebra.

(i) Show that the map
$$\nu\colon A \times A \to k \quad ; \quad (a,b) \mapsto \operatorname{Trd}_A(ab)$$
is a symmetric k-bilinear form.
(ii) Show that the form ν is nondegenerate, i.e. that the set
$$\{a \in A | \operatorname{Trd}_A(ax) = 0 \text{ for all } x \in A\}$$
is reduced to $\{0\}$.

Exercise 7.3. Let A be a finite-dimensional central simple k-algebra of degree n. Let $x \in A$ and $P = \operatorname{Cprd}_A(x) \in k[X]$ its reduced characteristic polynomial.

(i) Show that $P(x) = 0 \in A$.
(ii) Assume that $x \in A^\times$, and let $Q = \operatorname{Cprd}_A(x^{-1}) \in k[X]$. Show that
$$P(X) = (-X)^n \cdot \operatorname{Nrd}_A(x) \cdot Q(X^{-1}) \in k[X] \subset k[X, X^{-1}].$$

Exercise 7.4. Let D be a finite-dimensional central division k-algebra of degree 3. When $E \subset D$ is a subset, we write
$$E^\perp = \{x \in D | \operatorname{Trd}_D(ex) = 0 \text{ for all } e \in E\}.$$

(i) If $V \subset D$ is a k-subspace, show that $\dim_k V^\perp = 9 - \dim_k V$. (Hint: Use Exercise 7.3.)
(ii) Let K be a commutative k-subalgebra of D. Show that $K = k$ or that K/k is a field extension of degree 3.
(iii) Let $x \in D^\times$ be such that $\operatorname{Trd}_D(x) = \operatorname{Trd}_D(x^{-1}) = 0$. Show that $x^3 = \operatorname{Nrd}_D(x) \in k \subset D$. (Hint: Use Exercise 7.3.)
(iv) Let $E \subset D$ be a maximal subfield. Find $z \in D - k$ such that $\operatorname{Trd}_D(z) = \operatorname{Trd}_D(z^{-1}) = 0$. (Hint: Pick a nonzero element $u_1 \in E^\perp$, and find $u_2 \in \{u_1^{-1}\}^\perp \cap E$ such that $u_2 \notin u_1 k$. Set $z = u_1 u_2^{-1}$.)
(v) Let F be the k-subalgebra of D generated by z. Find $y \in D - F$ such that
$$\operatorname{Trd}_D(yz) = \operatorname{Trd}_D(yz^2) = \operatorname{Trd}_D(z^{-1}y^{-1}) = \operatorname{Trd}_D(z^{-2}y^{-1}) = 0.$$
(Hint: Pick $v_1 \in F^\perp - F$. Let $V = \{z^{-1}, z^{-2}\}^\perp$, and find a nonzero $v_2 \in (v_1 V) \cap F$. Set $y = v_2^{-1} v_1$.)
(vi) Let L be the k-subalgebra of D generated by y. Show that zyz^{-1} commutes with y and deduce that $zyz^{-1} \in L$. (Hint: Show that $\operatorname{Nrd}_D(yz^2)\operatorname{Nrd}_D(z^{-1}) = \operatorname{Nrd}_D(yz)$, and expand using (iii).)
(vii) Show that $y \mapsto zyz^{-1}$ defines a structure of Galois $\mathbb{Z}/3$-algebra on L.
(viii) Deduce that D is cyclic.

(ix) Conclude that every finite-dimensional central simple k-algebra of degree 3 is cyclic (this is a theorem of Wedderburn[1]).

Exercise 7.5. Let $n \geq 1$ be an integer, and $\omega \in k$ a root of unity of order n. Let $a, b \in k^\times$. Consider the Galois $\mathbb{Z}/n$-algebra $R_a = k[X]/(X^n - a)$, where $i \in \mathbb{Z}/n$ acts by $X \mapsto \omega^i X$. Up to isomorphism R_a depends only on the class of a in $k^\times/k^{\times n}$ (and on n and the choice of ω). Let us denote the cyclic algebra (R_a, b) by $(a, b)_\omega$.

(i) Show that $(a, b)_\omega \simeq ((b, a)_\omega)^{\mathrm{op}}$.
(ii) If $a \neq 1$, show that $(1 - a, a)_\omega \simeq M_n(k)$.

We define the extension $K = k(\sqrt[n]{a})$ as the splitting field of the polynomial $X^n - a \in k[X]$.

(iii) Show that the extension K/k is Galois, that $\mathrm{Gal}(L/k) \simeq \mathbb{Z}/m$ for some m dividing n, and that $R_a = \mathrm{Ind}_{\mathbb{Z}/m}^{\mathbb{Z}/n}(K)$ under that isomorphism.
(iv) Prove the "reciprocity law":

$$a \in \mathrm{N}_{k(\sqrt[n]{b})/k}(k(\sqrt[n]{b})) \iff b \in \mathrm{N}_{k(\sqrt[n]{a})/k}(k(\sqrt[n]{a})).$$

[1] on the other hand, one may construct central simple algebras of degree 4 (over an appropriate field) which are not cyclic.

Part 3

Cohomology

CHAPTER 8

The Brauer group and 2-cocycles

In this chapter, we define the second cohomology group of a commutative discrete group equipped with a continuous action of a profinite group, using a concrete approach in terms of cocycles. A more sophisticated approach will be developed in the next chapter, but this will not make this chapter obsolete. In fact, it is crucial to use this down-to-earth approach in order to make the connections with first cohomology sets of noncommutative groups, that is, with torsors.

We have seen that central simple algebras of degree n may be described using the first cohomology set of PGL_n. We will obtain an alternative description of the Brauer group, as the second cohomology group of $\mathbb{G}_m$. It is in fact a recurring situation that objects can be described either as low-degree cohomology of a complicated group, or as higher-degree cohomology of a simpler group. This new description of the Brauer group has several advantages; in particular this is a group on the nose, and the classes of algebras of different degrees live in the same cohomology set.

In this chapter we only prove that the Brauer group can be embedded into the second cohomology group of $\mathbb{G}_m$. This fact still has substantial consequences that can be expressed in an elementary fashion involving central simple algebras, but are difficult to prove without cohomology. In particular we show that the class of every central simple algebra is torsion in the Brauer group, and that its order (called the period of the algebra) divides its index. We deduce a primary decomposition theorem for division algebras, due to Brauer.

It is actually not very difficult to finish the identification Brauer group with the second cohomology group of $\mathbb{G}_m$, using the methods of this chapter via the so-called crossed-product construction. We prefer to leave this result to the next chapters, where more sophisticated methods will allow us to give a somewhat more natural proof.

1. 2-cocyles

We fix a profinite group Γ. We will still use the multiplicative notation for the group laws of discrete Γ-modules, even though they is commutative.

Definition 8.1.1. Let M be a discrete Γ-module. A 2-cocyle of Γ with values in M is a continuous map $\alpha\colon \Gamma\times\Gamma\to M$ (for the discrete topology on M) that we denote by $(\sigma,\tau)\mapsto \alpha_{\sigma,\tau}$, and such that

$$(\gamma\alpha_{\sigma,\tau})\cdot\alpha_{\gamma,\sigma\tau} = \alpha_{\gamma\sigma,\tau}\cdot\alpha_{\gamma,\sigma} \quad \text{for all } \gamma,\sigma,\tau\in\Gamma. \tag{8.1.a}$$

We denote the set of 2-cocyles of Γ with values in M by $Z^2(\Gamma,M)$. It is naturally an abelian group, for the operation defined by setting, for $\xi,\eta\in Z^2(\Gamma,M)$

$$(\xi\cdot\eta)_{\sigma,\tau} = \xi_{\sigma,\tau}\cdot\eta_{\sigma,\tau} \quad \text{for all } \sigma,\tau\in\Gamma.$$

A continuous map $\beta\colon \Gamma\times\Gamma\to M$, denoted by $(\sigma,\tau)\mapsto\beta_{\sigma,\tau}$, is called a 2-*coboundary* if there exists a continuous map $a\colon\Gamma\to M$, denoted by $\sigma\mapsto a_\sigma$, such that

$$\beta_{\sigma,\tau}=a_\sigma\cdot(\sigma a_\tau)\cdot a_{\sigma\tau}^{-1}\quad\text{for all }\sigma,\tau\in\Gamma.$$

A straightforward computation shows that a 2-coboundary is automatically a 2-cocyle, and the set of 2-coboundaries, denoted by $B^2(\Gamma,M)$, is a subgroup of $Z^2(\Gamma,M)$. We define

$$H^2(\Gamma,M)=Z^2(\Gamma,M)/B^2(\Gamma,M).$$

Two 2-cocyles in $Z^2(\Gamma,M)$ are called *cohomologous* if they have the same class in $H^2(\Gamma,M)$.

Composing 2-cocycles with a morphism of discrete Γ-modules $f\colon A\to B$ yields a group morphism

$$f_*\colon H^2(\Gamma,A)\to H^2(\Gamma,B).$$

PROPOSITION 8.1.2. *Let B be a discrete Γ-group and $A\subset B$ a discrete Γ-subgroup such that $a\cdot b=b\cdot a$ for all $a\in A$ and $b\in B$. Then the quotient $C=B/A$ is a discrete Γ-group, and there is an exact sequence of pointed sets*

$$\{*\}\to A^\Gamma\to B^\Gamma\to C^\Gamma\xrightarrow{\delta}H^1(\Gamma,A)\to H^1(\Gamma,B)\to H^1(\Gamma,C)\xrightarrow{\delta^2}H^2(\Gamma,A).$$

If $x\in H^1(\Gamma,C)$ is represented by a 1-cocyle $\xi\colon\Gamma\to C$, then $\delta^2(x)\in H^2(\Gamma,A)$ is represented by the 2-cocycle $\alpha\colon\Gamma\times\Gamma\to A$ defined by setting

$$\alpha_{\sigma,\tau}=\beta_\sigma\cdot(\sigma\beta_\tau)\cdot\beta_{\sigma\tau}^{-1}\quad\textit{for }\sigma,\tau\in\Gamma,$$

where $\beta\colon\Gamma\to B$ is any continuous map such that $\beta_\gamma\in B$ maps to $\xi_\gamma\in C$ for all $\gamma\in\Gamma$.

PROOF. First note that such a continuous map β exists. Indeed choosing a preimage $s(c)\in B$ of each $c\in C$ defines a map $s\colon C\to B$, which is continuous because C has the discrete topology, and we may take $\beta=s\circ\xi$.

Next observe that $\alpha_{\sigma,\tau}$ belongs to $A\subset B$, because its image in C is $\xi_\sigma\cdot(\sigma\xi_\tau)\cdot\xi_{\sigma\tau}^{-1}=1$, as ξ is a 1-cocyle. The continuity of α follows from Lemma 4.2.14, for if β factors as $\Gamma/U\to B^U$ for some open normal subgroup U of Γ, then α factors as $(\Gamma/U)\times(\Gamma/U)\to B^U$. Now, for $\gamma,\sigma,\tau\in\Gamma$, we have in $A\subset B$

$$\begin{aligned}(\gamma\alpha_{\sigma,\tau})\cdot\alpha_{\gamma,\sigma\tau}&=(\gamma\alpha_{\sigma,\tau})\cdot\beta_\gamma\cdot(\gamma\beta_{\sigma\tau})\cdot\beta_{\gamma\sigma\tau}^{-1}\\&=\beta_\gamma\cdot(\gamma\alpha_{\sigma,\tau})\cdot(\gamma\beta_{\sigma\tau})\cdot\beta_{\gamma\sigma\tau}^{-1}\\&=\beta_\gamma\cdot(\gamma\beta_\sigma)\cdot(\gamma\sigma\beta_\tau)\cdot(\gamma\beta_{\sigma\tau}^{-1})\cdot(\gamma\beta_{\sigma\tau})\cdot\beta_{\gamma\sigma\tau}^{-1}\\&=\beta_\gamma\cdot(\gamma\beta_\sigma)\cdot(\gamma\sigma\beta_\tau)\cdot\beta_{\gamma\sigma\tau}^{-1}\\&=\beta_\gamma\cdot(\gamma\beta_\sigma)\cdot\beta_{\gamma\sigma}^{-1}\cdot\beta_{\gamma\sigma}\cdot(\gamma\sigma\beta_\tau)\cdot\beta_{\gamma\sigma\tau}^{-1}\\&=\alpha_{\gamma,\sigma}\cdot\alpha_{\gamma\sigma,\tau},\end{aligned}$$

proving that α belongs to $Z^2(\Gamma,A)$. The image of α in $Z^2(\Gamma,B)$ is visibly a 2-coboundary.

If $\beta'\colon\Gamma\to B$ is another map lifting ξ, then for each $\gamma\in\Gamma$ we have $\beta'_\gamma=a_\gamma\cdot\beta_\gamma$, where $a_\gamma\in A$. Thus, for $\sigma,\tau\in\Gamma$, we have in A

$$\alpha'_{\sigma,\tau}=\beta'_\sigma\cdot(\sigma\beta'_\tau)\cdot\beta'^{-1}_{\sigma\tau}=a_\sigma\cdot(\sigma a_\tau)\cdot a_{\sigma\tau}^{-1}\cdot\beta_\sigma\cdot(\sigma\beta_\tau)\cdot\beta_{\sigma\tau}^{-1}=a_\sigma\cdot(\sigma a_\tau)\cdot a_{\sigma\tau}^{-1}\cdot\alpha_{\sigma,\tau},$$

proving that α' and α are cohomologous. We have proved that the class of α in $H^2(\Gamma,A)$ does not depend on the choice of the map β.

Now assume that $\xi'\colon \Gamma \to C$ is cohomologous to ξ. Then there is $c \in C$ such that

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

Let $b \in B$ be a preimage of C. Then the map $\beta'\colon \Gamma \to B$ defined by setting $\beta'_\gamma = b^{-1} \cdot \beta_\gamma \cdot (\gamma b)$ for all $\gamma \in \Gamma$ is a lifting of ξ', and for $\sigma, \tau \in \Gamma$, we have in A

$$\begin{aligned}\beta'_\sigma \cdot (\sigma\beta'_\tau) \cdot \beta'^{-1}_{\sigma\tau} &= b^{-1} \cdot \beta_\sigma \cdot (\sigma b) \cdot (\sigma b^{-1}) \cdot (\sigma\beta_\tau) \cdot (\sigma\tau b) \cdot (b^{-1} \cdot \beta_{\sigma\tau} \cdot (\sigma\tau b))^{-1} \\ &= b^{-1} \cdot \beta_\sigma \cdot (\sigma\beta_\tau) \cdot \beta^{-1}_{\sigma\tau} \cdot b \\ &= b^{-1} \cdot \alpha_{\sigma,\tau} \cdot b = \alpha_{\sigma,\tau},\end{aligned}$$

as $\alpha_{\sigma,\tau}$ is central in B. We have proved that the class of α in $H^2(\Gamma, A)$ depends only on the class of ξ in $H^1(\Gamma, C)$.

Assume that α is a 2-coboundary. Then there exists a continuous map $a\colon \Gamma \to A$ such that, for all $\sigma, \tau \in \Gamma$,

$$\beta_\sigma \cdot (\sigma\beta_\tau) \cdot \beta^{-1}_{\sigma\tau} = a_\sigma \cdot (\sigma a_\tau) \cdot a^{-1}_{\sigma\tau}.$$

Setting $\zeta_\gamma = \beta_\gamma \cdot a^{-1}_\gamma$ for $\gamma \in \Gamma$ defines a continuous map $\zeta\colon \Gamma \to B$. This map is 1-cocycle, since for all $\sigma, \tau \in \Gamma$,

$$\zeta_\sigma \cdot (\sigma\zeta_\tau) = \beta_\sigma \cdot a^{-1}_\sigma \cdot (\sigma\beta_\tau) \cdot (\sigma a_\tau)^{-1} = \beta_{\sigma\tau} \cdot a^{-1}_{\sigma\tau} = \zeta_{\sigma\tau}.$$

Since for $\gamma \in \Gamma$, the element a_γ lies in $A = \ker(B \to C)$, the image of ζ_γ in C is ξ_γ. Thus the class of ζ in $H^1(\Gamma, B)$ maps to the class of ξ in $H^1(\Gamma, C)$, proving the exactness of the sequence at $H^1(\Gamma, C)$, and the rest was established in Corollary 6.4.13. □

Corollary 8.1.3. *Let B be a discrete Γ-module and $A \subset B$ a discrete Γ-submodule. Let $C = B/A$. Then the exact sequence of Proposition 8.1.2 may be extended to an exact sequence of groups*

$$1 \to A^\Gamma \to B^\Gamma \to C^\Gamma \to H^1(\Gamma, A) \to H^1(\Gamma, B) \to H^1(\Gamma, C) \to H^2(\Gamma, A) \to H^2(\Gamma, B).$$

Proof. In view of Corollary 6.4.13 and Proposition 8.1.2, the only point to verify is exactness at $H^2(\Gamma, A)$. From the explicit description of the map δ^2 given in Corollary 6.4.13, it is clear that the composite $H^1(\Gamma, C) \to H^2(\Gamma, A) \to H^2(\Gamma, B)$ is trivial. Let now $\alpha\colon \Gamma \times \Gamma \to A$ be a 2-cocyle whose image in $Z^2(\Gamma, B)$ is a 2-coboundary. This means that there exists a continuous map $\beta\colon \Gamma \to B$ such that

$$\alpha_{\sigma,\tau} = \beta_\sigma \cdot (\sigma\beta_\tau) \cdot \beta^{-1}_{\sigma\tau} \quad \text{for all } \sigma, \tau \in \Gamma.$$

Since α takes values in $A \subset B$, the image of $\beta_\sigma \cdot (\sigma\beta_\tau) \cdot \beta^{-1}_{\sigma\tau}$ in C vanishes for every $\sigma, \tau \in \Gamma$, which proves that the composite $\xi\colon \Gamma \xrightarrow{\beta} B \to C$ is a 1-cocyle. It follows from the explicit formula for the map δ^2 given in Proposition 8.1.2 that the class of ξ in $H^1(\Gamma, C)$ is mapped to the class of α in $H^2(\Gamma, A)$. □

Remark 8.1.4. The exact sequence of Corollary 8.1.3 can be further extended on the right using the morphism $H^2(\Gamma, B) \to H^2(\Gamma, C)$.

The exact sequence of Proposition 8.1.2 is functorial in the following sense. To a commutative diagram of discrete Γ-groups with exact rows

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 1 \end{tikzcd}$$

such that $a \cdot b = b \cdot a$ for all $a \in A, b \in B$, resp. $a \in A', b \in B'$, corresponds a commutative diagram of pointed sets with exact rows

$$\begin{tikzcd}
\{*\} \arrow[r] & A^\Gamma \arrow[r] \arrow[d] & B^\Gamma \arrow[r] \arrow[d] & C^\Gamma \arrow[r] \arrow[d] & H^1(\Gamma, A) \arrow[r] \arrow[d] & H^1(\Gamma, B) \arrow[r] \arrow[d] & H^1(\Gamma, C) \arrow[r] \arrow[d] & H^2(\Gamma, A) \arrow[d] \\
\{*\} \arrow[r] & A'^\Gamma \arrow[r] & B'^\Gamma \arrow[r] & C'^\Gamma \arrow[r] & H^1(\Gamma, A') \arrow[r] & H^1(\Gamma, B') \arrow[r] & H^1(\Gamma, C') \arrow[r] & H^2(\Gamma, A').
\end{tikzcd}$$

This assertion may be verified using the explicit formula for the connecting maps δ (see Proposition 6.4.10) and δ^2.

If G is a k-group such that $G(k_s)$ is abelian, we will write

$$H^2(k, G) = H^2(\mathrm{Gal}(k_s/k), G(k_s)).$$

Thus if

$$1 \to A \to B \to C \to 1$$

is an exact sequence of k-groups such that $a \cdot b = b \cdot a$ for all $a \in A(k_s)$ and $b \in B(k_s)$, we have by Proposition 8.1.2 an exact sequence of pointed sets

$$\{*\} \to A(k) \to B(k) \to C(k) \xrightarrow{\delta} H^1(k, A) \to H^1(k, B) \to H^1(k, C) \xrightarrow{\delta^2} H^2(k, A)$$

which is functorial in the sense described above.

2. The Brauer group, II

Recall from §7.3 that every finite-dimensional central simple k-algebra A of degree n has a class $[A] \in H^1(k, \mathrm{PGL}_n)$. The short exact sequence of k-groups (see (7.3.b))

$$1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1.$$

yields by Proposition 8.1.2 an exact sequence of pointed sets

$$H^1(k, \mathrm{GL}_n) \to H^1(k, \mathrm{PGL}_n) \xrightarrow{\delta_n} H^2(k, \mathbb{G}_m). \tag{8.2.a}$$

We will use the additive notation in the abelian group $H^2(k, \mathbb{G}_m)$.

LEMMA 8.2.1. *Let A be a finite-dimensional central simple k-algebra of degree n. Then $\delta_n[A] = 0$ in $H^2(k, \mathbb{G}_m)$ if and only if A is split.*

PROOF. Since δ_n is a morphism of pointed sets, we have $\delta_n[A] = 0$ when A is split. The converse follows from the exact sequence (8.2.a), since $H^1(k, \mathrm{GL}_n)$ vanishes by Hilbert's Theorem 90 (Proposition 7.1.1). □

LEMMA 8.2.2. *Let A, B be finite-dimensional central simple k-algebras. Set $m = \deg(A)$ and $n = \deg(B)$. Then*

$$\delta_m([A]) + \delta_n([B]) = \delta_{mn}([A \otimes_k B]) \in H^2(k, \mathbb{G}_m)$$

PROOF. By Proposition 8.1.2 (and the discussion below it), the diagram (7.3.c) yields a commutative diagram

$$\begin{tikzcd}
H^1(k, \mathrm{PGL}_m) \times H^1(k, \mathrm{PGL}_n) \arrow[r] \arrow[d, "(\delta_m, \delta_n)"'] & H^1(k, \mathrm{PGL}_m \times \mathrm{PGL}_n) \arrow[r] \arrow[d] & H^1(k, \mathrm{PGL}_{mn}) \arrow[d, "\delta_{mn}"] \\
H^2(k, \mathbb{G}_m) \times H^2(k, \mathbb{G}_m) \arrow[r] & H^2(k, \mathbb{G}_m \times \mathbb{G}_m) \arrow[r] & H^2(k, \mathbb{G}_m)
\end{tikzcd}$$

Since the map $\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ in the diagram (7.3.c) is the group operation of $\mathbb{G}_m$, it follows that the lower composite in the above diagram is the operation in the group $H^2(k, \mathbb{G}_m)$. The upper composite maps $([A],[B])$ to $[A \otimes_k B]$ by Proposition 7.3.1, and the statement follows. $\square$

Proposition 8.2.3. *Mapping a finite-dimensional central simple k-algebra A to the element $\delta_{\deg(A)}([A])$ yield an injective group morphism*

$$\mathrm{Br}(k) \to H^2(k, \mathbb{G}_m).$$

Proof. Let A be a finite-dimensional central simple k-algebra of degree m. Since $\delta_n([M_n(k)]) = 0$ for any integer n, it follows from Lemma 8.2.2 that $\delta_m[A] = \delta_{mn}(M_n(A))$. Thus $A \mapsto \delta_m[A]$ induces a map $\mathrm{Br}(k) \to H^2(k, \mathbb{G}_m)$ which is injective by Lemma 8.2.1, and a group morphism by Lemma 8.2.2. $\square$

Remark 8.2.4. We will prove later that this morphism is in fact bijective.

3. The period

Theorem 8.3.1. *Let A be a finite-dimensional central simple k-algebra. Then* $\mathrm{ind}(A) \cdot [A] = 0$ *in* $\mathrm{Br}(k)$.

Proof. We may assume that A is division, and let $n = \mathrm{ind}(A) = \deg(A)$. The commutative diagram of k-groups with exact rows (where $\det \colon \mathrm{GL}_n \to \mathbb{G}_m$ denotes the morphism of k-groups sending a matrix to its determinant, and $n \colon \mathbb{G}_m \to \mathbb{G}_m$ is the morphism $x \mapsto x^n$)

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, "n"] & \mathrm{GL}_n \arrow[r] \arrow[d, "\det"] & \mathrm{PGL}_n \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r, "="] & \mathbb{G}_m \arrow[r] & 1 \arrow[r] & 1
\end{tikzcd}$$

gives rise to a commutative diagram of pointed sets

$$\begin{tikzcd}
H^1(k, \mathrm{PGL}_n) \arrow[r, "\delta_n"] \arrow[d] & H^2(k, \mathbb{G}_m) \arrow[d, "n"] \\
\{*\} \arrow[r] & H^2(k, \mathbb{G}_m)
\end{tikzcd}$$

It follows that $n\delta_n([A]) = 0$ in $H^2(k, \mathbb{G}_m)$, so that by Proposition 8.2.3 we have $n[A] = 0$ in $\mathrm{Br}(k)$. $\square$

Corollary 8.3.2. *For every finite-dimensional central simple k-algebra A, there exist integers $r, n \in \mathbb{N} - \{0\}$ such that $A^{\otimes n} \simeq M_r(k)$.*

Corollary 8.3.3. *Let L/k be a field extension of finite degree. Then the map* $\mathrm{Br}(L/k) \to \mathrm{Br}(L/k)$ *given by multiplication by $[L : k]$ is zero.*

Proof. This follows from Corollary 3.2.3 and Theorem 8.3.1. $\square$

Proposition 8.3.4. *Assume that the field k has positive characteristic p and is perfect (i.e. every algebraic extension of k is separable). Then the map* $\mathrm{Br}(k) \to \mathrm{Br}(k)$ *given by multiplication by p is an isomorphism.*

PROOF. The map $k_s^\times \to k_s^\times$ given by $x \mapsto x^p$ is injective because k_s has characteristic p, and surjective because k_s is algebraically closed. It follows that multiplication by p is bijective in $H^2(\mathrm{Gal}(k_s/k), k_s^\times) = H^2(k, \mathbb{G}_m)$, hence injective in $\mathrm{Br}(k)$ by Proposition 8.2.3. Now for every element $x \in \mathrm{Br}(k)$, there exists a nonzero integer n such that $nx = 0$ by Theorem 8.3.1. If $n = pm$ for some integer m, we must have $mx = 0$, as multiplication by p is injective in $\mathrm{Br}(k)$. We may thus assume that n is prime to p. Writing $1 = un + vp$ with $u, v \in \mathbb{Z}$, we have $x = unx + vpx = p(vx)$, proving that multiplication by p is surjective in $\mathrm{Br}(k)$. □

DEFINITION 8.3.5. Let A be a finite-dimensional central simple k-algebra. The order of the class of A in the group $\mathrm{Br}(k)$ is called the *period* of A, and is denoted by $\mathrm{per}(A)$.

The period of A is thus the smallest integer $n > 0$ such that $A^{\otimes n}$ splits. By Theorem 8.3.1, we have

$$\mathrm{per}(A) \mid \mathrm{ind}(A). \tag{8.3.a}$$

The next proposition is reminiscent of Proposition 3.2.8.

PROPOSITION 8.3.6. *Let A be a finite-dimensional central simple k-algebra, and L/k a field extension of finite degree. Then*

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

PROOF. The first divisibility is clear. The element $\mathrm{per}(A_L) \cdot [A]$ belongs to $\mathrm{Br}(L/k)$, hence $[L:k]\,\mathrm{per}(A_L) \cdot [A] = 0$ in $\mathrm{Br}(k)$ by Corollary 8.3.3, which yields the second divisibility. □

PROPOSITION 8.3.7. *Let A be a finite-dimensional central simple k-algebra. Then the integers* $\mathrm{per}(A)$ *and* $\mathrm{ind}(A)$ *have the same prime divisors.*

PROOF. In view of (8.3.a), every prime divisor of $\mathrm{per}(A)$ certainly divides $\mathrm{ind}(A)$. Conversely, let p be a prime divisor of $\mathrm{ind}(A)$. Let L/k be a separable field extension splitting A and such that $[L:k] = \mathrm{ind}(A)$ (see Corollary 3.3.4). Then L is contained in some finite Galois extension E/k by Lemma 4.3.8. Let H be a p-Sylow subgroup of $\mathrm{Gal}(E/k)$, and set $K = E^H$. Then $[K:k]$ is prime to p and $[E:K]$ is a power of p. The integer $\mathrm{ind}(A)$ divides the product $[K:k]\,\mathrm{ind}(A_K)$ by Proposition 3.2.8, hence $\mathrm{ind}(A_K)$ is divisible by p. Moreover $\mathrm{ind}(A_K)$ divides $[E:K]$ (by Corollary 3.2.3), hence $\mathrm{ind}(A_K)$ is a power of p. Thus $\mathrm{per}(A_K)$ is a power of p by (8.3.a). Since A_K is not split (as its index is divisible by p), it follows that $\mathrm{per}(A_K) \neq 1$, so that $p \mid \mathrm{per}(A_K) \mid \mathrm{per}(A)$. □

PROPOSITION 8.3.8 (Brauer). *Let D be a finite-dimensional central division k-algebra. Write*

$$\mathrm{ind}(D) = q_1 \cdots q_n$$

where $q_1, \ldots, q_n$ are powers of pairwise distinct prime numbers. Then there are finite-dimensional central division k-algebras D_i such that $\mathrm{ind}(D_i) = q_i$ *for $i = 1, \ldots, n$ and*

$$D \simeq D_1 \otimes_k \cdots \otimes_k D_n.$$

PROOF. For $i = 1, \ldots, n$, let p_i be the prime divisor of q_i. By Theorem 8.3.1 we may write $\mathrm{per}(D) = b_1 \cdots b_n$, where $b_i \mid q_i$ for each $i = 1, \ldots, n$. The elements $r_i = \mathrm{per}(D)/b_i$ for $i = 1, \ldots, n$ are coprime, hence there exist integers $a_1, \ldots, a_n \in \mathbb{Z}$ such that $a_1 r_1 + \cdots + a_n r_n = 1$. For each $i = 1, \ldots, n$, let D_i be a finite-dimensional central division k-algebra whose class in $\mathrm{Br}(k)$ is $a_i r_i \cdot [D]$. Then $D_1 \otimes_k \cdots \otimes_k D_n$ is Brauer equivalent to

D. Also, for each $i = 1, \ldots, n$ we have $\operatorname{per}(D_i) \mid b_i$ (as $b_i \cdot [D_i] = a_i \operatorname{per}(D) \cdot [D] = 0$), hence $\operatorname{ind}(D_i)$ is a power of p_i by Proposition 8.3.7. It follows from Corollary 3.2.11 (applied $n-1$ times) that the k-algebra $D_1 \otimes_k \cdots \otimes_k D_n$ is division, hence isomorphic to D. Since $\operatorname{ind}(D_1) \cdots \operatorname{ind}(D_n) = q_1 \cdots q_n$, we see that $\operatorname{ind}(D_i) = q_i$ for all $i = 1, \ldots, n$ (by looking at the p_i-adic valuation). $\square$

CHAPTER 9

Cohomology of groups

In this chapter we present the classical construction of group cohomology (with abelian coefficients) using homological methods. The aim is to define cohomology groups in degrees higher than two, in a way which permits to extend the long exact sequences obtained earlier.

The main purpose of this machinery is to produce (infinite) long exact sequences of cohomology groups from short exact sequences of coefficients groups. Besides, this approach has two important consequences, including for cohomology groups in degrees 1 and 2; both of those can be obtained directly in low degrees, but the homological approach is particularly effective in these situations. The first such consequence is Shapiro's Lemma computing the cohomology coinduced modules. Like Hilbert's Theorem 90, this lemma provides vanishing results, which are at the basis of many computations of Galois cohomology groups. The second consequence is the construction of corestriction morphisms, together with the associated projection formula. This is a very useful tool when trying to control torsion phenomena in the cohomology groups and passing to subgroups (the so-called "transfer" or "restriction-corestriction" arguments).

We start with the cohomology of finite groups, and more generally, discrete groups. This is done using projective resolutions of the module $\mathbb{Z}$ equipped with the trivial group action. The cohomology of profinite groups (the main case of interest for Galois cohomology) can then be obtained as the direct limit of the cohomology of its finite quotients. These cohomology groups cannot simply be constructed using projective resolutions as in the finite case, because such resolutions need not exist in the category of discrete modules when the group is not discrete. They could, however, be constructed directly using injective resolutions of the coefficient module, a strategy that is not pursued here.

1. Projective Resolutions

In this section, we fix a (unital associative) ring R. As before, an R-module means a left R-module.

Definition 9.1.1. An R-module P is called *projective* if for every surjective R-module morphism $M \to N$, the natural morphism $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$ is surjective.

Lemma 9.1.2. *Every direct summand of a projective R-module is projective.*

Proof. Let P be a projective R-module, and B a direct summand of P. Let $M \to N$ be a surjective morphism of R-modules and $f : B \to N$ a morphism of R-modules. By projectivity of P, the composite $P \to B \to N$ lifts to a morphism $P \to M$. Then the composite $B \to P \to M$ is a lifting of f. We have proved that B is projective. $\square$

Proposition 9.1.3. *An R-module is projective if and only if it is a direct summand of a free module.*

PROOF. Let P be a projective R-module. Let F be the free R-module on the basis e_p for $p \in P$. The morphism of R-modules $f\colon F \to P$ given by $e_p \mapsto p$ is visibly surjective. By projectivity of P, we find a morphism of R-modules $s\colon P \to F$ such that $f \circ s = \mathrm{id}_P$. We have proved that P is a direct summand of F.

Let now L be a free R-module, with basis l_α for $\alpha \in A$. Let $M \to N$ be a surjective morphism of R-modules and $f\colon L \to N$ a morphism of R-modules. For each $\alpha \in A$, pick a preimage $m_\alpha \in M$ of $f(l_\alpha) \in N$. Then $l_\alpha \mapsto m_\alpha$ defines a morphism of R-modules $F \to M$ such that the composite $F \to M \to N$ is f. We have proved that L is projective, and conclude using Lemma 9.1.2. □

DEFINITION 9.1.4. A *chain complex (of R-modules) C* is a collection of R-modules C_i and morphisms of R-modules $d_i^C\colon C_i \to C_{i-1}$ for $i \in \mathbb{Z}$, satisfying

$$d_{i-1}^C \circ d_i^C = 0 \quad \text{for all } i \in \mathbb{Z}.$$

The chain complex C is called *exact* if $\ker d_i^C = \operatorname{im} d_{i+1}^C$ for all $i \in \mathbb{Z}$. A morphism of chain complexes $f\colon C \to C'$ is a collection of morphisms $f_i\colon C_i \to C_i'$ such that

$$f_{i-1} \circ d_i^C = d_i^{C'} \circ f_i \quad \text{for all } i \in \mathbb{Z}.$$

DEFINITION 9.1.5. Let M be an R-module. A *resolution* $C \to M$ is a chain complex C such that $C_i = 0$ for $i < 0$, together with a morphism $C_0 \to M$ such that the augmented chain complex

$$\cdots \to C_1 \to C_0 \to M \to 0$$

is exact. A resolution $C \to M$ is said to be projective if each C_i is so.

LEMMA 9.1.6. *Every R-module admits a projective resolution.*

PROOF. Let M be an R-module. Set $M = P_{-1}$ and $P_i = 0$ for $i < -1$. We proceed by induction, and assume that the exact sequence $P_i \to P_{i-1} \to \cdots \to P_0 \to P_{-1} \to 0$ is constructed for some $i \geq -1$. Let $N = \ker(P_i \to P_{i-1})$, and let P_{i+1} be the free module on the basis e_n for $n \in N$. Then P_{i+1} is projective by Proposition 9.1.3. The morphism of R-modules $P_{i+1} \to N$ given by sending $e_n \mapsto n$ is surjective, and the composite $P_{i+1} \to N \subset P_i$ fits into the required exact sequence. □

DEFINITION 9.1.7. We say that the morphisms of chain complexes $f, g\colon C \to C'$ are *homotopic* if there exists a collection of morphisms $s_i\colon C_i \to C_{i+1}'$ for $i \in \mathbb{Z}$ such that

$$f_i - g_i = d_{i+1}^{C'} \circ s_i + s_{i-1} \circ d_i^C.$$

A morphism of chain complexes $f\colon M \to N$ is a *homotopy equivalence* if there exists a morphism of chain complexes $g\colon N \to M$ such that $f \circ g$ is homotopic to the identity of N and $g \circ f$ is homotopic to the identity of M.

PROPOSITION 9.1.8. *Let E and P be chain complexes of R-modules. Assume that*

(i) $P_i = E_i = 0$ *for* $i < -1$.
(ii) P_i *is projective for* $i \geq 0$.
(iii) E *is exact.*

Let $g\colon P_{-1} \to E_{-1}$ be a morphism of R-modules. Then there exists a morphism of chain complexes of R-modules $f\colon P \to E$ such that $f_{-1} = g$. This morphism is unique up to homotopy.

PROOF. We construct $f_i \colon P_i \to E_i$ inductively, starting with $f_{-1} = g$. Assume that $i \geq 0$ and that f_{i-1} is constructed. The composite $f_{i-1} \circ d_i^P \colon P_i \to E_{i-1}$ has image contained into $\ker d_{i-1}^E$, because

$$d_{i-1}^E \circ f_{i-1} \circ d_i^P = f_{i-2} \circ d_{i-1}^P \circ d_i^P = 0.$$

By exactness of the chain complex E, the morphism $E_i \to \ker d_{i-1}^E$ induced by d_i^E is surjective, hence by projectivity of P_i, we may find a morphism of R-modules $f_i \colon P_i \to E_i$ such that $d_i^E \circ f_i = f_{i-1} \circ d_i^P$.

Now let $f, f' \colon P \to E$ be two morphisms of chain complexes extending g. We construct for each $i \in \mathbb{Z}$ a morphism of R-modules $s_i \colon P_i \to E_{i+1}$ such that

$$f_i - f'_i = d_{i+1}^E \circ s_i + s_{i-1} \circ d_i^P$$

by induction on i. We let $s_i = 0$ for $i < -1$. Assume that s_{i-1} is constructed. Then

$$\begin{aligned} d_i^E \circ (f_i - f'_i) &= (f_{i-1} - f'_{i-1}) \circ d_i^P \\ &= d_i^E \circ s_{i-1} \circ d_i^P + s_{i-2} \circ d_{i-1}^P \circ d_i^P \\ &= d_i^E \circ s_{i-1} \circ d_i^P, \end{aligned}$$

so that the morphism $(f_i - f'_i) - s_{i-1} \circ d_i^P \colon P_i \to E_i$ has image in $\ker d_i^E$. By exactness of the chain complex E, the morphism $E_{i+1} \to \ker d_i^E$ is surjective. By projectivity of P_i, we obtain a morphism $s_i \colon P_i \to E_{i+1}$ such that $d_{i+1}^E \circ s_i = (f_i - f'_i) - s_{i-1} \circ d_i^P$, as required. □

COROLLARY 9.1.9. *Let M be an R-module, and let $P \to M$ and $P' \to M$ projective resolutions. Then there exists a morphism of chain complexes $P \to P'$ such that the composites $P_0 \to P'_0 \to M$ and $P_0 \to M$ coincide. Such a morphism is unique up to homotopy, and is a homotopy equivalence.*

PROOF. By Proposition 9.1.8, the identity of M extends to morphisms of chain complexes $P \to P'$ and $P' \to P$, which are unique up to homotopy. The composite $P \to P' \to P$ and the identity of P are both extensions of the identity of M. They must be homotopic by the unicity part of Proposition 9.1.8. For the same reason, the composite $P' \to P \to P'$ is homotopic to the identity of P'. □

2. Cochain complexes

DEFINITION 9.2.1. A *cochain complex (of R-modules) C* is a collection of R-modules C^i and morphisms of R-modules $d_C^i \colon C^i \to C^{i+1}$ for $i \in \mathbb{Z}$, called *coboundary morphisms*, satisfying

$$d_C^{i+1} \circ d_C^i = 0 \quad \text{for all } i \in \mathbb{Z}.$$

The R-module

$$H^i(C) = \ker d_C^i / \operatorname{im} d_C^{i-1}$$

is called the *i-th cohomology* of the cochain complex C. A morphism of cochain complexes $f \colon C \to C'$ is a collection of morphisms of R-modules $f^i \colon C^i \to C'^i$ such that

$$f^{i+1} \circ d_C^i = d_{C'}^i \circ f^i \quad \text{for all } i \in \mathbb{Z}.$$

Such a morphism induces morphisms of R-modules $H^i(C) \to H^i(C')$ for all $i \in \mathbb{Z}$.

Definition 9.2.2. We say that the morphisms of cochain complexes $f, g\colon C \to C'$ are *homotopic* if there is a collection of morphisms $s^i\colon C^i \to C'^{i-1}$ for $i \in \mathbb{Z}$ such that

$$f^i - g^i = d_{C'}^{i-1} \circ s^i + s^{i+1} \circ d_C^i.$$

A morphism of cochain complexes $f\colon C \to C'$ is a *homotopy equivalence* if there exists a morphism of cochain complexes $g\colon C' \to C$ such that $f \circ g$ is homotopic to the identity of C' and $g \circ f$ is homotopic to the identity of C.

Proposition 9.2.3. *Homotopic morphisms induce the same morphism in cohomology.*

Proof. In the notation of Definition 9.2.2, the morphism $d_{C'}^{i-1} \circ s^i$ has image contained in $\operatorname{im} d_{C'}^{i-1}$ and the kernel of the morphism $s^{i+1} \circ d_C^i$ contains $\ker d_C^i$. These morphisms thus induce the zero morphism in cohomology by construction. □

Corollary 9.2.4. *A homotopy equivalence induces isomorphisms in cohomology.*

Definition 9.2.5. A sequence of cochain complexes

$$0 \to C' \to C \to C'' \to 0$$

is called *exact* if the sequence

$$0 \to C'^i \to C^i \to C''^i \to 0$$

is exact for each $i \in \mathbb{Z}$.

Proposition 9.2.6. *An exact sequence of cochain complexes of R-modules*

$$0 \to C' \to C \to C'' \to 0$$

induces an exact sequence of R-modules

$$\cdots \to H^{i-1}(C'') \to H^i(C') \to H^i(C) \to H^i(C'') \to H^{i+1}(C) \to \cdots$$

Given a commutative diagram of cochain complexes of R-modules

$$\begin{tikzcd}
0 \arrow[r] & C' \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & D' \arrow[r] & D \arrow[r] & D'' \arrow[r] & 0
\end{tikzcd}$$

having exact rows, the induced diagram of R-modules

$$\begin{tikzcd}
\cdots \arrow[r] & H^{i-1}(C'') \arrow[r] \arrow[d] & H^i(C') \arrow[r] \arrow[d] & H^i(C) \arrow[r] \arrow[d] & H^i(C'') \arrow[r] \arrow[d] & H^{i+1}(C') \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & H^{i-1}(D'') \arrow[r] & H^i(D') \arrow[r] & H^i(D) \arrow[r] & H^i(D'') \arrow[r] & H^{i+1}(D') \arrow[r] & \cdots
\end{tikzcd}$$

is commutative.

Proof. (The is the so-called "snake lemma"; details are left as an exercise.) Given $a \in H^{i-1}(C'')$, choose a representative $b \in C''^{i-1}$ such that $d_{C''}^{i-1}(b) = 0$. Pick a preimage $c \in C^{i-1}$ of b, and let $e = d_C^{i-1}(c) \in C^i$. Then e is mapped to zero in C''^i, hence is the image of an element $f \in C'^i$. One may then check that the class of f in $H^i(C')$ does not depend on any of the choices made, and that the map $\partial\colon H^{i-1}(C'') \to H^i(C')$ given sending x to the class of f is a morphism of R-modules fitting into the above exact sequences and diagrams. □

3. Cohomology of discrete groups

In this section G is a group (endowed with the discrete topology). We consider the ring $\mathbb{Z}[G]$ defined as the free abelian group on the basis e_g for $g \in G$, with the multiplication given by $e_g e_h = e_{gh}$ for $g, h \in G$. Observe that a $\mathbb{Z}[G]$-module structure on an abelian group A is the same thing as an action of the group G by group automorphisms, the action of $g \in G$ corresponding to left multiplication by $e_g \in \mathbb{Z}[G]$. In order to lighten the notation, we will usually denote the element $e_g \in \mathbb{Z}[G]$ simply by g. We will use the additive notation for the group action on a $\mathbb{Z}[G]$-module A, and denote the action of an element $g \in G$ on A by $x \mapsto gx$.

The cohomology groups. Let A be $\mathbb{Z}[G]$-module and C a chain complex of $\mathbb{Z}[G]$-modules. We denote by $\mathrm{Hom}_{\mathbb{Z}[G]}(C, A)$ the cochain complex of of abelian groups (i.e. $\mathbb{Z}$-modules) such that $(\mathrm{Hom}_{\mathbb{Z}[G]}(C, A))^i = \mathrm{Hom}_{\mathbb{Z}[G]}(C_i, A)$ for all $i \in \mathbb{Z}$, and

$$d^i_{\mathrm{Hom}_{\mathbb{Z}[G]}(C,A)} \colon \mathrm{Hom}_{\mathbb{Z}[G]}(C_i, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(C_{i+1}, A)$$

is the morphism induced by composition with d^C_{i+1}.

A morphism of chain complexes of $\mathbb{Z}[G]$-modules $f \colon C \to C'$ induces a morphism of cochain complexes of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}[G]}(f, A) \colon \mathrm{Hom}_{\mathbb{Z}[G]}(C', A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(C, A).$$

If f is homotopic to g, then $\mathrm{Hom}_{\mathbb{Z}[G]}(f, A)$ is homotopic to $\mathrm{Hom}_{\mathbb{Z}[G]}(g, A)$. Thus a homotopy equivalence $C \to C'$ induces a homotopy equivalence $\mathrm{Hom}_{\mathbb{Z}[G]}(C', A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(C, A)$, and therefore isomorphisms $H^q(\mathrm{Hom}_{\mathbb{Z}[G]}(C', A)) \to H^q(\mathrm{Hom}_{\mathbb{Z}[G]}(C, A))$ for all q by Corollary 9.2.4.

DEFINITION 9.3.1. Let A be a $\mathbb{Z}[G]$-module. We view $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module with trivial G-action, and choose a projective resolution $P \to \mathbb{Z}$. By the discussion above and Corollary 9.1.9, for each $q \in \mathbb{Z}$ the group $H^q(\mathrm{Hom}_{\mathbb{Z}[G]}(P, A))$ is independent of the choice of the projective resolution P, up to a canonical isomorphism. We denote this group by $H^q(G, A)$.

It follows from the construction that $H^q(G, A) = 0$ for $q < 0$.

REMARK 9.3.2. If $G = 1$, then $H^0(G, A) = A$ and $H^q(G, A) = 0$ for all $q > 0$. Indeed a projective resolution P of $\mathbb{Z}$ is given by setting $P_0 = \mathbb{Z}$ and $P_i = 0$ for $i \neq 0$, where the morphism $P_0 \to \mathbb{Z}$ is the identity.

LEMMA 9.3.3. *For every $\mathbb{Z}[G]$-module A, we have $H^0(G, A) = A^G$.*

PROOF. Observe that $A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Let $P \to \mathbb{Z}$ be a projective resolution, as $\mathbb{Z}[G]$-module. The exact sequence of $\mathbb{Z}[G]$-modules

$$P_1 \to P_0 \to \mathbb{Z} \to 0$$

induces an exact sequence of abelian groups (exercise)

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A),$$

so that

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = \ker(\mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A)) = H^0(\mathrm{Hom}_{\mathbb{Z}[G]}(P, A)). \quad \square$$

Let now $f\colon A \to A'$ be a morphism of $\mathbb{Z}[G]$-modules. Composition with f induces a morphism of cochain complex of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P,A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P,A')$$

and thus morphisms of abelian groups for all q

$$f_*\colon H^q(G,A) \to H^q(G,A').$$

Observe that for every q, the map

$$\mathrm{Hom}_{\mathbb{Z}[G]}(A,A') \to \mathrm{Hom}_{\mathbb{Z}}(H^q(G,A),H^q(G,A')) \quad ; \quad f \mapsto f_*$$

is a morphism of abelian groups, and that the associations $A \mapsto H^q(G,A)$ and $f \mapsto f_*$ define a functor from the category of $\mathbb{Z}[G]$-modules to the category of abelian groups.

PROPOSITION 9.3.4. *Every exact sequence of $\mathbb{Z}[G]$-modules*

$$0 \to A \to B \to C \to 0$$

induces an exact sequence of abelian groups

$$\cdots \to H^{q-1}(G,C) \to H^q(G,A) \to H^q(G,B) \to H^q(G,C) \to \cdots$$

Given a commutative diagram of $\mathbb{Z}[G]$-modules

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

having exact rows, the induced diagram of abelian groups

$$\begin{tikzcd}
\cdots \arrow[r] & H^{q-1}(G,C) \arrow[r] \arrow[d] & H^q(G,A) \arrow[r] \arrow[d] & H^q(G,B) \arrow[r] \arrow[d] & H^q(G,C) \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & H^{q-1}(G,C') \arrow[r] & H^q(G,A') \arrow[r] & H^q(G,B') \arrow[r] & H^q(G,C') \arrow[r] & \cdots
\end{tikzcd}$$

is commutative.

PROOF. Let $P \to \mathbb{Z}$ be a projective resolution. Since each $\mathbb{Z}[G]$-modules P_i is projective, we have an exact sequence of cochain complexes of abelian groups

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(P,A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P,B) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P,C) \to 0.$$

The statement (including the fact that the long exact sequence obtained does not depend on the choice of P) is then a consequence of Proposition 9.2.6. $\square$

REMARK 9.3.5. Let A, B be $\mathbb{Z}[G]$-modules, and set $B = A \oplus C$. Then the morphisms $A \to B \to A$ and $C \to B \to C$ induce decompositions $H^q(G,B) = H^q(G,A) \oplus H^q(G,C)$ as abelian groups for each $q \geq 0$. In this case the connecting homomorphisms $H^{q-1}(G,C) \to H^q(G,A)$ appearing in Proposition 9.3.4 are zero.

Let now $\psi\colon G \to G'$ be a group morphism and A a $\mathbb{Z}[G']$-module. We may view any $\mathbb{Z}[G']$-module as a $\mathbb{Z}[G]$-module using ψ. Choose a projective resolution P of the $\mathbb{Z}[G]$-module $\mathbb{Z}$, and a projective resolution P' of the $\mathbb{Z}[G']$-module $\mathbb{Z}$. Then by Proposition 9.1.8 there exists a morphism of chain complexes of $\mathbb{Z}[G]$-modules $f\colon P \to P'$, which is unique up to homotopy. This morphism induces a morphism of cochain complexes of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}[G']}(P', A) = \mathrm{Hom}_{\mathbb{Z}[G]}(P', A) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}[G]}(f,A)} \mathrm{Hom}_{\mathbb{Z}[G]}(P, A).$$

Taking the cohomology, we obtain morphisms of abelian groups

$$\psi^* \colon H^q(G', A) \to H^q(G, A)$$

for all q, which does not depend on the choices of P, P' or f by Proposition 9.2.3.

In particular, when $H \subset G$ is a subgroup, we have thus constructed the *restriction morphisms*

$$\mathrm{Res}^G_H \colon H^q(G, A) \to H^q(H, A).$$

Explicit resolutions. We now describe a canonical projective resolution of the $\mathbb{Z}[G]$-module $\mathbb{Z}$ (endowed with the trivial G-action). For each $i \in \mathbb{N}$, let L_i be the free abelian group on the basis G^{i+1}. A G-action is given by $g(g_0, \dots, g_i) = (gg_0, \dots, gg_i)$. The $\mathbb{Z}[G]$-module L_i is free, a basis being given by the elements $(1, g_1, \dots, g_i)$. For $i \geq 1$, consider the morphism of abelian groups $d^L_i \colon L_i \to L_{i-1}$ defined by

$$d^L_i(g_0, \dots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \dots, \widehat{g_j}, \dots, g_i),$$

where the notation $\widehat{g_j}$ means that the element g_j is omitted. Let us write $L_i = 0$ for $i < -1$ and $d^L_i = 0$ for $i \leq 0$. We have thus constructed a chain complex of $\mathbb{Z}[G]$-modules L. We define a morphism of abelian groups $\varepsilon \colon L_0 \to \mathbb{Z}$ by $(g_0) \mapsto 1$ for all $g_0 \in G$. Note that ε is a morphism of $\mathbb{Z}[G]$-modules for the trivial G-action on $\mathbb{Z}$, and that $\varepsilon \circ d^L_0 = 0$.

Let us define a chain complex of $\mathbb{Z}[G]$-modules $\widetilde{L}$ by setting $\widetilde{L}_i = L_i$ for $i \neq -1$ and $\widetilde{L}_{-1} = \mathbb{Z}$ with the trivial G-action, together with $d^{\widetilde{L}}_i = d^L_i$ for $i \neq 0$, and $d^L_0 = \varepsilon$.

LEMMA 9.3.6. *The complex $\widetilde{L}$ is exact.*

PROOF. Consider the group morphisms (which are not $\mathbb{Z}[G]$-linear in general!)

$$s_i \colon \widetilde{L}_i \to \widetilde{L}_{i+1} \colon (g_0, \dots, g_i) \mapsto (1, g_0, \dots, g_i)$$

for $i \geq 0$. Let $s_{-1} \colon \mathbb{Z} = \widetilde{L}_{-1} \to \widetilde{L}_0$ be given by $n \mapsto n(1)$, and set $s_i = 0$ for $i < -1$. Then $d^{\widetilde{L}}_{i+1} \circ s_i + s_{i-1} \circ d^{\widetilde{L}}_i = \mathrm{id}_{\widetilde{L}_i}$ for all i, which implies the statement. □

REMARK 9.3.7. We just proved that $\widetilde{L}$ is homotopic to 0, when viewed as a complex of $\mathbb{Z}$-modules. Of course, this is in general not true as a complex of $\mathbb{Z}[G]$-modules.

When A is a $\mathbb{Z}[G]$-module, we obtain a cochain complex of abelian groups $C(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(L, A)$. For $i \in \mathbb{Z}$, we thus have

$$C^i(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(L_i, A),$$

and set

$$Z^i(G, A) = \ker d^i_{C(G,A)} \quad \text{and} \quad B^i(G, A) = \mathrm{im}\, d^i_{C(G,A)}.$$

Since each L_i is free, hence L is a projective resolution of the $\mathbb{Z}[G]$-module $\mathbb{Z}$ (Lemma 9.3.6), it follows that

$$H^i(G, A) = Z^i(G, A)/B^i(G, A).$$

For $g_1, \dots, g_i \in G$, the elements

$$[g_1, \dots, g_i] = (1, g_1, g_1g_2, \dots, g_1 \cdots g_i)$$

for a basis of the $\mathbb{Z}[G]$-module L_i. An element $f \in C^i(G,A)$ then corresponds to a map $a\colon G^i \to A$ given by

$$(g_1,\dots,g_i) \mapsto a_{g_1,\dots,g_i} = f[g_1,\dots,g_i].$$

The element $d^i_{C(G,A)}(f) \in C^{i+1}(G,A)$ is then given by the map $b\colon G^{i+1} \to A$ defined by

$$b_{g_1,\dots,g_{i+1}} = g_1 a_{g_2,\dots,g_{i+1}} + \sum_{j=1}^{i} (-1)^j a_{g_1,\dots,g_j g_{j+1},\dots,g_{i+1}} + (-1)^{i+1} a_{g_1,\dots,g_i}. \tag{9.3.a}$$

Example 9.3.8 (1-cocyles). An element $\xi\colon g \mapsto a_g$ of $C^1(G,A)$ belongs to $Z^1(G,A)$ if and only if $g_1\xi_{g_2} - \xi_{g_1 g_2} + \xi_{g_1} = 0$ for all $g_1, g_2 \in G$, which is exactly (6.4.a) written additively. The element ξ belongs to $B^1(G,A)$ if and only if there exists $a \in A$ such that $\xi_{g_1} = g_1 a - a$ for all $g_1 \in G$, which means that the 1-cocyle ξ is cohomologous to the trivial 1-cocyle. Thus we recover the group $H^1(G,A)$ defined earlier when G is finite.

Example 9.3.9 (2-cocyles). An element $\alpha\colon (g,h) \mapsto a_{g,h}$ of $C^2(G,A)$ belongs to $Z^2(G,A)$ if and only if

$$0 = g_1\alpha_{g_2,g_3} - \alpha_{g_1g_2,g_3} + \alpha_{g_1,g_2g_3} - \alpha_{g_1,g_2}$$

for all $g_1,g_2,g_3 \in G$, which is exactly (8.1.a) written additively. The element α belongs to $B^2(G,A)$ if and only if there exists a map $a\colon G \to A$ denoted by $g \mapsto a_g$ such that

$$\alpha_{g_1,g_2} = g_1 a_{g_2} - a_{g_1g_2} + a_{g_1}$$

for all $g_1, g_2 \in G$, which means that the 2-cocyle α is a 2-coboundary. Thus we recover the group $H^2(G,A)$ defined earlier when G is finite.

Remark 9.3.10. Under the identifications of Example 9.3.8 and Example 9.3.9, the long exact sequence of Proposition 8.1.2 coincides with the relevant part of the long exact sequence of Proposition 9.3.4 (this may be checked using (9.3.a)).

Example 9.3.11 (Cohomology of cyclic groups). Assume that the group G is finite and cyclic, generated by σ. Consider the elements

$$N = \sum_{g\in G} g \in \mathbb{Z}[G] \quad ; \quad D = \sigma - 1 \in \mathbb{Z}[G].$$

We define a projective resolution C of the $\mathbb{Z}[G]$-module $\mathbb{Z}$ as follows. Set $C_i = 0$ if $i < 0$ and $C_i = \mathbb{Z}[G]$ if $i \geq 0$. For $i > 0$, the morphism $d^C_i\colon C_i \to C_{i-1}$ is defined as the multiplication with D if i is odd, and the multiplication with N if i is even. The morphism $C_0 = \mathbb{Z}[G] \to \mathbb{Z}$ is given by $g \mapsto 1$ for all $g \in G$. One verifies easily that the complex C is exact (observe that $\mathbb{Z}[G] \simeq \mathbb{Z}[X]/(X^n - 1)$ with $\sigma \mapsto X$ and $n = |G|$).

Let now A be a $\mathbb{Z}[G]$-module. Then for $i \geq 0$, we have $\operatorname{Hom}_{\mathbb{Z}[G]}(C_i, A) = A$, and the morphism $\operatorname{Hom}_{\mathbb{Z}[G]}(C_i,A) \to \operatorname{Hom}_{\mathbb{Z}[G]}(C_{i+1},A)$ corresponds to the endomorphism of A given by the action of N if i is odd, and by the action of D if i is even. Noting that A^G is the kernel of $D\colon A \to A$, and letting ${}_NA$ be the kernel of $N\colon A \to A$, we obtain for $q > 0$

$$H^q(G,A) = \begin{cases} A^G/NA & \text{if } q \text{ is even,} \\ {}_NA/DA & \text{if } q \text{ is odd.} \end{cases}$$

Coinduced modules.

Definition 9.3.12. Let H be a subgroup of G, and B a $\mathbb{Z}[H]$-module. We define a $\mathbb{Z}[G]$-module

$$\mathrm{M}_H^G(B) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B),$$

where the G-action is defined by letting $gf\colon \mathbb{Z}[G] \to B$ be the map given by $x \mapsto f(xg)$, when $g \in G$ and $f\colon \mathbb{Z}[G] \to B$.

Equivalently, one may think of $\mathrm{M}_H^G(B)$ as the set of maps $f\colon G \to B$ such that $f(hx) = hf(x)$ for all $h \in H$ and $x \in G$, with the group structure given by pointwise operations on B, and the G-action given by $(gf)(x) = f(xg)$ for $g, x \in G$.

Example 9.3.13. Assume that G is finite, and let S be the split Galois G-algebra of Example 5.5.8 over the field k. Then $S \simeq \mathrm{M}_1^G(k)$ as $\mathbb{Z}[G]$-modules. Moreover, a map $G \to k$ is invertible in S if and only if it takes values in $k^\times$. Thus $S^\times \simeq \mathrm{M}_1^G(k^\times)$ as $\mathbb{Z}[G]$-modules.

Let H be a subgroup of G, and B a $\mathbb{Z}[H]$-module. We consider the morphism of $\mathbb{Z}[H]$-modules

$$\rho\colon \mathrm{M}_H^G(B) \to B \quad ; \quad f \mapsto f(1).$$

Lemma 9.3.14. *Let H be a subgroup of G. Let A be a $\mathbb{Z}[G]$-module and B a $\mathbb{Z}[H]$-module. Then the morphism of abelian groups*

$$\mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{M}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(A, B) \quad ; \quad f \mapsto \rho \circ f$$

is bijective.

Proof. Let us construct the inverse morphism. Let $\varphi\colon A \to B$ be a morphism of $\mathbb{Z}[H]$-modules. Consider the map $\psi\colon A \to \mathrm{M}_H^G(B)$ sending $a \in A$ to the morphism of $\mathbb{Z}[H]$-modules $\mathbb{Z}[G] \to B$ given by $g \mapsto \varphi(ga)$. The map ψ is a morphism of $\mathbb{Z}[G]$-modules, so that $\varphi \mapsto \psi$ defines a morphism of abelian groups $\mathrm{Hom}_{\mathbb{Z}[H]}(A, B) \to \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{M}_H^G(B))$.

Clearly $\rho \circ \psi = \varphi$. Conversely, assume that $\varphi = \rho \circ f$ for some $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{M}_H^G(B))$. Then for any $a \in A$ and $g \in G$,

$$\psi(a)(g) = \varphi(ga) = \rho(f(ga)) = \rho(g(f(a))) = (g(f(a)))(1) = f(a)(g)$$

so that $\psi = f$. $\square$

Proposition 9.3.15 (Shapiro's Lemma). *Let H be a subgroup of G and B a $\mathbb{Z}[H]$-module. Then the composite*

$$H^q(G, \mathrm{M}_H^G(B)) \xrightarrow{\mathrm{Res}_H^G} H^q(H, \mathrm{M}_H^G(B)) \xrightarrow{\rho_*} H^q(H, B)$$

is bijective, for every $q \geq 0$.

Proof. The $\mathbb{Z}[H]$-module $\mathbb{Z}[G]$ is free, a basis being given by (the elements corresponding to) a set of representatives of G/H. It follows from Proposition 9.1.3 that any projective $\mathbb{Z}[G]$-module is also projective as a $\mathbb{Z}[H]$-module. Thus if P is a projective resolution of the $\mathbb{Z}[G]$-module $\mathbb{Z}$, it is also a projective resolution of the $\mathbb{Z}[H]$-module $\mathbb{Z}$. Lemma 9.3.14 shows that that morphism of complexes of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P, \mathrm{M}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(P, \mathrm{M}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(P, B)$$

is an isomorphism, and the result follows by passing to cohomology. $\square$

COROLLARY 9.3.16. *Let B be an abelian group. Then $H^q(G, \mathrm{M}_1^G(B)) = 0$ for $q > 0$.*

PROOF. This follows from Remark 9.3.2 and Proposition 9.3.15. □

Now assume that $H \subset G$ is a subgroup of finite index, and let A be a $\mathbb{Z}[G]$-module. Let $f \in \mathrm{M}_H^G(A)$. If $X \subset G$ is a set of representatives of G/H, consider the element

$$u = \sum_{x \in X} x f(x^{-1}) \in A. \tag{9.3.b}$$

From the fact that f is a morphism of $\mathbb{Z}[H]$-modules follows that u does not depend on the choice of the set of representatives $X \subset G$. If $g \in G$, then

$$\sum_{x \in X} x(gf)(x^{-1}) = \sum_{x \in X} x f(x^{-1}g) = g \sum_{y \in g^{-1}X} y f(y^{-1}) = gu,$$

since $g^{-1}X \subset G$ is again a set of representatives of G/H. We have thus defined a morphism of $\mathbb{Z}[G]$-modules

$$\mu\colon \mathrm{M}_H^G(A) \to A \quad ; \quad f \mapsto u \tag{9.3.c}$$

which using Proposition 9.3.15 induces the *corestriction morphisms* for all q

$$\mathrm{Cores}_H^G\colon H^q(H, A) = H^q(G, \mathrm{M}_H^G(A)) \xrightarrow{\mu_*} H^q(G, A).$$

PROPOSITION 9.3.17. *Let H be a subgroup of finite index in G. Let A be a $\mathbb{Z}[G]$-module. Then the composite*

$$H^q(G, A) \xrightarrow{\mathrm{Res}_H^G} H^q(H, A) \xrightarrow{\mathrm{Cores}_H^G} H^q(G, A)$$

coincides with multiplication by $[G : H]$, for every $q \geq 0$.

PROOF. Consider the morphism of $\mathbb{Z}[G]$-modules

$$\sigma\colon A \to \mathrm{M}_H^G(A)$$

sending $a \in A$ to the map $G \to A$ given by $g \mapsto ga$. Since $\rho \circ \sigma$ is the identity of the $\mathbb{Z}[H]$-module A, it follows from Proposition 9.3.15 that the induced morphism

$$H^q(G, A) \xrightarrow{\sigma_*} H^q(G, \mathrm{M}_H^G(A)) = H^q(H, A)$$

coincides with Res_H^G. Now it follows from the formula (9.3.b) that the composite

$$A \xrightarrow{\sigma} \mathrm{M}_H^G(A) \xrightarrow{\mu} A$$

is multiplication by $[G : H]$. □

COROLLARY 9.3.18. *Let H be a subgroup of finite index in G and A a $\mathbb{Z}[G]$-module. If the morphism $A \to A$ given by multiplication by $[G : H]$ is bijective, then the maps $\mathrm{Res}_H^G\colon H^q(G, A) \to H^q(H, A)$ are injective for all $q \geq 0$.*

PROOF. Denote by $f\colon A \to A$ the morphism given by multiplication by $[G : H]$. Then the morphisms $H^q(G, A) \to H^q(G, A)$ given by $(f^{-1})_*$ and f_* are mutually inverse. Since the morphism f_* is given by multiplication by $[G : H]$ in $H^q(G, A)$, it follows from Proposition 9.3.17 that Res_H^G must be injective. □

COROLLARY 9.3.19. *If G is finite, then the morphisms $H^q(G, A) \to H^q(G, A)$ given by multiplication by $|G|$ are zero for all $q > 0$.*

Proof. By Proposition 9.3.17 multiplication by $|G|$ in $H^q(G,A)$ factors through $H^q(1,A)$, which vanishes when $q>0$ by Remark 9.3.2. □

4. Cohomology of profinite groups

Direct limits. We now discuss the notion of direct limit, which is in a sense dual to the notion of inverse limit introduced in §4.1. Here we will limit ourselves to the case of abelian groups.

Definition 9.4.1. Let $(\mathcal{A},\leq)$ be a directed set (Definition 4.1.1). A *direct system* of abelian groups (indexed by $\mathcal{A}$) is the data of:

— for each $\alpha\in\mathcal{A}$ an abelian group E_α,

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

These data must satisfy the following conditions:

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

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

Definition 9.4.2. The *direct limit* of a direct system of abelian groups $(E_\alpha,f_{\alpha\beta})$ is defined as

$$E=\varinjlim E_\alpha=\Big(\bigoplus_{\alpha\in\mathcal{A}}E_\alpha\Big)/F$$

where F is the subgroup generated by the elements $x-f_{\alpha\beta}(x)$, for $x\in E_\alpha$ and $\alpha\leq\beta$ in $\mathcal{A}$.

The direct limit E is equipped with group morphisms $\iota_\alpha\colon E_\alpha\to E$ for every $\alpha\in\mathcal{A}$, such that $\iota_\beta\circ f_{\alpha\beta}=\iota_\alpha$ for all $\alpha\leq\beta$ in $\mathcal{A}$. It enjoys the following universal property: if $s_\alpha\colon E_\alpha\to S$ for $\alpha\in\mathcal{A}$ is a collection of group morphisms satisfying $s_\beta\circ f_{\alpha\beta}=s_\alpha$ for all $\alpha\leq\beta$ in $\mathcal{A}$, then there is a unique map $s\colon E\to S$ such that $s_\alpha=s\circ\iota_\alpha$ for all $\alpha\in\mathcal{A}$.

Lemma 9.4.3. *Let (E_α) be a direct system of abelian groups indexed by the directed set $\mathcal{A}$, and let E its direct limit.*

(i) We have $E=\bigcup_{\alpha\in\mathcal{A}}\iota_\alpha(E_\alpha)$.

(ii) For all $\alpha\in\mathcal{A}$ we have $\ker\iota_\alpha=\bigcup_{\alpha\leq\beta}\ker f_{\alpha\beta}$.

Proof. (i) : By construction, any element $e\in E$ may be written as $\iota_{\alpha_1}(e_1)+\cdots+\iota_{\alpha_n}(e_n)$ for some $\alpha_i\in\mathcal{A}$ and $e_i\in E_{\alpha_i}$ for $i=1,\dots,n$. As $\mathcal{A}$ is directed, we may find $\alpha\in\mathcal{A}$ such that $\alpha_i\leq\alpha$ for all $i=1,\dots,n$. Then

$$e=\iota_{\alpha_1}(e_1)+\cdots+\iota_{\alpha_n}(e_n)=\iota_\alpha(f_{\alpha_1\alpha}(e_1)+\cdots+f_{\alpha_n\alpha}(e_n))$$

belongs to $\iota_\alpha(E_\alpha)$.

(ii) : Certainly $\ker f_{\alpha\beta}\subset\ker\iota_\alpha$ for all $\alpha\leq\beta$ in $\mathcal{A}$. Conversely, let $x\in\ker\iota_\alpha$. Then we may find indices $\alpha_i\leq\beta_i$ in $\mathcal{A}$ and elements $x_i\in E_{\alpha_i}$ for $i=1,\dots,n$ such that

$$x=\sum_{i=1}^n(x_i-f_{\alpha_i\beta_i}(x_i))\in\bigoplus_{\gamma\in\mathcal{A}}E_\gamma. \tag{9.4.a}$$

Pick $\beta\in\mathcal{A}$ such that $\alpha\leq\beta$ and $\beta_i\leq\beta$ for all $i=1,\dots,n$. The morphisms $f_{\gamma\beta}$ for $\gamma\leq\beta$ in $\mathcal{A}$ define a morphism $\varphi_\beta\colon\bigoplus_{\gamma\leq\beta}E_\gamma\to E_\beta$. Taking the image of (9.4.a) under

φ_β yields

$$f_{\alpha\beta}(x) = \sum_{i=1}^{n} (f_{\alpha_i\beta}(x_i) - f_{\beta_i\beta} \circ f_{\alpha_i\beta_i}(x_i)) = 0. \qquad \square$$

Example 9.4.4. Let A be an abelian group. Let $(\mathcal{A}, \leq)$ be a directed set, and $A_\alpha \subset A$ a collection of subgroups such that $A_\alpha \subset A_\beta$ whenever $\alpha \leq \beta$. Then the family A_α defines a direct system, where the transition morphisms are the inclusions $A_\alpha \subset A_\beta$. It follows from Lemma 9.4.3 that the natural group morphism $\varinjlim A_\alpha \to A$ is injective, and its image coincides with $\bigcup_{\alpha\in\mathcal{A}} A_\alpha$.

Observe that if $(E_\alpha), (E'_\alpha)$ are direct systems of abelian groups indexed by the same directed set $\mathcal{A}$, and $E'_\alpha \to E_\alpha$ for all $\alpha \in \mathcal{A}$ are group morphisms compatible with the transition maps, there is a unique group morphism $\varinjlim E'_\alpha \to \varinjlim E_\alpha$ compatible with the morphisms ι_α.

Proposition 9.4.5. *Let $\mathcal{A}$ be a directed set, and $(E_\alpha), (E'_\alpha), (E''_\alpha)$ direct systems of abelian groups indexed by $\mathcal{A}$. Assume given exact sequence of groups*

$$E'_\alpha \to E_\alpha \to E''_\alpha$$

for all $\alpha \in \mathcal{A}$, compatibly with the transition morphisms. Then the induced sequence

$$\varinjlim E'_\alpha \to \varinjlim E_\alpha \to \varinjlim E''_\alpha$$

is exact.

Proof. By Lemma 9.4.3 (i), every element $x \in \varinjlim E_\alpha$ is represented by $e \in E_\alpha$ for some $\alpha \in \mathcal{A}$. Let $e'' \in E''_\alpha$ be the image of e. If the image of x in $\varinjlim E''_\alpha$ vanishes, then by Lemma 9.4.3 (ii) there exists $\beta \geq \alpha$ in $\mathcal{A}$ such that the image of e'' vanishes in E''_β, which implies that the image of e in E_β is the image of an element $e' \in E'_\beta$, by the assumption of exactness. The image of e' in $\varinjlim E'_\alpha$ defines the required preimage of x. $\square$

Let now C_α be a cochain complex of abelian groups for each $\alpha \in \mathcal{A}$, where $\mathcal{A}$ is a directed set. Assume given for each $\alpha \leq \beta$ in $\mathcal{A}$ a morphism of complexes $f_{\alpha\beta} \colon C_\alpha \to C_\beta$, such that $f_{\alpha\alpha} = \mathrm{id}_{C_\alpha}$ for all $\alpha \in \mathcal{A}$, and $f_{\beta\gamma} \circ f_{\alpha\beta} = f_{\alpha\gamma}$ for all $\alpha \leq \beta \leq \gamma$ in $\mathcal{A}$. Then for each $n \in \mathbb{Z}$ the collection (C^n_α) is an inverse system of abelian groups indexed by $\mathcal{A}$, and we may define a cochain complex of abelian groups C by setting $C^n = \varinjlim C^n_\alpha$ and $d^n_C = \varinjlim d^n_{C_\alpha}$ for each $n \in \mathbb{Z}$. There are natural morphisms of complexes of abelian groups $C_\alpha \to C$ for all $\alpha \in \mathcal{A}$.

Corollary 9.4.6. *Let $n \in \mathbb{Z}$. In the above situation, the induced morphisms $H^n(C_\alpha) \to H^n(C)$ yield an isomorphism of abelian groups*

$$\varinjlim H^n(C_\alpha) \to H^n(C).$$

Proof. Consider the subgroups of C^n

$$Z^n = \ker d^n_C \quad ; \quad B^n = \operatorname{im} d^{n-1}_C$$

as well as the subgroups of C_α, for $\alpha \in \mathcal{A}$,

$$Z^n_\alpha = \ker d^n_{C_\alpha} \quad ; \quad B^n_\alpha = \operatorname{im} d^{n-1}_{C_\alpha}.$$

Proposition 9.4.5 shows that the morphism $\varinjlim Z^n_\alpha \to C^n$ induces an isomorphism $\varinjlim Z^n_\alpha \to Z^n$. The morphism $d^{n-1}_{C_\alpha}$ factors as $C^{n-1}_\alpha \to B^n_\alpha \to C^n_\alpha$, hence d^{n-1}_C factors a $C^{n-1} \to \varinjlim B^n_\alpha \to C^n$. By Proposition 9.4.5 the morphism $C^{n-1} \to \varinjlim B^n_\alpha$ is surjective, and the morphism $\varinjlim B^n_\alpha \to C^n$ is injective. It follows that the morphism $\varinjlim B^n_\alpha \to C^n$ induces an isomorphism $\varinjlim B^n_\alpha \to B^n$. We thus obtain a commutative diagram of abelian groups

$$\begin{tikzcd}
0 \arrow[r] & \varinjlim B^n_\alpha \arrow[r] \arrow[d] & \varinjlim Z^n_\alpha \arrow[r] \arrow[d] & \varinjlim H^n(C_\alpha) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B^n \arrow[r] & Z^n \arrow[r] & H^n(C) \arrow[r] & 0
\end{tikzcd}$$

where the left and middle vertical arrows are isomorphisms. The lower row is exact by definition of the cohomology groups, and the upper row is exact by Proposition 9.4.5. It follows from a diagram chase (the "5-lemma") that the right vertical arrow is an isomorphism, proving the corollary. □

Continuous cohomology. We now fix a profinite group Γ. Let A be a discrete Γ-module.

DEFINITION 9.4.7. Let $n \in \mathbb{N}$. Let $C^n(\Gamma, A)$ be the group of maps $\Gamma^n \to A$ which are continuous for the discrete topology on A. Denoting by Γ_{dis} be the group Γ endowed with the discrete topology, we may view $C^n(\Gamma, A)$ as a subgroup of $C^n(\Gamma_{\text{dis}}, A)$ (the group of all maps $\Gamma^n \to A$). The morphism $d^n \colon C^n(\Gamma_{\text{dis}}, A) \to C^{n+1}(\Gamma_{\text{dis}}, A)$ (see (9.3.a)) maps $C^n(\Gamma, A)$ into $C^{n+1}(\Gamma, A)$. We have thus constructed a cochain complex of abelian groups $C(\Gamma, A)$, and we denote by $H^n(\Gamma, A)$ its cohomology groups.

REMARK 9.4.8. As observed in Example 9.3.8 and Example 9.3.9, we recover the cohomology groups previously defined for $n = 0, 1, 2$.

PROPOSITION 9.4.9. *An exact sequence of discrete* Γ*-modules*

$$0 \to A \to B \to C \to 0$$

induces an exact sequence of abelian groups

$$\cdots \to H^{q-1}(\Gamma, C) \to H^q(\Gamma, A) \to H^q(\Gamma, B) \to H^q(\Gamma, C) \to \cdots$$

Given a commutative diagram of discrete Γ*-modules*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

having exact rows, the induced diagram of abelian groups

$$\begin{tikzcd}
\cdots \arrow[r] & H^{q-1}(\Gamma, C) \arrow[r] \arrow[d] & H^q(\Gamma, A) \arrow[r] \arrow[d] & H^q(\Gamma, B) \arrow[r] \arrow[d] & H^q(\Gamma, C) \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & H^{q-1}(\Gamma, C') \arrow[r] & H^q(\Gamma, A') \arrow[r] & H^q(\Gamma, B') \arrow[r] & H^q(\Gamma, C') \arrow[r] & \cdots
\end{tikzcd}$$

is commutative.

Proof. This will follow from Proposition 9.2.6 once we have proved that the sequences of cochain complexes

$$0 \to C^n(\Gamma, A) \to C^n(\Gamma, B) \to C^n(\Gamma, C) \to 0$$

are exact. The only nontrivial point is the surjectivity of the last morphism. To prove this, choose a map (not a group morphism!) $C \to B$ such that the composite $C \to B \to C$ is the identity. This map is continuous for the discrete topologies (as is any map), hence induces a map $C^n(\Gamma, C) \to C^n(\Gamma, B)$ such that the composite $C^n(\Gamma, C) \to C^n(\Gamma, B) \to C^n(\Gamma, C)$ is the identity. This concludes the proof. $\square$

Proposition 9.4.10. *Let $\mathcal{A}$ be a directed set, and U_α for $\alpha \in \mathcal{A}$ an inverse system of open normal subgroups of Γ (where transition maps are the inclusions). Assume that each open normal subgroup of Γ contains U_α for some $\alpha \in \mathcal{A}$. Let A be a discrete Γ-module, and for each $\alpha \in \mathcal{A}$ let $A_\alpha \subset A^{U_\alpha}$ be a discrete Γ-submodule. Assume that $A_\alpha \subset A_\beta$ for each $\alpha \le \beta$ in $\mathcal{A}$, and that $A = \bigcup_{\alpha \in \mathcal{A}} A_\alpha$.*

Then there are natural identifications

$$\varinjlim C^n(\Gamma/U_\alpha, A_\alpha) = C^n(\Gamma, A) \quad \text{and} \quad \varinjlim H^n(\Gamma/U_\alpha, A_\alpha) = H^n(\Gamma, A).$$

Proof. We may view $C^n(\Gamma/U_\alpha, A_\alpha)$ as a subgroup of $C^n(\Gamma_{\mathrm{dis}}, A)$, and identify $\varinjlim C^n(\Gamma/U_\alpha, A_\alpha)$ with $\bigcup_\alpha C^n(\Gamma/U_\alpha, A_\alpha)$ (Example 9.4.4). By Lemma 4.2.14, every $f \in C^n(\Gamma, A)$ lies in $C^n(\Gamma/U_\beta, A^{U_\beta})$ for some $\beta \in \mathcal{A}$. Since the image of f is finite (because Γ/U_β is finite), it is contained in A_α for some $\beta \le \alpha$. This proves that $\bigcup_\alpha C^n(\Gamma/U_\alpha, A_\alpha) = C^n(\Gamma, A)$, so that $\varinjlim C^n(\Gamma/U_\alpha, A_\alpha) = C^n(\Gamma, A)$. Since this identification is compatible with the coboundary morphisms, we may conclude using Corollary 9.4.6. $\square$

Let $H \subset \Gamma$ be a closed subgroup and A a discrete Γ-module. The natural morphisms $C^q(\Gamma, A) \to C^q(H, A)$ are compatible with the coboundary morphisms, hence induce morphisms in cohomology, for every $q \ge 0$

$$\operatorname{Res}^\Gamma_H \colon H^q(\Gamma, A) \to H^q(H, A).$$

Observe that every open normal subgroup of H contains a subgroup of the form $U \cap H$, where U is an open normal subgroup of Γ (this follows from Lemma 4.2.5 (i)). Thus it follows from Proposition 9.4.10 that $\operatorname{Res}^\Gamma_H \colon H^q(\Gamma, A) \to H^q(H, A)$ may be identified with the direct limit of the morphisms

$$\operatorname{Res}^{\Gamma/U}_{H/(U\cap H)} \colon H^q(\Gamma/U, A^U) \to H^q(H/(U \cap H), A^U), \tag{9.4.b}$$

where U runs over the open normal subgroups of Γ.

Proposition 9.4.11. *Let $H \subset \Gamma$ be a closed subgroup and A a discrete Γ-module. Assume that for each open normal subgroup U of Γ, the map $A^U \to A^U$ given by multiplication by $[\Gamma/U : H/(U \cap H)]$ is bijective. Then the morphism $\operatorname{Res}^\Gamma_H \colon H^q(\Gamma, A) \to H^q(H, A)$ is injective for every q.*

Proof. Since each morphism (9.4.b) is injective by Corollary 9.3.18, the statement follows from Proposition 9.4.5 (in view of observation just above). $\square$

Let now B be a H-module. We let $\mathrm{M}^\Gamma_H(B)$ be the set of continuous maps $f \colon \Gamma \to B$ such that $f(hx) = hf(x)$ for all $h \in H$ and $x \in \Gamma$, with the group structure given by pointwise operations on B, and the Γ-action given by $(gf)(x) = f(xg)$ for $g, x \in \Gamma$. Every element $f \in \mathrm{M}_H^\Gamma(B)$ factors as $\Gamma/U \to B$ for some normal open subgroup U of Γ (see Lemma 4.2.14), hence is fixed by U. We have thus constructed a discrete Γ-module $\mathrm{M}_H^\Gamma(B)$. Observe that $\mathrm{M}_H^\Gamma(B)$ is naturally a Γ_{dis}-submodule of $\mathrm{M}_{H_{\mathrm{dis}}}^{\Gamma_{\mathrm{dis}}}(B)$. We define a morphism of H-modules

$$\rho\colon \mathrm{M}_H^\Gamma(B) \to B \quad ; \quad f \mapsto f(1).$$

Proposition 9.4.12 (Shapiro's Lemma — profinite version). *Let $H \subset \Gamma$ be a closed subgroup and B a H-module. Then for every q the composite*

$$H^q(\Gamma, \mathrm{M}_H^\Gamma(B)) \xrightarrow{\mathrm{Res}_H^\Gamma} H^q(H, \mathrm{M}_H^\Gamma(B)) \xrightarrow{\rho_*} H^q(H, B)$$

is bijective.

Proof. Let U be an open normal subgroup of Γ, and let $f \in \mathrm{M}_H^\Gamma(B)$. Then $f \in \mathrm{M}_H^\Gamma(B)^U$ if and only if $f\colon \Gamma \to B$ factors through the quotient Γ/U. Assume that $f \in \mathrm{M}_H^\Gamma(B)^U$, and set $V = U \cap H$. For any $u \in V$ and $x \in \Gamma$ we have $v = x^{-1}ux \in U$, hence

$$f(x) = (vf)(x) = f(ux) = uf(x),$$

proving that the image of f is contained in B^V. This yields an identification, as Γ/U-modules

$$\mathrm{M}_{H/V}^{\Gamma/U}(B^V) = \mathrm{M}_H^\Gamma(B)^U.$$

We may thus view the morphism $\rho\colon \mathrm{M}_H^\Gamma(B) \to B$ as the direct limit of the morphisms $\rho\colon \mathrm{M}_{H/V}^{\Gamma/U}(B^V) \to B^V$ considered in §9.3. Now each composite

$$H^q(\Gamma/U, \mathrm{M}_{H/V}^{\Gamma/U}(B^V)) \xrightarrow{\mathrm{Res}_{H/V}^{\Gamma/U}} H^q(H/V, \mathrm{M}_{H/V}^{\Gamma/U}(B^V)) \xrightarrow{\rho_*} H^q(H/V, B^V)$$

is an isomorphism by Proposition 9.3.15, and the statement follows by passing to the limit, in view of Proposition 9.4.10. □

Assume now that $H \subset \Gamma$ is an open subgroup, and let A be a discrete Γ-module. We define a map

$$\mu\colon \mathrm{M}_H^\Gamma(A) \to A \quad ; \quad f \mapsto \sum_{x \in X} xf(x^{-1}), \tag{9.4.c}$$

where $X \subset \Gamma$ is a set of representatives of Γ/H. We show as before (see just below the formula (9.3.b)) that μ is a morphism of discrete Γ-modules which does not depend on the choice of X. Alternatively, we may deduce these facts from §9.3, since the map μ above factors as $\mathrm{M}_H^\Gamma(A) \subset \mathrm{M}_{H_{\mathrm{dis}}}^{\Gamma_{\mathrm{dis}}}(A) \to A$, where the last map is the morphism of Γ_{dis}-modules μ defined in (9.3.c). Using Proposition 9.4.12 we obtain for each q the *corestriction morphism*

$$\mathrm{Cores}_H^\Gamma\colon H^q(H, A) = H^q(\Gamma, \mathrm{M}_H^\Gamma(A)) \xrightarrow{\mu_*} H^q(\Gamma, A).$$

Proposition 9.4.13. *Let H be an open subgroup of Γ and A a discrete Γ-module. Then for every q the composite*

$$H^q(\Gamma, A) \xrightarrow{\mathrm{Res}_H^\Gamma} H^q(H, A) \xrightarrow{\mathrm{Cores}_H^\Gamma} H^q(\Gamma, A)$$

coincides with multiplication by $[\Gamma : H]$.

Proof. Consider the morphism of discrete Γ-modules $\sigma\colon A \to \mathrm{M}_H^\Gamma(A)$ sending $a \in A$ to the map $\Gamma \to A$ given by $\gamma \mapsto \gamma a$. Since $\rho \circ \sigma$ is the identity of the discrete H-module A, it follows from Proposition 9.4.12 that the induced morphism

$$H^q(\Gamma, A) \xrightarrow{\sigma_*} H^q(\Gamma, \mathrm{M}_H^\Gamma(A)) = H^q(H, A)$$

coincides with Res_H^Γ. Now it follows from the formula (9.4.c) that the composite

$$A \xrightarrow{\sigma} \mathrm{M}_H^\Gamma(A) \xrightarrow{\mu} A$$

is multiplication by $[\Gamma : H]$. □

CHAPTER 10

Cohomological dimension

In the final chapter, we apply the homological methods of the previous chapter. We first finish the proof of the identification of the Brauer group with the second cohomology of $\mathbb{G}_m$, using Shapiro's Lemma. We deduce the existence of corestriction morphisms (sometimes called transfer maps) for Brauer groups. When L/k is a finite separable extension, this morphism associates to each finite-dimensional central simple L-algebra a central division k-algebra.

Next we briefly discuss the notions of cohomological dimension of a profinite group, and of a field. This concept encodes the complexity of a field from a certain cohomological point of view. The first interesting case is that of fields of cohomological dimension at most one. We provide several characterisation of such fields, including the fact that the Brauer group of every of its separable extension vanishes.

The source of most classical examples of such fields are the so-called C_1-fields, also called "quasi-algebraically closed fields". We prove that C_1-fields have cohomological dimension at most one (the converse does not hold, but seeing this requires some work). Finite fields are C_1-fields by Chevalley-Warning's Theorem, which provides another reason for the commutativity of finite division rings (Wedderburn's Theorem proved earlier). The chapter ends with a proof of Tsen's Theorem (assuming basic algebraic geometry), which asserts that fields of transcendence degree one over an algebraically closed field are C_1-fields, providing another interesting example of vanishing of Brauer groups. The third important examples of C_1-fields, which will not be discussed, are the complete discretely valued fields with algebraically closed residue fields, for instance power series fields over an algebraically closed field.

1. The Brauer group, III

LEMMA 10.1.1. *Let L/k be a finite Galois extension of degree n, and set $G = \mathrm{Gal}(L/k)$. Then the connecting morphism of pointed sets*

$$H^1(G, \mathrm{PGL}_n(L)) \to H^2(G, L^\times)$$

arising from the sequence (7.3.a) *is bijective.*

PROOF. As in Lemma 8.2.1, injectivity follows from the vanishing of $H^1(G, \mathrm{GL}_n(L))$ by Hilbert's Theorem 90 (Proposition 7.1.1). Let us denote by K the field L equipped with the trivial G-action. Sending an element of $a \in K_L$ to the endomorphism $x \mapsto ax$ of K_L yields an injective morphism of L-algebras $K_L \to \mathrm{End}_L(K_L)$. Choosing a basis of K, we thus view K_L as an L-subalgebra of $M_n(L)$. This yields a commutative diagram of G-groups, having exact rows

$$\begin{tikzcd} 1 \arrow[r] & L^\times \arrow[r] \arrow[d, "="] & (K_L)^\times \arrow[r] \arrow[d] & (K_L)^\times/L^\times \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & L^\times \arrow[r] & \mathrm{GL}_n(L) \arrow[r] & \mathrm{PGL}_n(L) \arrow[r] & 1 \end{tikzcd}$$

and thus by Proposition 8.1.2 and Corollary 8.1.3 a commutative diagram of pointed sets, where the upper row is exact

$$\begin{tikzcd} H^1(G,(K_L)^\times/L^\times) \arrow[r] \arrow[d] & H^2(G,L^\times) \arrow[r] \arrow[d, "="] & H^2(G,(K_L)^\times) \\ H^1(G,\mathrm{PGL}_n(L)) \arrow[r] & H^2(G,L^\times) & \end{tikzcd} \tag{10.1.a}$$

Now, we may view $K_L = L_K$ as a Galois G-algebra over K, which is split by Corollary 5.5.13. It follows from Example 9.3.13 that $(L_K)^\times \simeq \mathrm{M}_1^G(K^\times)$ as $\mathbb{Z}[G]$-modules, hence by Shapiro's Lemma (Corollary 9.3.16), we have

$$H^2(G,(K_L)^\times) = H^2(G,(L_K)^\times) = 1.$$

In view of the diagram (10.1.a), we deduce that the map $H^1(G,\mathrm{PGL}_n(L)) \to H^2(G,L^\times)$ is surjective. □

Proposition 10.1.2. *The morphism of Proposition 8.2.3 is a group isomorphism*

$$\mathrm{Br}(k) \simeq H^2(k,\mathbb{G}_m).$$

Proof. Injectivity has been proved in Proposition 8.2.3. By Lemma 4.2.14, every 2-cocycle $\mathrm{Gal}(k_s/k) \times \mathrm{Gal}(k_s/k) \to k_s^\times$ factors as a 2-cocyle $\alpha\colon \mathrm{Gal}(L/k) \times \mathrm{Gal}(L/k) \to (k_s^\times)^{\mathrm{Gal}(k_s/L)} = L^\times$, where L/k is a finite Galois extension. Let $n = [L:k]$ and $G = \mathrm{Gal}(L/k)$. By Lemma 10.1.1, the class of α in $H^2(G,L^\times)$ admits a preimage in $H^1(G,\mathrm{PGL}_n(L))$, whose image in $H^1(k,\mathrm{PGL}_n)$ is the required preimage of the class of the original 2-cocyle in $H^2(k,\mathbb{G}_m)$ (here we have used Remark 9.3.10). □

Corollary 10.1.3. *If n is an integer prime to the characteristic of k, then the kernel of the morphism* $\mathrm{Br}(k) \to \mathrm{Br}(k)$ *given by multiplication by n is isomorphic to* $H^2(k,\mu_n)$.

Proof. The exact sequence of Lemma 7.1.4 yields an exact sequence of pointed sets

$$H^1(k,\mathbb{G}_m) \to H^2(k,\mu_n) \to H^2(k,\mathbb{G}_m) \xrightarrow{n} H^2(k,\mathbb{G}_m).$$

Since $H^1(k,\mathbb{G}_m) = \{*\}$ by Hilbert's Theorem 90 (Proposition 7.1.1), the statement follows from the identification of Proposition 10.1.2. □

Let L/k be a finite separable extension. The morphism

$$\mathrm{Cores}_{\mathrm{Gal}(k_s/L)}^{\mathrm{Gal}(k_s/k)}\colon H^2(\mathrm{Gal}(k_s/L),k_s^\times) \to H^2(\mathrm{Gal}(k_s/k),k_s^\times)$$

yields, in view of Proposition 10.1.2, a group morphism

$$\mathrm{Cores}_{L/k}\colon \mathrm{Br}(L) \to \mathrm{Br}(k).$$

PROPOSITION 10.1.4. *Let L/k be a finite separable extension. Then the composite*

$$\mathrm{Br}(k) \to \mathrm{Br}(L) \xrightarrow{\mathrm{Cores}_{L/k}} \mathrm{Br}(k)$$

is multiplication by $[L : k]$.

PROOF. This follows from Proposition 9.4.13. $\square$

REMARK 10.1.5. Proposition 10.1.4 yields a new proof of Theorem 8.3.1. Indeed by Corollary 3.3.4, we find a separable extension L/k of degree $\mathrm{ind}(A)$ splitting A, so that $\mathrm{ind}(A) \cdot [A] = [L : k] \cdot [A] = \mathrm{Cores}_{L/k}([A_L]) = 0$ by Proposition 10.1.4.

2. Cohomological dimension

In this section we fix a profinite group Γ. Let p be a prime number. When A is an abelian group, let us denote by $A\{p\} \subset A$ the subgroup of those $a \in A$ such that $p^n a = 0$ for some integer n. We say that A is *of p-primary torsion* if $A\{p\} = A$, and that A *has no p-primary torsion* if $A\{p\} = 0$. We say that a discrete Γ-module is of p-primary torsion if the underlying abelian group is so.

DEFINITION 10.2.1. We define the *p-cohomological dimension* of Γ as

$$\inf\{n \in \mathbb{N} | H^q(\Gamma, A) = 0 \text{ for all } q > n \text{ and discrete } \Gamma\text{-modules } A \text{ of } p\text{-primary torsion}\},$$

and denoted by $\mathrm{cd}_p(\Gamma) \in \mathbb{N} \cup \{\infty\}$. The *cohomological dimension* of Γ, denoted by $\mathrm{cd}(\Gamma) \in \mathbb{N} \cup \{\infty\}$, is defined as the supremum of the p-cohomological dimensions of Γ, where p runs over the prime numbers.

Observe that

$$\mathrm{cd}_p(\Gamma) = \sup\{q \in \mathbb{N} | H^q(\Gamma, A) \neq 0 \text{ for some discrete } \Gamma\text{-module } A \text{ of } p\text{-primary torsion}\}.$$

LEMMA 10.2.2. *Let $H \subset \Gamma$ be a closed subgroup, and B a discrete H-module. If B is of p-primary torsion, so is $\mathrm{M}_H^\Gamma(B)$.*

PROOF. Every element $f \in \mathrm{M}_H^\Gamma(B)$ is a continuous map $\Gamma \to B$. The image $f(\Gamma)$ is compact by Proposition 4.1.9 and discrete (as B is so), hence finite. Therefore $f(\Gamma) \subset B$ is annihilated by some power of p, hence so is f. $\square$

LEMMA 10.2.3. *If $n \in \mathbb{N}$ is such that $H^{n+1}(\Gamma, A) = 0$ for all discrete Γ-modules A of p-primary torsion, then $\mathrm{cd}_p(\Gamma) \leq n$.*

PROOF. We prove that $H^q(\Gamma, A) = 0$ for all discrete Γ-modules A of p-primary torsion when $q > n$. We proceed by induction on q, the case $q = n + 1$ being the assumption. Let A be a discrete Γ-module of p-primary torsion. The map $\sigma \colon A \to \mathrm{M}_1^\Gamma(A)$ sending $a \in A$ to the map $\Gamma \to A$ given by $\gamma \mapsto \gamma a$ is an injective group morphism, allowing us to view A as a discrete Γ-submodule of $\mathrm{M}_1^\Gamma(A)$. Since the discrete Γ-module $\mathrm{M}_1^\Gamma(A)$ is of p-primary torsion (Lemma 10.2.2), so is its quotient $Q = \mathrm{M}_1^\Gamma(A)/A$. Part of the long exact sequence of Proposition 9.4.9 reads

$$H^{q-1}(\Gamma, Q) \to H^q(\Gamma, A) \to H^q(\Gamma, \mathrm{M}_1^\Gamma(A))$$

Since $H^q(\Gamma, \mathrm{M}_1^\Gamma(A)) = H^q(1, A) = 0$ by Shapiro's Lemma (Proposition 9.4.12), and $H^{q-1}(\Gamma, Q) = 0$ by induction, we conclude that $H^q(\Gamma, A) = 0$, as required. $\square$

Lemma 10.2.4. *Let Γ be a pro-p-group and A a discrete Γ-module of p-primary torsion. If $A \neq 0$, then A admits a discrete Γ-submodule isomorphic to $\mathbb{Z}/p$ with trivial Γ-action.*

Proof. Let a be a nonzero element of A, and U an open normal subgroup of Γ acting trivially on a. The set $E = \{\gamma a, \gamma \in \Gamma\}$ is finite, since it admits a transitive action of the finite group Γ/U. The subgroup $B \subset A$ generated by E is a discrete Γ-submodule, and the Γ-action on B factors through the finite quotient $G = \Gamma/U$. The assumption that A is of p-primary torsion implies that B is finite and that $|B|$ is a power of p. Since G is a finite p-group and $B \neq 0$, it follows that $B^G \neq 0$ (otherwise B would be the disjoint union of $\{0\}$ and nontrivial orbits of the p-group G, which have cardinality divisible by p). Let b be a nonzero element of B^G, and n the smallest integer such that $p^n b = 0$. Then $p^{n-1}b$ generates a subgroup of B^G isomorphic to $\mathbb{Z}/p$, which is a discrete Γ-submodule of A having trivial Γ-action. $\square$

Lemma 10.2.5. *Let Γ be a pro-p-group. Consider $\mathbb{Z}/p$ as a discrete Γ-module with trivial action. If $n \in \mathbb{N}$ is such that $H^{n+1}(\Gamma, \mathbb{Z}/p) = 0$ then $\operatorname{cd}_p(\Gamma) \leq n$.*

Proof. Let A be a discrete Γ-module of p-primary torsion. By Lemma 10.2.3, it will suffice to prove that $H^{n+1}(\Gamma, A) = 0$. Assume that $H^{n+1}(\Gamma, A) \neq 0$. We order the set $\mathcal{S}$ of discrete Γ-submodules of A by inclusion. If (A_α) is a totally ordered subset of $\mathcal{S}$, then $B = \bigcup_\alpha A_\alpha$ is a discrete Γ-module, and we have by Proposition 9.4.10

$$H^{n+1}(\Gamma, B) = \varinjlim H^{n+1}(\Gamma, A_\alpha).$$

Thus if $H^{n+1}(\Gamma, A_\alpha) = 0$ for all α, we have $H^{n+1}(\Gamma, B) = 0$. Applying Zorn's lemma, we obtain a maximal discrete Γ-submodule B of A such that $H^{n+1}(\Gamma, B) = 0$. Then $A \neq B$. By Lemma 10.2.4, the discrete Γ-module A/B contains a discrete Γ-submodule isomorphic to $\mathbb{Z}/p$. This yields a discrete Γ-submodule C of A fitting into an exact sequence of discrete Γ-modules

$$0 \to B \to C \to \mathbb{Z}/p \to 0.$$

Part of the associated long exact sequence of Proposition 9.4.9 reads

$$H^{n+1}(\Gamma, B) \to H^{n+1}(\Gamma, C) \to H^{n+1}(\Gamma, \mathbb{Z}/p).$$

The extreme terms vanish, hence so does the middle one, contradicting the maximality of B. $\square$

Lemma 10.2.6. *Let $H \subset \Gamma$ be a closed subgroup.*

(i) We have $\operatorname{cd}_p(H) \leq \operatorname{cd}_p(\Gamma)$.
(ii) If for each open normal subgroup U of Γ, the index $[\Gamma/U : H/(U \cap H)]$ is prime to p, then $\operatorname{cd}_p(H) = \operatorname{cd}_p(\Gamma)$.

Proof. (i): Let B be a discrete H-module of p-primary torsion such that $H^q(H, B) \neq 0$. Then $C = \mathrm{M}_H^\Gamma(B)$ is a discrete Γ-module of p-primary torsion (Lemma 10.2.2) such that $H^q(\Gamma, C) \neq 0$ by Shapiro's Lemma (Proposition 9.4.12).

(ii): Let A be a discrete Γ-module of p-primary torsion such that $H^q(\Gamma, A) \neq 0$. It follows from Proposition 9.4.11 that $H^q(\Gamma, A) \to H^q(H, A)$ is injective, hence $H^q(\Gamma, A) \neq 0$. $\square$

The additive version of Hilbert's Theorem 90 (Proposition 7.2.1) admits a generalisation to cohomology groups of higher degrees, given just below. This contrasts with the usual (multiplicative) version of this theorem (Proposition 7.1.1), since already $H^2(k,\mathbb{G}_m)=\mathrm{Br}(k)$ can be nontrivial (Proposition 10.1.2).

PROPOSITION 10.2.7. *We have* $H^q(k,\mathbb{G}_a)=0$ *for all* $q\geq 1$.

PROOF. Let L/k be a finite Galois extension and $G=\mathrm{Gal}(L/k)$. Let K be the field L with trivial G-action. Then the Galois G-algebra L_K over K is split (Corollary 5.5.13), hence $L_K\simeq \mathrm{M}_1^G(K)$ as $\mathbb{Z}[G]$-modules (Example 9.3.13), so that $H^q(G,L_K)=0$ by Shapiro's Lemma (Corollary 9.3.16). Now the k-vector space k is a direct summand of K, hence the $\mathbb{Z}[G]$-module L is a direct summand of L_K. It follows that the group $H^q(G,L)$ is a direct summand of $H^q(G,L_K)=0$ (see Remark 9.3.5), hence vanishes. Passing to the limit over all such L yields the result. □

REMARK 10.2.8. The normal basis theorem asserts that, in fact, we have $L\simeq \mathrm{M}_1^G(k)$ as $\mathbb{Z}[G]$-module, when L/k is a finite Galois extension and $G=\mathrm{Gal}(L/k)$.

COROLLARY 10.2.9. *Let k be a field of characteristic $p>0$. Then* $\mathrm{cd}_p(\mathrm{Gal}(k_s/k))\leq 1$.

PROOF. Let P be a pro-p-Sylow subgroup of $\mathrm{Gal}(k_s/k)$ (see Proposition 4.2.10). Then $\mathrm{cd}_p(\mathrm{Gal}(k_s/k))=\mathrm{cd}_p(P)$ by Lemma 10.2.6 (ii). Replacing k with $(k_s)^P$, we may thus assume that $\mathrm{Gal}(k_s/k)$ is a pro-p-group.

The exact sequence of k-groups of Lemma 7.2.2 yields an exact sequence

$$H^1(k,\mathbb{G}_a)\to H^2(k,\mathbb{Z}/p)\to H^2(k,\mathbb{G}_a).$$

The extreme terms vanish by Proposition 10.2.7, hence so does the middle one, which proves the statement by Lemma 10.2.5. □

PROPOSITION 10.2.10. *Let p be a prime number. The following are equivalent.*

(i) For all separable field extensions K/k, the group $\mathrm{Br}(K)$ *has no p-primary torsion.*
(ii) The norm map $\mathrm{N}_{L/K}\colon L^\times\to K^\times$ *is surjective for all separable field extensions K/k and Galois extensions L/K such that* $[L:K]=p$.

If the characteristic of k is not equal to p, these conditions are equivalent to:

(iii) We have $\mathrm{cd}_p(\mathrm{Gal}(k_s/k))\leq 1$.

PROOF. (i) ⇒ (ii) : Let $Q=K^\times/\mathrm{N}_{L/K}(L^\times)$. We may view L as a Galois $\mathbb{Z}/p$-algebra over K (Example 5.5.7), so that Q injects into $\mathrm{Br}(K)$ by Proposition 7.4.11. Moreover we have $x^p=\mathrm{N}_{L/K}(x)$ for any $x\in K$, which implies that Q is of p-primary torsion. By (i) the group Q is trivial, which means that $\mathrm{N}_{L/K}\colon L^\times\to K^\times$ is surjective.

(ii) ⇒ (i) : We may assume that $K=k$. Let E/k be as in Lemma 4.3.16. Since every finite subextension of E/k has degree prime to p, it follows from Lemma 3.5.9 and Corollary 8.3.3 that for each element $x\in\mathrm{Br}(E/k)$ there exists an integer m prime to p such that $mx=0$. This implies that $\mathrm{Br}(E/k)$ has no p-primary torsion.

We now prove that $\mathrm{Br}(E)=0$, which will imply that $\mathrm{Br}(k)=\mathrm{Br}(E/k)$ has no p-primary torsion, as required. If $\mathrm{Br}(E)\neq 0$, there exists a finite Galois extension L/E such that $\mathrm{Br}(L/E)\neq 0$. Let us choose L/E minimal with this property, in the sense that $\mathrm{Br}(F/E)=0$ for all Galois subextensions F/E of L/E such that $F\neq L$. Since $\mathrm{Gal}(L/E)$ is a nontrivial finite p-group (by Lemma 4.3.16), it contains a normal subgroup H isomorphic to $\mathbb{Z}/p$. Then $F=L^H$ is a Galois extension of E. Since $\mathrm{Gal}(L/F)\simeq\mathbb{Z}/p$, it follows from (ii) and Theorem 7.4.13 that $\mathrm{Br}(L/F) = 0$. Therefore $\mathrm{Br}(L/E) = \mathrm{Br}(F/E)$, contradicting the choice of L.

(iii) $\Rightarrow$ (i) : If $a \in \mathrm{Br}(k)$ is such that $p^n a = 0$ for some integer n, it is the image of an element of $H^2(k, \mu_{p^n}) = H^2(\mathrm{Gal}(k_s/k), \mu_{p^n}(k_s))$ by Corollary 10.1.3. The discrete $\mathrm{Gal}(k_s/k)$-module $\mu_{p^n}(k_s)$ is of p-primary torsion, hence $H^2(\mathrm{Gal}(k_s/k), \mu_{p^n}(k_s)) = 0$ by (iii), and thus $a = 0$.

(i) $\Rightarrow$ (iii) : Let P be a pro-p-Sylow subgroup of $\mathrm{Gal}(k_s/k)$ (see Proposition 4.2.10). Then $\mathrm{cd}_p(\mathrm{Gal}(k_s/k)) = \mathrm{cd}_p(P)$ by Lemma 10.2.6 (ii). Replacing k with $(k_s)^P$, we may thus assume that $\mathrm{Gal}(k_s/k)$ is a pro-p-group. Let us write $X^p - 1 = (X-1)Q \in k[X]$, where $Q \in k[X]$. Then Q is a separable polynomial of degree $p-1$. We claim that Q has a root in k. Indeed, otherwise k_s/k would contain a subextension L/k such that $1 < [L : k] < p$. The index of the open subgroup $\mathrm{Gal}(k_s/L)$ of $\mathrm{Gal}(k_s/k)$ is a power of p (because $\mathrm{Gal}(k_s/k)$ is a pro-p-group), and coincides with $[L : k]$ (by Theorem 4.3.11), contradicting the relations $1 < [L : k] < p$.

Therefore k must contain a root of unity of order p (a root of Q), so that $\mathbb{Z}/p \simeq \mu_p$ as k-groups. Since $H^2(k, \mu_p) = 0$ by (i) and Corollary 10.1.3, it follows that $H^2(k, \mathbb{Z}/p) = 0$, which implies that $\mathrm{cd}_p(\mathrm{Gal}(k_s/k)) \leq 1$ by Lemma 10.2.5. $\square$

Proposition 10.2.11. *The following are equivalent:*

- *(i) We have* $\mathrm{cd}(\mathrm{Gal}(k_s/k)) \leq 1$*, and if k is of characteristic $p > 0$ the group* $\mathrm{Br}(K)$ *has no p-primary torsion for every separable extension K/k.*
- *(ii) For every separable extension K/k, we have* $\mathrm{Br}(K) = 0$*.*
- *(iii) For every separable extension K/k, and every finite Galois extension L/K, the norm map* $\mathrm{N}_{L/K} \colon L^\times \to K^\times$ *is surjective.*

Proof. Let K/k be a separable extension. We claim that $\mathrm{Br}(K) = 0$ if and only $\mathrm{Br}(K)$ has no p-primary torsion for every prime p. Indeed by Theorem 8.3.1 for any $x \in \mathrm{Br}(K)$, there exists a nonzero element $n \in \mathbb{N}$ such that $nx = 0$. Let us assume that n is chosen minimal. If $x \neq 0$, then we may write $n = pm$ for some prime p and integer m. Then $mx \in \mathrm{Br}(K)\{p\}$, hence vanishes if $\mathrm{Br}(K)$ has no p-primary torsion, contradicting the minimality of n. This proves the claim.

In view of Proposition 10.2.10 and Corollary 10.2.9, it will thus suffice to prove that the condition (iii) holds if it holds under the additional assumption that $[L : K]$ is prime. First assume that $G = \mathrm{Gal}(L/K)$ is a p-group for some prime p, and proceed by induction on $[L : K]$, the case $[L : K] = 1$ being trivial. If $[L : K] > 1$, there exists a normal subgroup $H \subset G$ such that $G/H \simeq \mathbb{Z}/p$. Let $E = L^H$. Then the extension E/K is Galois and $\mathrm{Gal}(E/K) \simeq \mathbb{Z}/p$, hence $\mathrm{N}_{E/K} \colon E^\times \to K^\times$ is surjective by assumption. By the induction hypothesis $\mathrm{N}_{L/E} \colon L^\times \to E^\times$ is also surjective. By transitivity of the norm maps (Corollary 5.3.4) we deduce that $\mathrm{N}_{L/K} \colon L^\times \to K^\times$ is surjective, concluding the inductive proof.

We now return to the general case, when $\mathrm{Gal}(L/K)$ is arbitrary. Let $n = [L : K]$ and $x \in K^\times$. Then there exists an integer $m > 0$ such that $x^m \in \mathrm{N}_{L/K}(L^\times)$ (because $x^n = \mathrm{N}_{L/K}(x)$). Let us pick m minimal. If $m > 1$, then $m = pu$ for some prime number p and integer u. Let H be a p-Sylow subgroup of $\mathrm{Gal}(L/K)$, and consider the subfield $E = L^H$. Let $d = [E : K]$ and $y = x^u \in K^\times$. By the case considered above, we know that $\mathrm{N}_{L/E} \colon L^\times \to E^\times$ is surjective. Thus $y \in \mathrm{N}_{L/E}(L^\times) \subset E^\times$. Using the transitivity of the norm maps (Corollary 5.3.4) we obtain

$$y^d = \mathrm{N}_{E/K}(y) \in \mathrm{N}_{E/K} \circ \mathrm{N}_{L/E}(L^\times) = \mathrm{N}_{L/K}(L^\times).$$

Since $y^p = x^m \in \mathrm{N}_{L/K}(L^\times)$ and d is prime to p, we deduce that $y \in \mathrm{N}_{L/K}(L^\times)$. As $y = x^u$ with $u < m$, this contradicts the minimality of m. Thus $m = 1$ and $x \in \mathrm{N}_{L/K}(L^\times)$. □

Definition 10.2.12. We say that the field k has *dimension* ≤ 1 if it satisfies the conditions of Proposition 10.2.11.

Remark 10.2.13. Note that if the field k is perfect, then k has dimension ≤ 1 if and only if the profinite group $\mathrm{Gal}(k/k_s)$ has cohomological dimension ≤ 1. This follows from the fact that $\mathrm{Br}(k)$ has no p-primary torsion when k is a perfect field of characteristic p (see Proposition 8.3.4).

3. C_1-fields

Definition 10.3.1. The field k is called a *C_1-field* if for every homogeneous polynomial $P \in k[X_1, \dots, X_n]$ of degree $d < n$, there exist $x_1, \dots, x_n \in k$ such that $P(x_1, \dots, x_n) = 0$ and at least one x_i is nonzero.

Definition 10.3.2. Let $R \to S$ be a morphism of commutative rings. Assume that the R-module S is free of finite rank. For any $s \in S$, denote by $l_s \colon S \to S$ the map given by $x \mapsto sx$, and define $\mathrm{N}_{S/R}(s) = \det(l_s) \in R$.

Lemma 10.3.3. *In the situation of Definition 10.3.2, let $e_1, \dots, e_r$ be an R-basis of S. Then there exists a homogeneous polynomial D of degree r having coefficients in R, and such that for any $s_1, \dots, s_r \in R$ we have*

$$\mathrm{N}_{S/R}(s_1 e_1 + \dots + s_r e_r) = D(s_1, \dots, s_r).$$

Proof. Set $s = s_1 e_1 + \dots + s_r e_r$. The determinant of a matrix in $M_r(R)$ is a homogeneous polynomial of degree r in the coefficients of the matrix, with coefficients in R (this follows for instance from the Leibniz formula). The coefficients of the matrix in $M_r(R)$ of the endomorphism l_s (say in the basis $e_1, \dots, e_r$) are R-linear combinations of the elements $s_1, \dots, s_r$. The statement follows. □

Lemma 10.3.4. *Let $R \to S$ be a morphism of commutative k-algebras such that the R-module S is free of finite rank. Let $\varphi \colon B \to k$ be a morphism of commutative k-algebras. Then the following diagram commutes*

$$\begin{tikzcd}
S \otimes_k B \arrow[r, "\mathrm{id}_S \otimes \varphi"] \arrow[d, "\mathrm{N}_{(S\otimes_k B)/(R\otimes_k B)}"'] & S \arrow[d, "\mathrm{N}_{S/R}"] \\
R \otimes_k B \arrow[r, "\mathrm{id}_R \otimes \varphi"] & R
\end{tikzcd}$$

Proof. Let $x \in S \otimes_k B$. Let $e_1, \dots, e_r$ be a basis of the R-module S. Let $M \in M_r(R)$ be the matrix of $l_{(\mathrm{id}_S \otimes \varphi)(x)} \colon S \to S$ in that basis, and $N \in M_r(R \otimes_k B)$ be the matrix of $l_x \colon S \otimes_k B \to S \otimes_k B$ in the basis $e_1 \otimes 1, \dots, e_r \otimes 1$. Then M is the image of N under the morphism $M_r(R \otimes_k B) \to M_r(R)$ induced by by the ring morphism $\mathrm{id}_R \otimes \varphi$. Since the determinant of matrices commutes with morphisms of commutative rings (being given by a universal polynomial in the coefficients of the matrix), it follows that $(\mathrm{id}_R \otimes \varphi)(\det N) = \det M$. This proves the lemma. □

Lemma 10.3.5. *If k is a C_1-field, then so is every algebraic field extension of k.*

Proof. Let L/k be an algebraic extension, and $f \in L[X_1, \ldots, X_n]$ a homogeneous polynomial of degree $d < n$. While searching for a nonzero element $(x_1, \ldots, x_n) \in L^n$ such that $P(x_1, \ldots, x_n) = 0$, we may replace L with the subextension of k generated by the finitely many coefficients of f, and thus assume that L/k is finite. Let $e_1, \ldots, e_r$ be a k-basis of L. Consider the variables $Y_{i,j}$ for $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, n\}$, and denote the polynomial k-algebra (resp. L-algebra) in these variables by $k[Y]$ (resp. $L[Y]$). Consider the polynomial

$$g = \sum_{i=1}^{r} g_i e_i = f\Big(\sum_{i=1}^{r} e_i Y_{i,1}, \ldots, \sum_{i=1}^{r} e_i Y_{i,n}\Big) \in L[Y], \tag{10.3.a}$$

where each $g_i \in k[Y]$ is homogeneous of degree d. Then $\mathrm{N}_{L[Y]/k[Y]}(g)$ is a homogeneous polynomial of degree r in the variables $g_1, \ldots, g_r$ by Lemma 10.3.3, hence a homogeneous polynomial of degree dr in the nr variables $Y_{1,1}, \ldots, Y_{r,n}$. Since $dr < nr$ and k is a C_1-field, it follows that there exist elements $y_{1,1}, \ldots, y_{r,n} \in k$ not all zero such that

$$0 = \big(\mathrm{N}_{L[Y]/k[Y]}(g)\big)(y_{1,1}, \ldots, y_{r,n}). \tag{10.3.b}$$

Applying Lemma 10.3.4 to the morphism $\varphi \colon k[Y] \to k$ given by $Y_{i,j} \mapsto y_{i,j}$ for $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, n\}$, we obtain

$$\big(\mathrm{N}_{L[Y]/k[Y]}(g)\big)(y_{1,1}, \ldots, y_{r,n}) = \mathrm{N}_{L/k}(g(y_{1,1}, \ldots, y_{r,n})).$$

This element vanishes by (10.3.b), which implies that $g(y_{1,1}, \ldots, y_{r,n}) = 0$ (see Lemma 5.3.2). For $j \in \{1, \cdots, n\}$, let $z_j = e_1 y_{1,j} + \cdots + e_r y_{r,j} \in L$. Using (10.3.a), we conclude that

$$0 = g(y_{1,1}, \ldots, y_{r,n}) = f\Big(\sum_{i=1}^{r} e_i y_{i,1}, \ldots, \sum_{i=1}^{r} e_i y_{i,n}\Big) = f(z_1, \ldots, z_n) \in L,$$

where at least one of $z_1, \ldots, z_n \in L$ is nonzero. $\square$

Proposition 10.3.6. *If k is a C_1-field, then k has dimension ≤ 1 (in the sense of Definition 10.2.12).*

Proof. By Lemma 10.3.5, it will suffice to prove that $\mathrm{N}_{L/k} \colon L^\times \to k^\times$ is surjective when L/k is a finite Galois extension. Let $a \in k^\times$, and choose a k-basis $e_1, \ldots, e_d$ of L. Let us write $k[X] = k[X_1, \ldots, X_d]$ and $L[X] = L[X_1, \ldots, X_d]$. Then the polynomial in $d+1$ variables

$$P = aY^d - \mathrm{N}_{L[X]/k[X]}\Big(\sum_{i=1}^{d} X_i e_i\Big) \in k[Y, X_1, \ldots, X_d],$$

is homogeneous of degree d by Lemma 10.3.3. Since k is a C_1-field, we find elements $y, x_1, \ldots, x_d \in k$ which are not all zero and satisfy $P(y, x_1, \ldots, x_d) = 0$. Applying Lemma 10.3.4 to the morphism $\varphi \colon k[Y, X_1, \ldots, X_d] \to k$ given by $Y \mapsto y$ and $X_i \mapsto x_i$ for $i = 1, \ldots, d$, we obtain $ay^d = \mathrm{N}_{L/k}(x)$, where $x = x_1 e_1 + \cdots + x_d e_d \in L$. If $y = 0$, then $\mathrm{N}_{L/k}(x) = 0$, hence $x = 0$ (see Lemma 5.3.2). Thus $y \neq 0$, and $\mathrm{N}_{L/k}(xy^{-1}) = a$. $\square$

Proposition 10.3.7 (Chevalley–Warning). *Every finite field is a C_1-field.*

Proof. This can be proved by elementary (and clever) manipulations, see e.g. [**Ser73**, I,§2]. $\square$

Proposition 10.3.8 (Tsen). *Assume that k is algebraically closed, and consider its purely transcendental extension in one variable $k(t)$. Then $k(t)$ is a C_1-field.*

Proof. Let $f \in k(t)[X_1, \ldots, X_n]$ a homogeneous polynomial of degree $d < n$. While searching for a nonzero element $(x_1, \ldots, x_n) \in k(t)^n$ such that $f(x_1, \ldots, x_n) = 0$, we may replace multiply f with any power of t, and thus assume that $f \in k[t][X_1, \ldots, X_n]$. Let r be the maximal degree (as a polynomial in t) of a coefficient in $k[t]$ of f. Since $d < n$, we may find an integer N such that $dN + r < n(N + 1)$. For each $i = 1, \ldots, n$ consider the polynomial

$$P_i = \sum_{j=0}^{N} X_{i,j} t^j \in k[X_{i,0}, \ldots, X_{i,N}].$$

Then

$$f(P_1, \ldots, P_n) = \sum_{l=0}^{dN+r} f_l(X_{1,0}, \ldots, X_{n,N}) t^l,$$

where each f_l is a homogeneous polynomial (of degree d). Since k is algebraically closed, there exists elements $x_{1,0}, \ldots, x_{n,N} \in k$ not all zero and such that $f_l(x_{1,0}, \ldots, x_{n,N}) = 0$ for all $l = 0, \ldots, dN+r$ (this follows from basic algebraic geometry, see e.g. [**Har77**, I.1.13 and I.7.2]: the intersection of a hypersurfaces in the projective space $\mathbb{P}^b$ is nonempty when $b \geq a$; here $a = dN + r + 1$ and $b = n(N + 1)$). $\square$

Exercises

Exercise 10.1. Let $\overline{k}$ be an algebraic closure of k. We first assume that $\overline{k}/k$ is finite of prime order p, where p is unequal to the characteristic of k.

(i) Show that k contains a root of unity of order p.

(ii) Show that the extension $\overline{k}/k$ is generated by an element α such that $a = \alpha^p \in k$.

(iii) Show that $\mathrm{Br}(\overline{k}/k) \simeq H^2(k, \mathbb{Z}/p)$ and $k^\times/k^{\times p} \simeq H^1(k, \mathbb{Z}/p)$, and that each of these groups is isomorphic to $\mathbb{Z}/p$. (Hint: Use the computation of the cohomology of finite cyclic groups.)

(iv) Deduce that $\mathrm{N}_{\overline{k}/k}(\overline{k}^\times) = k^{\times p}$.

(v) Show that $\mathrm{N}_{\overline{k}/k}(\alpha) = (-1)^{p-1}a$.

(vi) Deduce that $p = 2$, that -1 is not a square in k, and that $\overline{k} \simeq k[X]/(X^2 + 1)$.

We now assume that $\overline{k}/k$ is finite (of possibly nonprime order) and that k has characteristic zero.

(vii) Assume that -1 is a square in k. Show that $k = \overline{k}$.

(viii) Assume that -1 is not a square in k. Show that $\overline{k} \simeq k[X]/(X^2 + 1)$.

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.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[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.

[Ser73] Jean-Pierre Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[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`.