Galois theory for schemes

H. W. Lenstra

Mathematisch Instituut
Universiteit Leiden
Postbus 9512, 2300 RA Leiden
The Netherlands

First edition: 1985
(Mathematisch Instituut, Universiteit van Amsterdam)
Second edition: 1997
(Department of Mathematics, University of California at Berkeley)
Electronic third edition: 2008

Table of contents

Acknowledgements are due to Mrs. L. van Iterson for typing the manuscript; to Mr. W. Bosma for preparing the bibliography, the list of symbols, and the index; to Mrs. D. Craig for preparing the second edition and a first electronic version; and to Mr. T. Vorselen for preparing the third edition.

Readers are requested to e-mail possible errors – mathematical, typographical, or otherwise – to <hwl@math.leidenuniv.nl>.

Introduction

One of the most pleasant ways to familiarize oneself with the basic language of abstract algebraic geometry is to study Galois theory for schemes. In these notes we prove the main theorem of this theory, assuming as known only the fundamental properties of schemes. The first five sections of Hartshorne's book [10], Chapter II, contain more than we need.

The main theorem of Galois theory for schemes classifies the *finite étale covering* of a connected scheme X in terms of the *fundamental group* $\pi(X)$ of X. After the main theorem has been proved, we treat a few elementary examples; but a systematic discussion of the existing techniques to calculate the fundamental group falls outside the scope of these notes.

For a precise statement of the theorem that we shall prove we refer to Section 1. Here we give an informal explanation.

We first consider the case of *topological spaces*. Let X, Y be topological spaces, and $f\colon Y \to X$ a continuous map. We call $f\colon Y \to X$ a *trivial covering* if Y may be identified with $X \times E$ for some discrete set E, in such a way that f becomes the projection $X \times E \to X$ on the first coordinate. The map f is said to be a *covering* of X if it is locally a trivial covering, i.e., if X can be covered by open sets U for which $f\colon f^{-1}(U) \to U$ is a trivial covering. An example of a non-trivial covering is suggested in Figure 1.

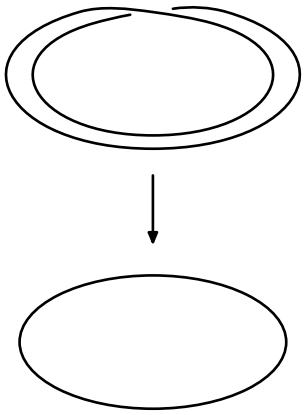
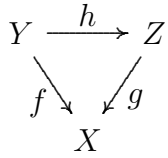


Figure 1.

This is an example of a *finite covering*, i.e., for each $x \in X$ the set $f^{-1}(x) \subset Y$ is finite. We call $\#f^{-1}(x)$ the *degree* of the covering at x; so the covering of Figure 1 has everywhere degree 2. A *map* from a covering $f\colon Y \to X$ to a covering $g\colon Z \to X$ is a continuous map $h\colon Y \to Z$ for which $f = gh$.



If X satisfies certain conditions then all coverings of X can be described by means of the *fundamental group* $\pi(X)$ of X. Suppose first that X is pathwise connected, and fix $x_0 \in X$. Then $\pi(X)$ is defined to be the group of homotopy classes of paths in X from x_0 to x_0. It is a theorem from algebraic topology that if X is connected, locally pathwise connected, and semilocally simply connected (see [8; 19]), the fundamental group $\pi(X)$ classifies all coverings of X, in the following sense. There is a one-to-one correspondence between coverings of X, up to isomorphism, and sets that are provided with an action of the group $\pi(X)$, also up to isomorphism. This correspondence is such that maps between coverings give rise to maps between the corresponding sets that respect the $\pi(X)$-action, and conversely. In other words, the *category* of coverings of X is equivalent to the category of sets provided with an action of $\pi(X)$.

There exist similar theories for wider classes of spaces, see [19, Notes to Chapter V]. In these theories the fundamental group is not defined with paths, but the existence of a group for which the coverings of X admit the above description is proved. This group is then defined to be the fundamental group of X.

A particularly wide class of spaces X can be treated if one wishes to classify only the *finite* coverings of X. For this it suffices that X be *connected*, i.e., have exactly one connected component. (In these notes the empty space is not considered to be connected.) For any connected space X there is a *topological* group $\hat{\pi}(X)$ such that the category of finite coverings of X is equivalent to the category of finite discrete sets provided with a *continuous* action of $\hat{\pi}(X)$. This result, which is difficult to locate in the literature [2], is treated in detail in these notes (see (1.15)), because of the close analogy with the case of schemes.

To find an analogue of the notion of a finite covering for *schemes*, one could repeat the definition given above. The only changes are that $f\colon Y \to X$ should be a morphism of schemes, and that E should be finite. This is, however, not the "correct" definition. Not only does it give nothing new (Exercise 5.22(a)), but it is too restrictive in the sense that many topological coverings cease to be coverings if one passes to the direct scheme-theoretic analogue. To illustrate this, and to show how *finite étale coverings* are more general, we consider an example.

Define $g \in \mathbb{C}[U,V]$ by $g = V^3 + 2V^2 - 15V - 4U$, and let C be the curve $\{(u,v) \in \mathbb{C} \times \mathbb{C} : g(u,v) = 0\}$. We consider the map $f\colon C \to \mathbb{C}$ sending (u,v) to u. Some real points of C

and their images under f in $\mathbb{R}$ are drawn in Figure 2. For each $u \in \mathbb{C}$, the number $\#f^{-1}(u)$ of points mapping to u is the number of zeros of $g(u,V) = V^3 + 2V^2 - 15V - 4u$, and this is 3 unless the discriminant of $g(u,V)$ vanishes. This discriminant equals $-432u^2 + 2288u + 14400 = -16(27u+100)(u-9)$, so $\#f^{-1}(u) = 3$ for $u \in \mathbb{C} - \{-\frac{100}{27},\ 9\}$. From this it can be deduced that f becomes a covering if points with $u = -\frac{100}{27}$ or $u = 9$ are removed; i.e., if $X = \mathbb{C} - \{-\frac{100}{27},\ 9\}$ and $Y = f^{-1}[X] \subset C$, then $f\colon Y \to X$ is a finite covering of topological spaces, and the degree is 3 everywhere.

The scheme-theoretic analogue is as follows. The scheme corresponding to X is $\operatorname{Spec} A$, where $A = \mathbb{C}[U, ((27U+100)(U-9))^{-1}]$, and Y corresponds to $\operatorname{Spec} B$, where $B = A[V]/gA[V]$. The morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ is *not* locally a trivial covering in the same way as this is true for the topological spaces. To see this, one looks at the generic point ξ of $\operatorname{Spec} A$. Its local ring is the field of fractions $Q(A) = \mathbb{C}(U)$ of A, and the fibre of $\operatorname{Spec} B \to \operatorname{Spec} A$ over ξ is the spectrum of $Q(B)$. That is a cubic field extension of $Q(A)$, so $\operatorname{Spec} Q(B) \to \operatorname{Spec} Q(A)$ is not a "trivial covering", and $\operatorname{Spec} B \to \operatorname{Spec} A$ is not "trivial" in a neighborhood of ξ.

It *is* true that $\operatorname{Spec} B \to \operatorname{Spec} A$ is a *finite étale* covering. The precise definition of this notion is given in Section 1. Translating this definition in concrete terms, one finds that the local "triviality" condition from the topological definition has been replaced by an analogous algebraic condition, namely that a certain *discriminant* does not vanish locally (cf. Exercises 1.3 and 1.6). In our topological example we saw that the existence of three points of Y mapping to u was implied by the non-vanishing of the discriminant at u, for $u \in X$. In the scheme-theoretic example this is still true if one restricts to *closed* points $u \in \operatorname{Spec} A$, since these have an algebraically closed residue class field $\mathbb{C}$; but the non-closed point $u = \xi$ has a residue class field $\mathbb{C}(U)$ that is *not* algebraically closed, and there is only *one* point of $\operatorname{Spec} B$ that maps to ξ; to compensate for this, it is "three times as large" in the sense that its residue class field is a cubic extension of $\mathbb{C}(U)$.

The algebraic nature of the definition of "finite étale" makes it also work well for fields different from $\mathbb{C}$, which is not the case with the topological definition. To illustrate this we write, for a subfield $K \subset \mathbb{C}$:

$$\begin{aligned} Y_K &= Y \cap (K \times K) = \{(u,v) \in K \times K : g(u,v) = 0,\ u \notin \{-\tfrac{100}{27},\ 9\}\}, \\ X_K &= X \cap K = K - \{-\tfrac{100}{27},\ 9\}, \\ A_K &= K[U, ((27U+100)(U-9))^{-1}], \\ B_K &= A_K[V]/gA_K[V], \end{aligned}$$

with $g = V^3 + 2V^2 - 15V - 4U$ as above.

Consider first $K = \mathbb{R}$. The map $Y_{\mathbb{R}} \to X_{\mathbb{R}}$ (see Figure 2) is still a covering, but it does not have degree 3 everywhere; at points u with $u > 9$ or $u < -\frac{100}{27}$ the degree is 1. The algebraic

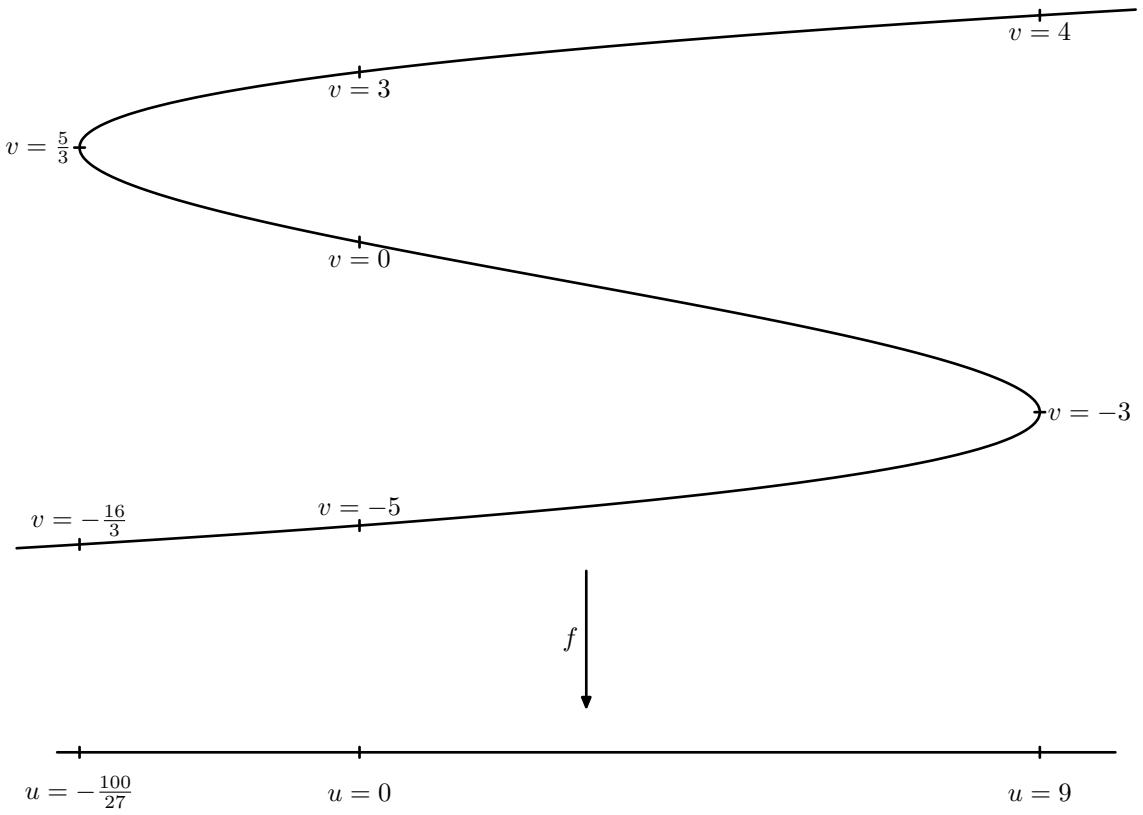


Figure 2.

definition, however, takes the "invisible points" into account, and $\operatorname{Spec} B_{\mathbb{R}} \to \operatorname{Spec} A_{\mathbb{R}}$ is a finite étale covering that has degree 3 everywhere. (The degree is defined in Section 5.)

For $K = \mathbb{Q}$, the map $Y_K \to X_K$ is not even a covering any more: $u = 0$ has three originals in $Y_{\mathbb{Q}}$, but $u = \frac{1}{n}$ has none, for $n \in \mathbb{Z}$, $n \neq 0$. The morphism $\operatorname{Spec} B_K \to \operatorname{Spec} A_K$, however, is a finite étale covering for $K = \mathbb{Q}$, and in fact for every subfield K of $\mathbb{C}$.

The main theorem to be proved in these notes asserts that for a connected scheme X the finite étale coverings of X can be classified in precisely the same way as the finite coverings of a connected topological space. A precise statement of the theorem is given in Section 1 (see 1.11). If X is the spectrum of a field, the theorem is essentially a reformulation of classical Galois theory for fields. The connection is explained in detail in Section 2. Section 3 contains an axiomatic treatment of the sort of categories that we are interested in. The proof of the theorem is thereby reduced to the verification of the axioms. For the case of finite coverings

of a connected topological space this verification is already done in Section 3, by way of example. The "affine" information that we need for the proof of the theorem is assembled in Section 4, and Section 5 contains the proof of the theorem. In Section 6 we show that the definitions we use are equivalent to those found in the literature, and we prove a theorem that enables us to treat some very elementary examples. The reader who wishes to see examples of greater interest is encouraged to go on and read [20, Chapter I, §5; 9; 22].

It is a natural question how to classify the finite étale coverings (or finite coverings) of a scheme (or topological space) X that is *not* connected. If, topologically, X is the disjoint union of its connected components, then such a classification is easily derived from our main theorem, cf. [9, Exposé V, numéro 9]. For the case of an affine scheme, see [18]. The general case, however, seems not to have been dealt with.

Prerequisites and conventions

Sets. By $\#S$ we denote the cardinality of a set S.

Topology. Topological spaces are not assumed to be Hausdorff. The empty space is not connected.

Categories and functors. Only a very basic familiarity with these notions is assumed. Most terms from category theory are defined where they are needed. See also [12].

Commutative algebra. Rings are always assumed to be *commutative with* 1, except in Exercises 1.18 and 4.40. The unit element is preserved by all ring homomorphisms, belongs to all subrings, and acts as the identity on all modules. The group of units of a ring A is denoted by A^*. If A is a ring, an *A-algebra* is a ring B equipped with a ring homomorphism $A \to B$. Everything we need from commutative algebra can be found in [1]. *Projective modules*, which are not in [1], are treated in Section 4.

Fields. We assume familiarity with ordinary finite Galois theory for fields. *Infinite* Galois theory is treated in Section 2. Several examples and exercises make use of valuation theory and algebraic number theory; see [5; 17; 26].

Schemes. Everything we need about schemes can be found in [10, Chapter II, Sections 1–5]. Schemes need not be separated, and are not assumed to be locally noetherian. The empty scheme is not connected.

Some exercises need more background. Appropriate references will then be given.

1 Statement of the main theorem

In this section we state the main theorem to be proved in these notes, and we discuss the relationship with algebraic topology.

1.1 Free modules. Let A be a ring and M a module over A. A collection of elements $(w_i)_{\in I}$ of M is called a *basis* of M (over A) if for every $x \in M$ there is a unique collection $(a_i)_{\in I}$ of elements of A such that $a_i = 0$ for all but finitely many $i \in I$ and $x = \sum_{i\in I} a_i w_i$. If M has a basis it is called *free* (over A). If A is not the zero ring and M is free with basis $(w_i)_{\in I}$, then the cardinality $\#I$ depends only on M, and not on the choice of the basis (Exercise 1.1). It is called the *rank* of M over A, notation: $\mathrm{rank}_A(M)$. If M is a finitely generated free module then the rank is finite (Exercise 1.1).

Let M be a finitely generated free A-module with basis $w_1, w_2, \ldots, w_n$ and let $f\colon M \to M$ be A-linear. Then

$$f(w_i) = \sum_{j=1}^{n} a_{ij} w_j \qquad (1 \le i \le n)$$

for certain $a_{ij} \in A$, and the trace $\mathrm{Tr}(f)$ of f is defined by

$$\mathrm{Tr}(f) = \sum_{i=1}^{n} a_{ii}.$$

This is an element of A that depends only on f, and not on the choice of the basis (see 4.8, or Exercise 1.2). It is easily checked that the map $\mathrm{Tr}\colon \mathrm{Hom}_A(M, M) \to A$ is A-linear.

1.2 Separable algebras. Let A be a ring, B an A-algebra, and suppose that B is finitely generated and free as an A-module. For every $b \in B$ the map $m_b\colon B \to B$ defined by $m_b(x) = bx$ is A-linear, and the trace $\mathrm{Tr}(b)$ or $\mathrm{Tr}_{B/A}(b)$ is defined to be $\mathrm{Tr}(m_b)$. The map $\mathrm{Tr}\colon B \to A$ is easily seen to be A-linear and to satisfy $\mathrm{Tr}(a) = \mathrm{rank}_A(B) \cdot a$ for $a \in A$.

The A-module $\mathrm{Hom}_A(B, A)$ is clearly free over A with the same rank as B. Define the A-linear map $\phi\colon B \to \mathrm{Hom}_A(B, A)$ by $(\phi(x))(y) = \mathrm{Tr}(xy)$, for $x, y \in B$. If ϕ is an isomorphism we call B *separable* over A, or a *free separable* A-algebra if we wish to stress the condition that B be finitely generated and free as an A-module. See Exercise 1.3 for a reformulation of this definition. In 4.13 and 6.10 we shall define the notion of separability for wider classes of A-algebras.

1.3 Examples. For any integer $n \ge 0$ the A-algebra A^n, with component-wise ring operations, is clearly a free separable A-algebra. If $A = \mathbb{Z}$ there are no others (see 1.12 and 6.18),

and the same thing is true if A is an algebraically closed field (see Theorem 2.7). Generally, if K is a field, then the free separable K-algebras are precisely the K-algebras of the form $\prod_{i=1}^{t} B_i$, where each B_i is a finite separable field extension of K in the sense of Galois theory, and $t \geq 0$, see Theorem 2.7. (Note that $t = 0$ gives the zero ring.) Further examples are found in Exercises 1.5 and 1.6.

1.4 Finite étale morphisms. A morphism $f\colon Y \to X$ of schemes is *finite étale* if there exists a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i the open subscheme $f^{-1}(U_i)$ of Y is affine, and equal to $\operatorname{Spec} B_i$, where B_i is a free separable A_i-algebra. In this situation we also say that $f\colon Y \to X$ is a *finite étale covering* of X.

In 6.9 we shall see that this definition is equivalent to the one found in the literature.

Note that a finite étale morphism is *finite* [10, Chapter II, Section 3], so for *every* open affine subset $U = \operatorname{Spec} A$ of X the open subscheme $f^{-1}(U)$ of Y is affine, $f^{-1}(U) = \operatorname{Spec} B$, where B is a finitely generated A-module. However, in this situation B need not be free as an A-module, but it is *projective*, see Section 4 and 5.2.

1.5 Examples. For any non-negative integer n and any scheme X, the disjoint union $X \amalg X \amalg \cdots \amalg X$ of n copies of X, with the obvious morphism to X, is easily seen to be a finite étale covering of X. Again it is true that for $X = \operatorname{Spec} \mathbb{Z}$ there are no others (see 1.12 and 6.18). If $X = \operatorname{Spec} K$, where K is a field, the finite étale coverings $Y \to X$ are precisely given by $Y = \coprod_{i=1}^{t} \operatorname{Spec} B_i$, with B_i and t as in 1.3. If $X = \operatorname{Spec} A$, where A is the ring of algebraic integers in an algebraic number field K, then the finite étale coverings $Y \to X$ are precisely given by $Y = \coprod_{i=1}^{t} \operatorname{Spec} A_i$, where $t \geq 0$ and where for each i the ring A_i is the ring of algebraic integers in a finite extension K_i of K that is unramified at all non-zero prime ideals of A, see 6.18.

1.6 Morphisms of coverings. A *morphism* from a finite étale covering $f\colon Y \to X$ to a finite étale covering $g\colon Z \to X$ is a morphism of schemes $h\colon Y \to Z$ for which $f = gh$. This notion enables us to speak of the *category of finite étale coverings of* X, for any fixed scheme X, notation: $\mathbf{FEt}_X$.

Our main theorem will describe this category for *connected* X. (*Connected* means for us that the space of X has exactly *one* connected component; in particular $X = \emptyset$ is *not* connected.)

1.7 Projective limits. A partially ordered set I is called *directed* if for any two $i, j \in I$ there exists $k \in I$ satisfying $k \geq i$ and $k \geq j$. A *projective system* consists of a directed partially ordered set I, a collection of sets $(S_i)_{i \in I}$, and a collection of maps $(f_{ij}\colon S_i \to S_j)_{i,j \in I,\ i \geq j}$ satisfying the conditions

$$f_{ii} = (\text{identity on } S_i) \quad \text{for each} \quad i \in I$$
$$f_{ik} = f_{jk} \circ f_{ij} \quad \text{for all} \quad i, j, k \in I \text{ with } i \geq j \geq k.$$

The *projective limit* of such a system, notation

$$\varprojlim S_i \quad \text{or} \quad \varprojlim_{i \in I} S_i$$

(the maps f_{ij} are usually clear from the context) is defined by

$$\varprojlim S_i = \{(x_i)_{i \in I} \in \prod_{i \in I} S_i \colon f_{ij}(x_i) = x_j \text{ for all } i, j \in I \text{ with } i \geq j\}.$$

If all S_i are groups, or rings, or modules over a ring A, and all f_{ij} are group homomorphisms, or ring homomorphisms, or A-module homomorphisms, then $\varprojlim S_i$ is a group, or a ring, or an A-module. Likewise, if all S_i are topological spaces, then $\varprojlim S_i$ can be made into a topological space by giving $\prod_{i \in I} S_i$ the product topology and $\varprojlim S_i$ the relative topology.

1.8 Profinite groups. Let I, $(\pi_i)_{i \in I}$, $(f_{ij})_{i,j \in I,\ i \geq j}$ be a projective system in which the π_i are *finite groups* and the f_{ij} *group homomorphisms.* Then $\pi = \varprojlim \pi_i$ is a group, and if each π_i is endowed with the discrete topology then π is a topological space, by 1.7. In fact, π is a *topological group* in the sense that the maps $\pi \times \pi \to \pi$, $(x, y) \mapsto xy$ and $\pi \to \pi$, $x \mapsto x^{-1}$, are continuous. A topological group that arises in this way is called a *profinite group.* Profinite groups are compact (Exercise 1.9(a)) and totally disconnected; it can be proved that conversely every compact totally disconnected topological group is profinite (see [5, Chapter V, Theorem 1]). A *homomorphism* of profinite groups is a continuous group homomorphism. An *isomorphism* is a homomorphism with a two-sided inverse that is again a homomorphism. Since each continuous bijection from a compact space to a Hausdorff space is a homeomorphism, each bijective homomorphism is an isomorphism.

1.9 Examples. Let G be an arbitrary group, and I the collection of normal subgroups of finite index of G. Let I be partially ordered by $N \geq N' \Leftrightarrow N \subset N'$. Then the collection of groups $(G/N)_{N \in I}$ gives rise to a projective system of finite groups, the transition maps $G/N \to G/N'$ (for $N \geq N'$) being the canonical homomorphisms. Hence $\hat{G} = \varprojlim G/N$ is a profinite group, and it is called the *profinite completion* of G. In particular we have

$$\hat{\mathbb{Z}} \;=\; \varprojlim_{n > 0} \mathbb{Z}/n\mathbb{Z},$$

the set of positive integers being partially ordered by divisibility. Since each $\mathbb{Z}/n\mathbb{Z}$ is a ring, $\hat{\mathbb{Z}}$ is in fact a *profinite ring* (definition obvious).

Next let p be a prime number, and I the set of positive integers, totally ordered in the usual way. Then $(\mathbb{Z}/p^n\mathbb{Z})_{n>0}$, with the obvious transition maps $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ (for $n \geq m$), is a projective system, and

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

is a profinite group. It is in fact a profinite ring, the *ring of p-adic integers.*

Other important examples of profinite groups occur in infinite Galois theory, see Theorem 2.2.

1.10 Group actions. Let G be a group. An action (on the left) of G on a set E is said to be *trivial* if $\sigma e = e$ for all $\sigma \in G$, $e \in E$, and *free* if $\sigma e \neq e$ for all $\sigma \in G$, $\sigma \neq 1$ and all $e \in E$. It is said to be *transitive* if E has exactly one orbit under G; in particular E is then non-empty.

A G-set is a set E equipped with an action of G on E. A *morphism* from a G-set E to a G-set E' is a map $f\colon E \to E'$ satisfying $f(\sigma e) = \sigma f(e)$ for all $\sigma \in G$ and $e \in E$. This enables us to speak about the category of G-sets.

If E is a G-set, we write $E^G = \{e \in E : \sigma e = e \text{ for all } \sigma \in G\}$.

Next let π be a *profinite* group. A π-set is a set E equipped with an action of π on E that is continuous in the sense that the map $\pi \times E \to E$ defining the action is continuous, if E has the discrete topology and $\pi \times E$ the product topology. (See Exercise 1.19 for a reformulation.) A *morphism* of π-sets is defined as above, and the category of *finite* π-sets is denoted by π-**sets.**

We are now able to formulate the *main theorem of Galois theory for schemes.*

1.11 Main theorem. *Let X be a connected scheme. Then there exists a profinite group π, uniquely determined up to isomorphism, such that the category $\mathbf{FEt}_X$ of finite étale coverings of X is equivalent to the category π-**sets** of finite sets on which π acts continuously.*

This theorem will be proved in 5.25. The profinite group π occurring in the theorem is called the *fundamental group* of X, notation: $\pi(X)$.

1.12 Examples. The disjoint union of n copies of X corresponds, under the equivalence in 1.11, to a finite set of n elements on which π acts trivially. The fact that for $X = \operatorname{Spec}\mathbb{Z}$ there are no other finite étale coverings of X is thus expressed by the group $\pi(\operatorname{Spec}\mathbb{Z})$ being *trivial.* The same is true for $\pi(\operatorname{Spec} K)$, where K is an algebraically closed field. More

generally, if K is an arbitrary field, then $\pi(\operatorname{Spec} K)$ is the Galois group of the separable closure of K over K, see 2.4 and 2.9. In this case we will prove Theorem 1.11 (except for the uniqueness statement) in Section 2, where we shall see that the theorem is only a reformulation of classical Galois theory. In particular, one has $\pi(\operatorname{Spec} K) \cong \hat{\mathbb{Z}}$ if K is a finite field (see 2.5).

Next let $X = \operatorname{Spec} A$, where A is the ring of integers in an algebraic number field K. Then $\pi(X)$ is the Galois group of M over K, where M is the maximal algebraic extension of K that is unramified at all non-zero prime ideals of A. More generally, if $a \in A$, $a \neq 0$, then $\pi(\operatorname{Spec} A[1/a])$ is the Galois group, over K , of the maximal algebraic extension of K that is unramified at all non-zero prime ideals of A not dividing a. These facts will be proved in 6.18.

If p is a prime number, then $\pi(\operatorname{Spec} \mathbb{Z}_p) \cong \hat{\mathbb{Z}}$, see 6.18. More examples will be given in 1.16 and 6.24.

1.13 The topological fundamental group. In the introduction we defined *coverings* of a topological space X, and *maps* between such coverings. This leads to the category of coverings of X. If X satisfies certain conditions then this category has a description analogous to the one given in 1.11, as follows.

For $x \in X$, the *fundamental group* $\pi(X, x)$ is the group of homotopy classes of closed paths through x; see [8; 19] for details. Now suppose that X is connected, locally pathwise connected, and semilocally simply connected; the last condition means that every $x \in X$ has a neighborhood U such that the natural map $\pi(U, x) \to \pi(X, x)$ is trivial. Then the group $\pi(X, x)$ is independent of the choice of $x \in X$, up to isomorphism, and denoting it by $\pi(X)$ we have the following theorem.

1.14 Theorem. *Let X be a topological space satisfying the above conditions. Then the category of coverings of X is equivalent to the category of $\pi(X)$-sets.*

For the proof of this theorem we refer to [8, Chapitre IX, numéro 6; 19, Chapter V].

The analogy with 1.11 is not complete: the fundamental group $\pi(X)$ has no topology, and the $\pi(X)$-sets need not be finite. As was said in the introduction, one obtains a much closer analogy by considering only *finite* coverings.

1.15 Theorem. *Let X be a connected topological space. Then there exists a profinite group $\hat{\pi}(X)$, uniquely determined up to isomorphism, such that the category of finite coverings of X is equivalent to the category $\hat{\pi}(X)$-**sets** of finite sets on which $\hat{\pi}(X)$ acts continuously.*

The proof of this theorem is given in 3.10.

Theorem 1.15 is weaker than 1.14 in the sense that it only classifies *finite* coverings of X, but it does so for a much wider class of topological spaces.

If X satisfies the conditions stated just before 1.14, then the group $\hat{\pi}(X)$ from 1.15 is the profinite completion of the fundamental group $\pi(X)$ occurring in 1.14, see Exercise 1.24.

The analogy between 1.11 and 1.15 is more than formal. If X is a non-singular variety over $\mathbb{C}$, and X_h is the associated complex analytic space (see [10, Appendix B]), then the algebraically defined fundamental group $\pi(X)$ from Theorem 1.11 is isomorphic to the topologically defined fundamental group $\hat{\pi}(X_h)$ from Theorem 1.15, which in turn is the profinite completion of the classical fundamental group from 1.14. (See [10, p. 442] and [20, pp. 40 & 118] for references.) This opens the possibility of calculating the algebraic fundamental group by topological means. This connection can even be used to calculate fundamental groups of schemes in characteristic p (see [9; 22], and the discussion in [20, Chapter I, Section 5]).

1.16 Example. If K is a field, then one has $\pi(\mathbb{P}^1_K) = \pi(\operatorname{Spec} K)$, where $\mathbb{P}^1_K$ denotes the projective line over K. If moreover $\operatorname{char}(K) = 0$, then one has also $\pi(\mathbb{A}^1_K) = \pi(\operatorname{Spec} K)$, where $\mathbb{A}^1_K$ is the affine line over K. (See 6.22 and 6.23.) For $K = \mathbb{C}$, this shows that $\pi(\mathbb{P}^1_{\mathbb{C}})$ and $\pi(\mathbb{A}^1_{\mathbb{C}})$ are both trivial. This is consistent with the above remarks, since the associated complex analytic spaces are simply connected, hence have a trivial fundamental group.

Exercises for Section 1

1.1 Let A be a ring, $A \neq 0$, and M an A-module with basis $(w_i)_{i \in I}$.

(a) Prove that there is a ring homomorphism from A to a field k, and that $\#I = \dim_k(M \otimes_A k)$.

(b) Suppose that M is a finitely generated A-module. Prove that $\#I$ is finite.

1.2 (a) Let $w_1, w_2, \ldots, w_n$ be a basis for M over A, and let

$$v_i = \sum_{j=1}^{n} a_{ij} w_j \in M \qquad (1 \leq i \leq n)$$

with $a_{ij} \in A$. Prove: $v_1, v_2, \ldots, v_n$ is a basis for M over $A \Leftrightarrow \det((a_{ij})_{1 \leq i,j \leq n}) \in A^*$.

(b) The trace $\mathrm{Tr}(C)$ of an $n \times n$-matrix $C = (c_{ij})_{1 \le i,j \le n}$ over A is defined by $\mathrm{Tr}(C) = \sum_{i=1}^{n} c_{ii}$. Prove

$$\begin{aligned} \mathrm{Tr}(CD) &= \mathrm{Tr}(DC), \\ \mathrm{Tr}(ECE^{-1}) &= \mathrm{Tr}(C) \end{aligned}$$

for $n \times n$-matrices C, D, E over A with $\det(E) \in A^*$.

(c) Prove that the trace of an A-endomorphism of a finitely generated free module, as defined in 1.1, is independent of the choice of the basis.

1.3 Let B be an A-algebra that is finitely generated and free as an A-module, with basis $w_1, w_2, \ldots, w_n$. Prove: B is separable over $A \Leftrightarrow \det(\mathrm{Tr}(w_i w_j))_{1 \le i,j \le n}) \in A^*$.

1.4 Let B be a free separable A-algebra, A' an A-algebra, and $B' = B \otimes_A A'$. Prove that B' is a free separable A'-algebra.

1.5 Let K be an algebraic number field with discriminant Δ and ring of integers A. Prove that $A[1/\Delta]$ is a free separable $\mathbb{Z}[1/\Delta]$-algebra.

1.6 Let A be a ring.

(a) Let $a \in A$. Prove that $A[X]/(X^2 - a)$ is a free separable A-algebra if and only if $2a \in A^*$.

(b) Let, more generally, $f \in A[X]$ be a monic polynomial. Prove that $A[X]/(f)$ is a free separable A-algebra if and only if the discriminant $\Delta(f)$ of f belongs to A^*.

1.7 Suppose that the scheme X is the disjoint union of two schemes X', X''. Prove that the category $\mathbf{FEt}_X$ is equivalent to a suitably defined "product category" $\mathbf{FEt}_{X'} \times \mathbf{FEt}_{X''}$.

1.8 Let $S = \varprojlim S_i$ be a projective limit as in 1.7, and define for each $j \in I$ the projection map $f_j \colon S \to S_j$ by $f_j((x_i)_{i \in I}) = x_j$. Prove that the system $(S, (f_j)_{j \in I})$ has the following "universal property":

(i) $f_{ij} \circ f_i = f_j$ for all $i, j \in I$ with $i \ge j$;

(ii) if T is a set and $(g_j \colon T \to S_j)_{j \in I}$ is a collection of maps satisfying $f_{ij} \circ g_i = g_j$ (for all $i, j \in I$ with $i \ge j$) then there is a unique map $g \colon T \to S$ such that $g_j = f_j \circ g$ for all $j \in I$.

Prove further that this universal property characterizes $(S, (f_j)_{j \in I})$ in the following sense: if S' is a set and $(f'_j \colon S' \to S_j)_{j \in I}$ a collection of maps satisfying the analogues of (i), (ii), then there is a unique bijection $f' \colon S' \to S$ such that $f'_j = f_j \circ f'$ for all $j \in I$.

1.9 Let the notation be as in 1.7, and $S = \varprojlim S_i$.

(a) Suppose that all sets S_i are endowed with a compact Hausdorff topology, that all S_i are non-empty, and that all maps f_{ij} are continuous. Prove that S is non-empty and compact. [*Hint:* Apply Tikhonov's theorem.]

(b) Suppose that all sets S_i are *finite* and *non-empty.* Prove that $S \neq \emptyset$.

(c) Suppose that I is countable, that all S_i are non-empty, and that all maps f_{ij} are surjective. Prove that $S \neq \emptyset$.

(d) Let I be the collection of all finite subsets of $\mathbb{R}$, and let I be partially ordered by inclusion. For each $i \in I$, let S_i be the set of *injective* maps $\phi\colon i \to \mathbb{Z}$, and let $f_{ij}\colon S_i \to S_j$ (for $j \subset i$) map ϕ to its restrictions $\phi|j$. Prove that this defines a projective system in which all S_i are non-empty and all f_{ij} are surjective, but that the projective limit S is empty.

1.10 Prove: If π_j is a profinite group for each j in a set J, then $\prod_{j\in J} \pi_j$ is a profinite group.

1.11 (Open and closed subgroups of profinite groups.) Let $\pi = \varprojlim \pi_i \subset \prod_{i\in I} \pi_i$ be a profinite group, with all π_i finite groups, and $f_j\colon \pi \to \pi_j$ the projection maps as in Exercise 1.8, for $j \in I$. Let further $\pi' \subset \pi$ be a subgroup.

(a) Prove: π' is open $\Leftrightarrow$ π' is closed and of finite index $\Leftrightarrow$ $\exists j \in J : \ker f_j \subset \pi'$.

(b) Prove: π' is closed $\Leftrightarrow$ there is a system of subgroups $(\rho_i \subset \pi_i)_{i\in I}$ with $\pi' = \pi \cap (\prod_{i\in I} \rho_i)$ (inside $\prod_{i\in I} \pi_i$) $\Leftrightarrow$ there is a system of subgroups $(\rho_i \subset \pi_i)_{i\in I}$ with $\pi' = \pi \cap (\prod_{i\in I} \rho_i)$ and for which in addition $f_{ij}[\rho_i] = \rho_j$ for all $i, j \in I$ with $i \geq j$.

(c) Prove that π' is profinite if it is closed.

(d) Suppose that π' is a closed normal subgroup. Prove that π/π', with the quotient topology, is profinite.

1.12 (a) Let G be a group, and $\hat{G}$ its profinite completion. Prove that there is a natural group homomorphism $f\colon G \to \hat{G}$ for which $f[G]$ is dense in $\hat{G}$.

(b) Prove: if G is a free group, then the natural map $f\colon G \to \hat{G}$ from (a) is injective.

(c) Let $G = \langle a, b, c, d : aba^{-1} = b^2,\ bcb^{-1} = c^2,\ cdc^{-1} = d^2,\ dad^{-1} = a^2\rangle$. Prove that G is infinite and that $\hat{G}$ is trivial (see [24, I.1.4]).

1.13 Let p be a prime number, and $\mathbb{Z}_p$ the ring of p-adic integers defined in 1.9. Prove:

(a) $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$;

(b) each $a \in \mathbb{Z}_p - \{0\}$ can be uniquely written in the form $a = up^n$ with $u \in \mathbb{Z}_p^*$, $n \in \mathbb{Z},\ n \geq 0$;

(c) $\mathbb{Z}_p$ is a local domain with residue class field $\mathbb{F}_p$.

1.14 Prove that there is an isomorphism $\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p$ of topological rings (definition obvious).

1.15 Let $\mathbb{Z}_{10} = \varprojlim_{n \geq 1} \mathbb{Z}/10^n\mathbb{Z}$.

(a) Prove that each $a \in \mathbb{Z}_{10}$ has a unique representation $a = \sum_{n=0}^{\infty} c_n 10^n$ with $c_n \in \{0, 1, \ldots, 9\}$.

(b) Prove that there exists a unique continuous function $v\colon \mathbb{Z}_{10} \to \mathbb{R}$ such that $v(a) = (\text{number of factors 2 in } a)^{-1}$ for each positive integer a.

(c) Let $(a_n)_{n=0}^{\infty}$ be a sequence of positive integers not divisible by 10 such that the number of factors 2 in a_n tends to infinity for $n \to \infty$. Prove that the sum of the digits of a_n in the decimal system tends to infinity for $n \to \infty$.

1.16 (a) Prove that each $a \in \hat{\mathbb{Z}}$ has a unique representation $a = \sum_{n=1}^{\infty} c_n n!$ with $c_n \in \{0, 1, \ldots, n\}$.

(b) Let $b \in \mathbb{Z}$, $b \geq 0$, and define the sequence $(a_n)_{n=0}^{\infty}$ of non-negative integers by $a_0 = b$, $a_{n+1} = 2^{a_n}$. Prove that $(a_n)_{n=0}^{\infty}$ converges in $\hat{\mathbb{Z}}$, and that $\lim_{n\to\infty} a_n \in \hat{\mathbb{Z}}$ is independent of b.

(c) Let $a = \lim_{n\to\infty} a_n$ as in (b), and write $a = \sum_{n=1}^{\infty} c_n n!$ as in (a). Compute c_n for $1 \leq n \leq 10$.

1.17 A subset J of a partially ordered set I is called *cofinal* if $\forall i \in I : \exists j \in J : j \geq i$.

(a) Prove: if J is a cofinal subset of a directed partially ordered set, then J is directed.

(b) Let the notation be as in 1.7, and let $J \subset I$ be a cofinal subset. Prove that there is a canonical bijection $\varprojlim_{j\in J} S_j \cong \varprojlim_{i\in I} S_i$.

(c) Prove: $\hat{\mathbb{Z}} \cong \varprojlim_{n>0} \mathbb{Z}/n!\mathbb{Z}$.

1.18 (Compact rings are profinite.) In this exercise, rings are not necessarily commutative. Let R be a compact Hausdorff topological ring with 1. It is the purpose of this exercise to show that R is a profinite ring.

(a) For an open neighborhood U of 0 in R, let $V = \{x \in R : R \times R \subset U\}$. Prove that V is a neighborhood of 0 in R. If moreover U is an additive subgroup of R, prove that V is an open two-sided ideal of R.

(b) Let $\chi\colon R \to \mathbb{R}/\mathbb{Z}$ be a continuous group homomorphism. Prove that $\ker \chi$ is open in R. [*Hint:* Choose U in (a) such that $\chi[U] \subset \mathbb{R}/\mathbb{Z}$ contains no non-trivial subgroup of $\mathbb{R}/\mathbb{Z}$.]

(c) Derive from (b) that the open additive subgroups U form a neighborhood base for 0 in R (see [11, Theorems 24.26 and 7.7]) and that the same is true for the open two-sided ideals.

(d) Conclude that $R \cong \varprojlim R/V$, the limit ranging over the open two-sided ideals $V \subset R$, and that R is profinite.

1.19 Let π be a profinite group acting on a set E. Prove that the action is continuous if and only if for each $e \in E$ the *stabilizer* $\pi_e = \{\sigma \in \pi : \sigma e = e\}$ is open in π, and for finite E if and only if the *kernel* $\pi' = \{\sigma \in \pi : \sigma e = e \text{ for all } e \in E\}$ of the action is open in π.

1.20 Let G be a group with profinite completion $\hat{G}$. Prove that the category of *finite* G-sets is equivalent to the category $\hat{G}$-**sets**.

1.21 (a) Prove that the category $\hat{\mathbb{Z}}$-**sets** is equivalent to the category whose objects are pairs (E, σ), with E a finite set and σ a permutation of E, a morphism from (E, σ) to (E', σ') being a map $f\colon E \to E'$ satisfying $f\sigma = \sigma' f$.

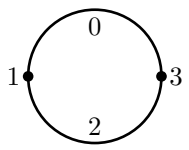
(b) Construct a profinite group π containing $\hat{\mathbb{Z}}$ as a closed normal subgroup of index 2, such that the category π-**sets** is equivalent to the category whose objects are triples (E, σ, τ), with E a finite set and σ and τ permutations of E for which $\sigma^2 = \tau^2 = \mathrm{id}_E$, a morphism from (E, σ, τ) to (E', σ', τ') being a map $f\colon E \to E'$ satisfying $f\sigma = \sigma' f$ and $f\tau = \tau' f$.

1.22 Let p be a prime number. Prove that $\pi(\operatorname{Spec} \mathbb{Z}[1/p])$ is infinite.

1.23 Let A be the ring of integers of an algebraic number field K. The *narrow ideal class group* C^* of K is the group of fractional A-ideals modulo the subgroup $\{A\alpha : \alpha \in K^*, \sigma(\alpha) > 0 \text{ for every field homomorphism } \sigma\colon K \to \mathbb{R}\}$. Let $\pi = \pi(\operatorname{Spec} A)$, and denote by π' the closure of the commutator subgroup of π. Prove that $\pi/\pi' \cong C^*$. [*Hint:* Use class field theory [5; 17].]

1.24 Let it be given that under the equivalence of categories in 1.14 finite coverings and finite sets correspond to each other. Deduce from this and Exercise 1.20 that the profinite group $\hat{\pi}(X)$ occurring in 1.15 is the profinite completion of the group $\pi(X)$ occurring in 1.14, if X is as in 1.14.

1.25 Let X be the topological space $\{0, 1, 2, 3\}$, the open sets being $\emptyset$, $\{0\}$, $\{2\}$, $\{0, 2\}$, $\{0, 1, 2\}$, $\{0, 3, 2\}$, X. Prove: $\hat{\pi}(X) \cong \hat{\mathbb{Z}}$.



1.26 (a) Let π be a profinite group such that $x^2 = 1$ for all $x \in \pi$. Prove that π is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\mathbf{n}}$ for a uniquely determined cardinal number $\mathbf{n}$, which is equal to the $\mathbb{Z}/2\mathbb{Z}$-dimension of the group of continuous group homomorphisms $\pi \to \mathbb{Z}/2\mathbb{Z}$.

(b) Let G be the additive group of a $\mathbb{Z}/2\mathbb{Z}$-vector space of dimension $\mathbf{k}$, where $\mathbf{k}$ is an infinite cardinal. Prove: $\hat{G} \cong (\mathbb{Z}/2\mathbb{Z})^{2^{\mathbf{k}}}$ as profinite groups.

(c) Construct a profinite group that is not isomorphic to the profinite completion of any abstract group.

1.27 Let X be an infinite topological space whose closed sets are exactly the finite subsets of X and X itself.

(a) Prove that every covering of X is trivial (see the Introduction), that X is connected, and that the group $\hat{\pi}(X)$ from 1.15 is trivial.

(b) Suppose that X is countable. Prove that X is not pathwise connected.

(c) Suppose that $\#X \geq \#\mathbb{R}$. Prove that X is locally pathwise connected and semilocally simply connected, and that $\pi(X)$ is trivial.

1.28 Let X be an irreducible topological space. Prove that the group $\hat{\pi}(X)$ from 1.15 is trivial.

1.29 Put $A = \mathbb{Z}[\sqrt{-3}]$, $B = \mathbb{Z}[X]/(X^4 + X^2 + 1)$ and $\beta = (X \bmod X^4 + X^2 + 1) \in B$. View B as an A-algebra via the ring homomorphism $A \to B$ mapping $\sqrt{-3}$ to $\beta - \beta^{-1}$. Prove that B is a free separable A-algebra.

1.30 Let p be a prime number, π the profinite group $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$, and $\pi' \subset \pi$ the closure of the subgroup generated by $(1 \bmod p^n)_{n=1}^{\infty}$.

(a) Prove that one has $\pi' \cong \mathbb{Z}_p$ as profinite groups, and that π' is a *pure* subgroup of π, i.e., $m\pi' = \pi' \cap m\pi$ for all $m \in \mathbb{Z}$.

(b) Prove that there is an isomorphism $\pi \cong \pi' \times (\pi/\pi')$ of abstract groups. [*Hint:* First look at finitely generated subgroups of π/π', next use compactness of π'.]

(c) Prove that π and $\pi' \times (\pi/\pi')$ are not isomorphic as profinite groups.

2 Galois theory for fields

In this section we explain the connection between the Main theorem 1.11 and classical Galois theory for fields. We denote by K a field. It is our purpose to show that the category of free separable K-algebras is anti-equivalent to the category of finite π-sets, for a certain profinite group π. This is a special case of the Main theorem, with $X = \operatorname{Spec} K$. In the general proof we shall use the contents of this section only for algebraically closed K. In that case, which is much simpler, the group π is trivial, so that the category of finite π-sets is just the category of finite sets.

We assume, in this section, familiarity with the theory of finite Galois extensions of fields.

2.1 Infinite Galois theory. Let $K \subset L$ be a field extension. We call $K \subset L$ a *Galois extension* if $K \subset L$ is algebraic and there exists a subgroup $G \subset \operatorname{Aut}(L)$ such that $K = L^G$; here we use the notation L^G from 1.10. If $K \subset L$ is a Galois extension we define the *Galois group* $\operatorname{Gal}(L/K)$ to be $\operatorname{Aut}_K(L)$; then we have $K = L^{\operatorname{Gal}(L/K)}$.

Let $\overline{K}$ be a fixed algebraic closure of K. If $F \subset K[X] - \{0\}$ is any collection of non-zero polynomials, the *splitting field* of F over K is the subfield of $\overline{K}$ generated by K and the zeros of the polynomials in F. We recall that $f \in K[X] - \{0\}$ is called *separable* if it has no multiple zero in $\overline{K}$, and that $\alpha \in \overline{K}$ is called *separable over* K if the irreducible polynomial of α over K is separable. We denote this irreducible polynomial by f_K^α. Let L be a subfield of $\overline{K}$ containing K. We call L *separable over* K if each $\alpha \in L$ is separable over K, and *normal* over K if for each $\alpha \in L$ the polynomial f_K^α splits completely in linear factors in $L[X]$.

2.2 Theorem. *Let K be a field, and L a subfield of $\overline{K}$ containing K. Denote by I the set of subfields E of L for which E is a finite Galois extension of K. Then I, when partially ordered by inclusion, is a directed partially ordered set. Moreover, the following four assertions are equivalent:*

(i) *L is a Galois extension of K;*
(ii) *L is normal and separable over K;*
(iii) *there is a set $F \subset K[X] - \{0\}$ of separable polynomials such that L is the splitting field of F over K;*
(iv) $\bigcup_{E \in I} E = L$.

Finally, if these conditions are satisfied, then there is a group isomorphism $\operatorname{Gal}(L/K) \cong \varprojlim_{E \in I} \operatorname{Gal}(E/K)$.

Remark. The projective limit, in the final assertion, is defined with respect to the natural restriction maps $\operatorname{Gal}(E/K) \to \operatorname{Gal}(E'/K)$, for $E, E' \in I$, $E' \subset E$. Since the groups

$\mathrm{Gal}(E/K)$, for $E \in I$ are *finite*, the isomorphism in the theorem shows that $\mathrm{Gal}(L/K)$ may be considered as a *profinite group*, as we shall do in the sequel. In particular, $\mathrm{Gal}(L/K)$ is *compact* and *Hausdorff.* The topology on $\mathrm{Gal}(L/K)$ is called the *Krull topology* (Wolfgang Krull, German mathematician, 1899–1971). See Exercise 2.3(a) for a different description of this topology.

Proof of 2.2. If $E, E' \in I$ then $EE' \in I$ so I is directed.

(i) $\Rightarrow$ (ii) Suppose that $K \subset L$ is Galois, with group G. Let $\alpha \in L$. Since α is algebraic over K, the orbit $G\alpha$ of α under G is finite. The polynomial $g = \prod_{\beta \in G\alpha}(X - \beta)$ has coefficients in $L^G = K$, and $g(\alpha) = 0$, so g is divisible by f_K^α. Since g splits completely into linear factors in $L[X]$, and has no multiple zeros, the same is true for f_K^α. (It is in fact easy to see that $g = f_K^\alpha$.) Therefore L is normal and separable over K.

(ii) $\Rightarrow$ (iii) Simply take $F = \{f_K^\alpha : \alpha \in L\}$.

(iii) $\Rightarrow$ (iv) For every *finite* set $F' \subset F$, the splitting field of F' over K belongs to I. The union of the fields in I obtained in this way is the splitting field of F over K, which is L.

(iv) $\Rightarrow$ (i) It suffices to construct, for each $\alpha \in L - K$, an element $\tau \in \mathrm{Aut}_K(L)$ for which $\tau(\alpha) \neq \alpha$. Choose $E_0 \in I$ with $\alpha \in E_0$. Since E_0 is finite Galois over K, there exists $\rho \in \mathrm{Gal}(E_0/K)$ with $\rho(\alpha) \neq \alpha$. Because $\overline{K}$ is an algebraic closure of E_0, the K-isomorphism $\rho\colon E_0 \xrightarrow{\sim} E_0$ can be extended to a K-isomorphism $\sigma\colon \overline{K} \xrightarrow{\sim} \overline{K}$. For each $E \in I$ we have $\sigma E = E$, since E is Galois over K. But $L = \bigcup_{E \in I} E$, so also $\sigma L = L$, and $\tau = \sigma|L$ is now the required K-automorphism of L with $\tau(\alpha) \neq \alpha$.

To prove the final assertion, we map $\mathrm{Gal}(L/K)$ to $\varprojlim_{E \in I} \mathrm{Gal}(E/K)$ by sending σ to $(\sigma|E)_{E \in I}$. It is straightforward to verify that this is a well-defined group isomorphism. This proves Theorem 2.2.

2.3 Main theorem of Galois theory. *Let $K \subset L$ be a Galois extension of fields with Galois group G. Then the set of intermediate fields of $K \subset L$ corresponds bijectively to the set of closed subgroups of G. More precisely, the maps*

$$\{E : E \text{ is a subfield of } L \text{ containing } K\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{H : H \text{ is a closed subgroup of } G\}$$

defined by

$$\phi(E) = \mathrm{Aut}_E(L), \qquad \psi(H) = L^H$$

are bijective and inverse to each other. This correspondence reverses the inclusion relations, K corresponds to G and L to $\{\mathrm{id}_L\}$. If E corresponds to H, then we have

(a) *$K \subset E$ is finite $\Leftrightarrow$ H is open; and $[E : K] = \mathrm{index}[G : H]$ if H is open;*

(b) *$E \subset L$ is Galois with* $\mathrm{Gal}(L/E) \cong H$ *(as topological groups);*
(c) *$\sigma[E]$ corresponds to $\sigma H \sigma^{-1}$, for every $\sigma \in G$;*
(d) *$K \subset E$ is Galois $\Leftrightarrow$ H is a normal subgroup of G; and* $\mathrm{Gal}(E/K) \cong G/H$ *(as topological groups) if $K \subset E$ is Galois.*

Proof. Let first E be an intermediate field. Since $K \subset L$ is normal and separable, the same is true for $E \subset L$, so $E \subset L$ is Galois and we can speak about $\mathrm{Gal}(L/E)$. Using that the sets

$$U_{\sigma,F} = \{\tau \in G : \tau|F = \sigma|F\} \subset G, \quad \text{for } \sigma \in G, \quad F \subset L, \quad \#F < \infty,$$

form a base for the open sets of G, and similarly for $\mathrm{Gal}(L/E)$, one easily sees that the inclusion map $\mathrm{Gal}(L/E) \to G$ is continuous. It follows that the image is *compact*, hence closed in G, so that the map ϕ is well defined. Also, since $E \subset L$ is Galois, we have $L^{\mathrm{Gal}(L/E)} = E$, so $\psi\phi(E) = E$.

Next let $H \subset G$ be a closed subgroup, $E = \psi(H) = L^H$, and $J = \phi\psi(H) = \mathrm{Aut}_E(L)$. We wish to prove $H = J$. The inclusion $H \subset J$ is obvious. Conversely, let $\sigma \in J$. In order to prove $\sigma \in H$ it suffices to show that σ is in the *closure* of H, which is H itself; in other words, given a finite subset $F \subset L$ it suffices to show that $U_{\sigma,F} \cap H \neq \emptyset$. Choose $M \in I$ (see 2.2) with $F \subset M$. Restricting the elements of H to M we obtain a subgroup H' of the finite group $\mathrm{Gal}(M/K)$, and $M^{H'} = L^H \cap M = E \cap M$. By the main theorem of finite Galois theory, the extension $M^{H'} \subset M$ is Galois with group H'. But $\sigma|M$ is the identity on $E \cap M = M^{H'}$, so $\sigma|M \in \mathrm{Gal}(M/M^{H'}) = H'$. Hence $\sigma|M = \tau|M$ for some $\tau \in H$, and therefore $\tau \in U_{\sigma,F} \cap H$, as required.

This completes the proof that ϕ and ψ are bijective and inverse to each other. It is clear that they reverse inclusions, that $\phi(K) = G$ and that $\psi(\{\mathrm{id}_L\}) = L$.

Let E correspond to H. The map that assigns to each $\sigma \in G$ its restriction to E yields in an obvious way an injective map

$$G/H \to \{\tau \colon E \to L : \tau \text{ is a field homomorphism, } \tau|K = \mathrm{id}_K\}.$$

This map is also surjective, since each $\tau \colon E \xrightarrow{\sim} \tau[E] \subset L$, $\tau|K = \mathrm{id}_K$, can be extended to an automorphism ρ of the algebraic closure, and then $\rho|L \in \mathrm{Gal}(L/K)$ since $K \subset L$ is normal.

We conclude that the above map is *bijective.* If $K \subset E$ is finite, then the number of field homomorphisms $\tau \colon E \to L$ with $\tau|K = \mathrm{id}_K$ is $[E : K]$, so then H is of finite index $[E : K]$ in G; since H and its cosets are closed this implies that H is open. Conversely, suppose that H is open. Since G is compact, H is of finite index in G. By the above, there are precisely $\mathrm{index}[G : H]$ field homomorphisms $\tau \colon E \to L$ with $\tau|K = \mathrm{id}_K$. It follows that for any *finite* extension $K \subset E'$ with $E' \subset E$ there are at most $\mathrm{index}[G : H]$ field homomorphisms

$\tau\colon E' \to L$ with $\tau|K = \mathrm{id}_K$, since any such τ can be extended to E. Hence $[E' : K] \leq \mathrm{index}[G : H]$ for all those E', and since E is the union of all E' this implies that $[E : K]$ is finite. This proves (a).

Above we saw already that there is a continuous bijection $\mathrm{Gal}(L/E) \to H$. Since each continuous bijection from a compact space to a Hausdorff space is a homeomorphism this proves (b).

Assertion (c) is proved as in finite Galois theory.

By 2.2, the extension $K \subset E$ is Galois if and only if it is normal, so if and only if $\sigma[E] = E$ for all $\sigma \in G$. By (c) this occurs if and only if H is normal in G. Suppose that these conditions are satisfied. Then the set of field homomorphisms $\tau\colon E \to L$ with $\tau|K = \mathrm{id}_K$ may be identified with $\mathrm{Gal}(E/K)$. Hence we have a bijection $G/H \xrightarrow{\sim} \mathrm{Gal}(E/K)$, which is easily checked to be a continuous group homomorphism, if we give G/H the quotient topology. As in (b) it follows that the map is a homeomorphism. This proves (d).

This concludes the proof of 2.3.

2.4 Separable closure. Let K be a field, and $\overline{K}$ an algebraic closure of K. The *separable closure* K_s of K is defined by

$$K_s = \{x \in \overline{K} : x \text{ is separable over } K\}.$$

This is a subfield of $\overline{K}$, and $K_s = \overline{K}$ if and only if K is perfect; in particular, $K_s = \overline{K}$ if $\mathrm{char}(K) = 0$. From 2.2 it follows that $K \subset K_s$ is Galois. The Galois group $\mathrm{Gal}(K_s/K)$ is called the *absolute Galois group* of K.

Observe that any finite separable field extension $K \subset E$ can be embedded in K_s. Using 2.3(a), (c) we conclude that there is a bijective correspondence between the set of isomorphism classes of finite separable extension fields E of K and the set of conjugacy classes of open subgroups of the absolute Galois group of K.

2.5 Example. Let $\mathbb{F}_q$ be a *finite* field, with $\#\mathbb{F}_q = q$ and with algebraic closure $\overline{\mathbb{F}}_q$. The only finite extensions of $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$ are the fields $\mathbb{F}_{q^n} = \{\alpha \in \overline{\mathbb{F}}_q : \alpha^{q^n} = \alpha\}$ for $n \in \mathbb{Z}$, $n \geq 1$. Each $\mathbb{F}_{q^n}$ is Galois over $\mathbb{F}_q$, with $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$, the generator of $\mathbb{Z}/n\mathbb{Z}$ corresponding to the Frobenius automorphism F with $F(\alpha) = \alpha^q$ for all α. Taking projective limits, we see that the absolute Galois group of $\mathbb{F}_q$ is isomorphic to $\hat{\mathbb{Z}}$, with $1 \in \hat{\mathbb{Z}}$ corresponding to $F \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. The closure of the subgroup generated by F is equal to the whole group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. This is expressed by saying that F is a *topological generator* of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

2.6 Finite algebras. Theorem. *Let B be a finite dimensional algebra over a field K. Then $B \cong \prod_{i=1}^{t} B_i$ for some $t \in \mathbb{Z}_{\geq 0}$ and certain K-algebras B_i that are local with nilpotent maximal ideals.*

Proof. If B is a *domain*, then for any $b \in B - \{0\}$, the map $B \to B$, $x \mapsto bx$, is injective, so by dimension considerations also surjective, so that $b \in B^*$. This shows that B is a field if it is a domain. Applying this to $B/\mathfrak{p}$, for $\mathfrak{p} \subset B$ prime, we see that any prime ideal $\mathfrak{p}$ of B is *maximal.* If $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ are distinct maximal ideals of B, then by the Chinese remainder theorem the natural map $B \to \prod_{i=1}^n B/\mathfrak{m}_i$ is surjective, so $n \leq \dim_K B$. This shows that B has only finitely many maximal ideals, say $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_t$. The intersection $\bigcap_{i=1}^t \mathfrak{m}_i$ is the intersection of all prime ideals of B, so it is the nilradical $\sqrt{0}$ of B. Since B is obviously noetherian, the ideal $\sqrt{0}$ is nilpotent, so $\prod_{i=1}^t \mathfrak{m}_i^N = 0$ for N sufficiently large. The $\mathfrak{m}_i$ are pairwise relatively prime, so the same is true for the $\mathfrak{m}_i^N$, and the Chinese remainder theorem therefore gives an isomorphism $B \xrightarrow{\sim} \prod_{i=1}^t B/\mathfrak{m}_i^N$. Here $B_i = B/\mathfrak{m}_i^N$ is local, since $\mathfrak{m}_i/\mathfrak{m}_i^N$ is its only maximal ideal, and it is clearly nilpotent. This proves 2.6.

The decomposition in 2.6 is uniquely determined, see Exercise 2.23.

A similar theorem, with a slightly more complicated proof, is true for Artin rings, see [1, Chapter 8].

2.7 Separable algebras. Theorem. *Let K be a field with algebraic closure $\overline{K}$, and let B be a finite dimensional K-algebra. Denote by $\overline{B}$ the $\overline{K}$-algebra $B \otimes_K \overline{K}$. Then the following four assertions are equivalent:*

(i) *B is separable over K;*
(ii) *$\overline{B}$ is separable over $\overline{K}$;*
(iii) *$\overline{B} \cong \overline{K}^n$ as $\overline{K}$-algebras, for some $n \geq 0$;*
(iv) *$B \cong \prod_{i=1}^t B_i$ as K-algebras, where each B_i is a finite separable field extension of K.*

Proof. (i) $\Leftrightarrow$ (ii) Let $w_1, w_2, \ldots, w_n$ be a K-basis for B. Then $w_1 \otimes 1, w_2 \otimes 1, \ldots, w_n \otimes 1$ is a $\overline{K}$-basis for $\overline{B}$. It follows that the diagram

$$\begin{array}{ccc} B & \hookrightarrow & \overline{B} \\ {\scriptstyle \mathrm{Tr}_{B/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{\overline{B}/\overline{K}}} \\ K & \hookrightarrow & \overline{K} \end{array}$$

(the horizontal arrows are the natural inclusions) is commutative. Hence $\mathrm{Tr}_{B/K}(w_i w_j) = \mathrm{Tr}_{\overline{B}/\overline{K}}((w_i \otimes 1)(w_j \otimes 1))$, and (i) $\Leftrightarrow$ (ii) now follows from Exercise 1.3.

(iii) $\Rightarrow$ (ii) is obvious (cf. 1.3).

(ii) $\Rightarrow$ (iii) Applying 2.6 to $\overline{K}, \overline{B}$ we see that $\overline{B} \cong \prod_{j=1}^u C_j$ for certain local $\overline{K}$-algebras C_j with nilpotent maximal ideals $\mathfrak{m}_j$. Since $\overline{B}$ is separable over $\overline{K}$ it clearly follows that each C_j is separable over $\overline{K}$. Let j be fixed, and let $\phi\colon C_j \to \overline{K}$ be any $\overline{K}$-linear function. By 1.2 there exists $c \in C_j$ with $\phi(x) = \mathrm{Tr}(cx)$ for all $x \in C_j$. Taking $x \in \mathfrak{m}_j$ and observing that

nilpotent maps have trace zero (over a field), we see that $\mathfrak{m}_j \subset \ker \phi$. This is true for each ϕ, so $\mathfrak{m}_j = \{0\}$ and C_j is a *field.* Since C_j is finite over $\overline{K}$ and $\overline{K}$ is algebraically closed we conclude $C_j = \overline{K}$, as required.

(iv) $\Rightarrow$ (iii) By the theorem of the primitive element we have $B_i = K(\beta_i) \cong K[X]/(f_i)$ with $f_i \in K[X]$ separable and irreducible. Hence $\overline{B}_i \cong \overline{K}[X]/(f_i)$, and since f_i splits into distinct linear factors $X - \alpha_{ij}$ in $\overline{K}[X]$ the Chinese remainder theorem now implies that $\overline{B}_i \cong \prod_j \overline{K}[X]/(X - \alpha_{ij}) \cong \overline{K}^{\deg(f_i)}$. This implies (iii).

(iii) $\Rightarrow$ (iv) Write $B = \prod_{i=1}^t B_i$ as in 2.6. For each $b \in B$ the subalgebra $K[b]$ generated by b is isomorphic to $K[X]/(f_b)$ for some $f_b \in K[X] - \{0\}$. Tensoring the injective map $K[X]/(f_b) \cong K[b] \subset B$ with $\overline{K}$ we find an injective map $\overline{K}[X]/(f_b) \to \overline{B}$. Thus by (iii) it follows that $\overline{K}[X]/(f_b)$ has no non-zero nilpotent elements, which means that f_b is a separable polynomial. In particular, if b is nilpotent then $X^n \in (f_b)$ for some n, so $X \in (f_b)$ and $b = 0$. This implies that all B_i are *fields.* If $b = (b_1, \ldots, b_t) \in \prod_{i=1}^t B_i = B$ is arbitrary then f_b equals the lcm of the irreducible polynomials of the b_i over K, so these are all separable. Therefore all B_i are separable field extensions of K, as required. (See also Exercise 2.24.)

This proves 2.7.

The technique used in this proof of making an algebra trivial by means of an extension of the base ring will later play an important role.

2.8 Remark. Let K be a field, and π its absolute Galois group (see 2.4). Combining 2.7, (i) $\Leftrightarrow$ (iv), with the remark made in 2.4 we see that giving a free separable K-algebra B is equivalent to giving a finite sequence of conjugacy classes of open subgroups of π, uniquely determined up to order. Decomposing a finite π-set (see 1.10) into orbits under π we see that finite π-sets are specified by exactly the same data, a finite sequence $\pi_1, \pi_2, \ldots, \pi_t$ of open subgroups of π corresponding to the disjoint union of the π-sets π/π_i. This yields a one-to-one correspondence between free separable K-algebras and finite π-sets. A more formal statement appears in the following theorem, where the correspondence is extended to morphisms between the objects.

2.9 Theorem. *Let K be a field and π its absolute Galois group (see* 2.4*). Then the categories* ${}_K\mathbf{SAlg}$ *of free separable K-algebras and* π**-sets** *of finite sets with a continuous action of π are anti-equivalent.*

Remark. It is clear from the definition in 1.4 that ${}_K\mathbf{SAlg}$ is anti-equivalent to $\mathbf{FEt}_{\operatorname{Spec} K}$. So Theorem 2.9 is exactly the case $X = \operatorname{Spec} K$ of the Main theorem 1.11, except for the uniqueness statement in 1.11.

Proof. The statement of the theorem means that there are contravariant functors $F\colon {}_K\mathbf{SAlg} \to \pi\text{-}\mathbf{sets}$ and $G\colon \pi\text{-}\mathbf{sets} \to {}_K\mathbf{SAlg}$ such that FG and GF are naturally equivalent to the identity functors on π-**sets** and ${}_K\mathbf{SAlg}$, respectively. This in turn means, for GF, that there is a collection of isomorphisms $\theta_B\colon B \to GF(B)$, one for each object B of ${}_K\mathbf{SAlg}$, such that for any morphism $f\colon B \to C$ in ${}_K\mathbf{SAlg}$, the diagram

$$\begin{array}{ccc} B & \xrightarrow{\quad f \quad} & C \\ {\scriptstyle\theta_B}\downarrow & & \downarrow{\scriptstyle\theta_C} \\ GF(B) & \xrightarrow{GF(f)} & GF(C) \end{array}$$

is commutative; and analogously for FG.

We shall now first define F. Let K_s be a separable closure of K, so that $\pi = \mathrm{Gal}(K_s/K)$. For each free separable B-algebra, let

$$F(B) = \mathrm{Alg}_K(B, K_s),$$

the set of K-algebra homomorphisms $B \to K_s$. If $g\colon B \to K_s$ is such a homomorphism and $\sigma \in \pi$, then $\sigma \circ g\colon B \to K_s$ is also such a homomorphism. This provides us with an action of the abstract group π on $\mathrm{Alg}_K(B, K_s)$. In order to see that this action is continuous, and that $\mathrm{Alg}_K(B, K_s)$ is a *finite* π-set (see 1.10), we write $B = \prod_{i=1}^{t} B_i$ as in 2.7(iv), and viewing B_i as a subfield of K_s we write $B_i = K_s^{\pi_i}$ with $\pi_i \subset \pi$ an open subgroup (see 2.4), for each i. Then $\mathrm{Alg}_K(B, K_s)$ may be identified with the disjoint union of the sets $\mathrm{Alg}_K(K_s^{\pi_i}, K_s)$, for $1 \leq i \leq t$. Here $\mathrm{Alg}_K(K_s^{\pi_i}, K_s)$ is the set of field homomorphisms $K_s^{\pi_i} \to K_s$ that are the identity on K, and as we have seen in the proof of the Main theorem 2.3 (with G, H, E, L for $\pi, \pi_i, K_s^{\pi_i}, K_s$) this set may be identified with π/π_i; and clearly this identification respects the π-action. We conclude that $\mathrm{Alg}_K(B, K_s)$ may be identified with the disjoint union $\coprod_{i=1}^{t} \pi/\pi_i$, and since the π_i are open in π this is a finite set on which π acts continuously.

This proves that $F(B)$ is an object of π-**sets.** Let $f\colon B \to C$ be a morphism in ${}_K\mathbf{SAlg}$, i.e., a K-algebra homomorphism from a free separable K-algebra B to a free separable K-algebra C. Then we define $F(f)\colon F(C) \to F(B)$ by $F(f)(g) = g \circ f$, for a K-algebra homomorphism $g\colon C \to K_s$. This is evidently a morphism of π-sets, and it is now straightforward to verify that F is a contravariant functor ${}_K\mathbf{SAlg} \to \pi\text{-}\mathbf{sets}$.

Next we define G. For a finite π-set E, let

$$G(E) = \mathrm{Mor}_\pi(E, K_s),$$

the set of morphisms of π-sets $E \to K_s$; this makes sense, since the underlying set of K_s is

a π-set. The K-algebra structure on K_s induces a K-algebra structure on $G(E)$, by

$$\begin{aligned}(f+g)(e) = f(e) + g(e), \qquad (fg)(e) = f(e)g(e),\\ (kf)(e) = k \cdot f(e), \qquad 1(e) = 1\end{aligned}$$

for all $f, g \in G(E)$, $k \in K$, $e \in E$. In order to see that $G(E)$ is *finite dimensional* and *separable* as a K-algebra we decompose E into its orbits under π, say $E = \coprod_{i=1}^{t} E_i$. Then $G(E)$ may be identified with the product of the K-algebras $G(E_i)$, for $1 \leq i \leq t$. As a π-set, we may identify E_i with π/π_i for some open subgroup $\pi_i \subset \pi$, see Exercise 1.19. Each morphism of π-sets $g\colon \pi/\pi_i \to K_s$ must be given by $g(\sigma\pi_i) = \sigma(a)$ for some $a \in K_s$ (namely, $a = g(\pi_i)$), and conversely if $a \in K_s$ then this is a well defined map of π-sets if and only if $a \in K_s^{\pi_i}$. Thus we see that $\mathrm{Mor}_\pi(\pi/\pi_i, K_s)$ may be identified with $K_s^{\pi_i}$, and this is an identification of K-algebras. We conclude that $G(E) \cong \prod_{i=1}^{t} K_s^{\pi_i}$, and by 2.3(a) and 2.7 this is a finite dimensional separable K-algebra.

If $f\colon E \to D$ is a morphism of π-sets then $G(f)\colon G(D) \to G(E)$, $G(f)(g) = g \circ f$, is a morphism of K-algebras, and this makes G into a contravariant functor π-**sets** $\to {}_K\mathbf{SAlg}$.

The functors F and G let $\prod_{i=1}^{t} K_s^{\pi_i}$ and $\coprod_{i=1}^{t} \pi/\pi_i$ correspond to each other, so clearly $B \cong GF(B)$ and $E \cong FG(E)$ for any free separable K-algebra B and any finite π-set E. We must now choose these isomorphisms in such a way that they are well behaved with respect to morphisms, as made precise at the beginning of this proof.

For a free separable K-algebra B, define

$$\theta_B\colon B \to GF(B) = \mathrm{Mor}_\pi(\mathrm{Alg}_K(B, K_s), K_s)$$

by $\theta_B(b)(g) = g(b)$, for $b \in B$ and $g \in \mathrm{Alg}_K(B, K_s)$. This is easily seen to be a well-defined K-algebra homomorphism. If $f\colon B \to C$ is a morphism in ${}_K\mathbf{SAlg}$ then the diagram

$$\begin{array}{ccc} B & \xrightarrow{\quad f \quad} & C \\ {\scriptstyle\theta_B}\downarrow & & \downarrow{\scriptstyle\theta_C} \\ GF(B) & \xrightarrow{GF(f)} & GF(C) \end{array}$$

is commutative, since for $b \in B$ and $g \in \mathrm{Alg}_K(C, K_s)$ we have

$$\begin{aligned}(\theta_C \circ f)(b)(g) &= \theta_C(f(b))(g) = g(f(b)),\\ \{[GF(f)](\theta_B(b))\}(g) &= \{\theta_B(b) \circ F(f)\}(g)\\ &= \theta_B(b)(g \circ f) = g \circ f(b) = g(f(b)).\end{aligned}$$

For $B = \prod_{i=1}^{t} K_s^{\pi_i}$ one checks in a straightforward way that θ_B is an isomorphism. Hence θ_B is an isomorphism for all B, and GF is naturally equivalent to the identity functor of ${}_K\mathbf{SAlg}$.

The proof that FG is naturally equivalent to the identity functor of π-**sets** is completely analogous. For a finite π-set E, one defines

$$\eta_E \colon E \to FG(E) = \mathrm{Alg}_K(\mathrm{Mor}_\pi(E, K_s), K_s)$$

by $\eta_E(e)(g) = g(e)$, for $e \in E$ and $g \in \mathrm{Mor}_\pi(E, K_s)$. This is easily seen to be a well-defined morphism of π-sets, and if $f \colon E \to D$ is a morphism of π-sets then by a calculation similar to the above one the diagram

$$\begin{array}{ccc} E & \xrightarrow{\quad f \quad} & D \\ {\scriptstyle \eta_E}\downarrow & & \downarrow{\scriptstyle \eta_D} \\ FG(E) & \xrightarrow{FG(f)} & FG(D) \end{array}$$

is commutative. For $E = \coprod_{i=1}^{t} \pi/\pi_i$ the map η_E is an isomorphism, so this is true for all E, as required.

This completes the proof of Theorem 2.9.

Exercises for Section 2

2.1 Let $K \subset L$ be a Galois extension of fields, and I a set of subfields $E \subset L$ with $K \subset E$ for which

$$[E : K] < \infty \ \text{ for every } E \in I$$
$$\bigcup_{E \in I} E = L.$$

Prove that I, when partially ordered by inclusion, is *directed* (see 1.7).

2.2 Let $K \subset L$ be a Galois extension of fields, and I any directed set of subfields $E \subset L$ with $K \subset E$ Galois for which $\bigcup_{E \in I} E = L$. Prove that there is an isomorphism of profinite groups $\mathrm{Gal}(L/K) \cong \varprojlim_{E \in I} \mathrm{Gal}(E/K)$. (N.B.: the groups $\mathrm{Gal}(E/K)$ need not be finite here, they are merely profinite.)

2.3 (a) Let $K \subset L$ be a Galois extension of fields, with Galois group G. View G as a subset of the set L^L of *all* functions $L \to L$. Let L be given the discrete topology and L^L the product topology. Prove that the topology of the profinite group G coincides with the relative topology inside L^L.

(b) Conversely, let L be any field and $G \subset \mathrm{Aut}(L)$ a subgroup that is compact when viewed as a subset of L^L (topologized as in (a)). Prove that $L^G \subset L$ is Galois with Galois group G.

(c) Prove that any profinite group is isomorphic to the Galois group of a suitably chosen Galois extension of fields.

2.4 Let $K \subset L$ be a Galois extension of fields. Prove that $\mathrm{Gal}(L/K)$ is not countably infinite.

2.5 Let $K \subset L$ be a Galois extension of fields, $S \subset \mathrm{Gal}(L/K)$ any subset, and $E = \{x \in L : \forall \sigma \in S : \sigma(x) = x\}$. Prove that $\mathrm{Gal}(L/E)$ is the closure of the subgroup of $\mathrm{Gal}(L/K)$ generated by S.

2.6 Let $K \subset L$ be a Galois extension of fields, and $H' \subset H \subset \mathrm{Gal}(L/K)$ closed subgroups with $\mathrm{index}[H : H'] < \infty$. Prove that $L^H \subset L^{H'}$ is finite, and that $[L^{H'} : L^H] = \mathrm{index}[H : H']$. Which part of the conclusion is still true if H', H are *not* necessarily closed?

2.7 Let K, L, F be subfields of a field Ω, and suppose that $K \subset L$ is Galois and that $K \subset F$. Prove that $F \subset L \cdot F$ is Galois, and that $\mathrm{Gal}(L \cdot F/F) \cong \mathrm{Gal}(L/L \cap F)$ (as topological groups).

2.8 Let K be a field. Prove that for every Galois extension $K \subset L$ the group $\mathrm{Gal}(L/K)$ is isomorphic to a quotient of the absolute Galois group of K.

2.9 (a) Suppose that H is a *finite* subgroup of the absolute Galois group of a field K. Prove that $\#H \leq 2$ and $\#H = 1$ if $\mathrm{char}(K) > 0$. [*Hint:* [15, Theorem 56].]

(b) Let K be a field with separable closure K_s, and $\alpha \in K_s$, $\alpha \notin K$. Let E be a subfield of K_s containing K that is maximal with respect to the property of not containing α. Prove that $\mathrm{Gal}(K_s/E) \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathrm{Gal}(K_s/E) \cong \mathbb{Z}_p$ for some prime number p.

2.10 A *Steinitz number* or *supernatural number* is a formal expression $a = \prod_{p \text{ prime}} p^{a(p)}$, where $a(p) \in \{0, 1, 2, \ldots, \infty\}$ for each prime number p. If $a = \prod_p p^{a(p)}$ is a Steinitz number, we denote by $a\hat{\mathbb{Z}}$ the subgroup of $\hat{\mathbb{Z}}$ corresponding to $\prod_p p^{a(p)}\mathbb{Z}_p$ (with $p^\infty\mathbb{Z}_p = \{0\}$) under the isomorphism $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ (Exercise 1.14).

(a) Prove that the map $a \mapsto a\hat{\mathbb{Z}}$ from the set of Steinitz numbers to the set of closed subgroups of $\hat{\mathbb{Z}}$ is bijective. Prove also that $a\hat{\mathbb{Z}}$ is open if and only if a is *finite* (i.e., $\sum_p a(p) < \infty$).

(b) Let $\mathbb{F}_q$ be a finite field, with algebraic closure $\overline{\mathbb{F}}_q$. For a Steinitz number a, let $\mathbb{F}_{q^a}$ be the set of all $x \in \overline{\mathbb{F}}_q$ for which $[\mathbb{F}_q(x) : \mathbb{F}_q]$ divides a (in an obvious sense). Prove that the map $a \mapsto \mathbb{F}_{q^a}$ is a bijection from the set of Steinitz numbers to the set of intermediate fields of $\mathbb{F}_q \subset \overline{\mathbb{F}}_q$. [Ernst Steinitz, German mathematician, 1871–1928.]

2.11 Let G be a profinite group. We call G *procyclic* if there exists $\sigma \in G$ such that the subgroup generated by σ is dense in G. Prove that the following assertions are equivalent:

(i) G is procyclic;

(ii) G is the projective limit of a projective system of finite cyclic groups;

(iii) $G \cong \hat{\mathbb{Z}}/a\hat{\mathbb{Z}}$ for some Steinitz number a (Exercise 2.10);

(iv) for any pair of open subgroups $H, H' \subset G$ with $\mathrm{index}[G : H] = \mathrm{index}[G : H']$ we have $H = H'$.

Prove also that the Steinitz number a in (iii) is unique if it exists.

2.12 Let K be a field with separable closure K_s. Prove that the absolute Galois group of K is procyclic (see Exercise 2.11) if and only if K has, for any positive integer n, at most one extension of degree n within K_s; and that it is isomorphic to $\hat{\mathbb{Z}}$ if and only if K has, for any positive integer n, exactly one extension of degree n within K_s.

2.13 (a) Let E be a torsion abelian group. Prove that E has exactly one $\hat{\mathbb{Z}}$-module structure, and that the scalar multiplication $\hat{\mathbb{Z}} \times E \to E$ defining this module structure is continuous, if E is given the discrete topology.

(b) Let E be the group of roots of unity in $\overline{\mathbb{Q}}^*$. Prove that the map $\hat{\mathbb{Z}}^* \to \mathrm{Aut}(E)$ induced by (a) is an isomorphism of groups.

(c) Write $\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(E)$, with E as in (b). Prove that $\mathbb{Q} \subset \mathbb{Q}(\zeta_\infty)$ is Galois, and that the natural map $\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \to \mathrm{Aut}(E) \cong \hat{\mathbb{Z}}^*$ is an isomorphism of topological groups.

(d) Prove that there are isomorphisms

$$\hat{\mathbb{Z}}^* \cong \prod_{p \text{ prime}} \mathbb{Z}_p^* \cong \hat{\mathbb{Z}} \times (\mathbb{Z}/2\mathbb{Z}) \times \prod_{p \text{ prime}} (\mathbb{Z}/(p-1)\mathbb{Z})$$

of topological groups.

2.14 Let $\mathbb{Q}(\sqrt{\overline{\mathbb{Q}}})$ be the subfield of $\overline{\mathbb{Q}}$ generated by $\{\sqrt{x} : x \in \mathbb{Q}\}$. Prove that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{\overline{\mathbb{Q}}})$ is Galois, and that the map

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\sqrt{\overline{\mathbb{Q}}})/\mathbb{Q}) &\to \mathrm{Hom}(\mathbb{Q}^*, \{\pm 1\}), \\ \sigma &\mapsto (a \mapsto \sigma(\sqrt{a})/\sqrt{a}) \end{aligned}$$

(for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{\overline{\mathbb{Q}}})/\mathbb{Q})$ and $a \in \mathbb{Q}^*$) is an isomorphism of topological groups, if $\mathrm{Hom}(\mathbb{Q}^*, \{\pm 1\})$ has the relative topology inside $\{\pm 1\}^{\mathbb{Q}^*}$. Prove also that this Galois group is isomorphic to the product of a countably infinite collection of copies of $\{\pm 1\}$.

2.15 Let $a \in \mathbb{Q}^*$, $n \in \hat{\mathbb{Z}}^*$, and write $a = b/c$, $b, c \in \mathbb{Z} - \{0\}$. Prove that there is a sequence $(n_i)_{i=0}^{\infty}$ of integers n_i for which

$$\begin{aligned} &n_i > 0, \quad \gcd(n_i, 2bc) = 1 \text{ for } i \geq 0, \\ &n = \lim_{i \to \infty} n_i \text{ in } \hat{\mathbb{Z}}. \end{aligned}$$

Define the Jacobi symbol $\left(\frac{a}{n}\right) \in \{\pm 1\}$ by $\left(\frac{a}{n}\right) \in \{\pm 1\}$ by $\left(\frac{a}{n}\right) = \lim_{i \to \infty} \left(\frac{b}{n_i}\right)/\left(\frac{c}{n_i}\right)$, where $\left(\frac{b}{n_i}\right), \left(\frac{c}{n_i}\right)$ are the ordinary Jacobi symbols. Prove that this is well-defined and independent of the choices made. Prove also that the map $\mathbb{Q}^* \times \hat{\mathbb{Z}}^* \to \{\pm 1\}$, $(a, n) \mapsto \left(\frac{a}{n}\right)$, is continuous and bimultiplicative ($\mathbb{Q}^*$ has the discrete topology).

2.16 Let the notation be as in Exercises 2.13, 2.14, and 2.15. Prove that $\mathbb{Q}(\sqrt{\overline{\mathbb{Q}}}) \subset \mathbb{Q}(\zeta_\infty)$, and that the induced homomorphism

$$\hat{\mathbb{Z}}^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{\overline{\mathbb{Q}}})/\mathbb{Q}) \cong \mathrm{Hom}(\mathbb{Q}^*, \{\pm 1\})$$

maps $n \in \hat{\mathbb{Z}}^*$ to the homomorphism sending $a \in \mathbb{Q}^*$ to $\left(\frac{a}{n}\right)$.

2.17 (**Kummer theory.**) Let K be a field with algebraic closure $\overline{K}$ and m a positive integer. Suppose that K contains a primitive m-th root of unity ζ_m, and let $E_m \subset K^*$ be the subgroup generated by ζ_m. Prove that there is a bijective correspondence between the collection of subfields $L \subset \overline{K}$ for which

$$K \subset L \text{ is Galois, } \mathrm{Gal}(L/K) \text{ is abelian, } \forall\, \sigma \in \mathrm{Gal}(L/K) : \sigma^m = \mathrm{id}_L$$

and the collection of subgroups $W \subset K^*$ for which $K^{*m} \subset W$; this correspondence maps L to $L^{*m} \cap K^*$ and W to $K(W^{1/m})$. Prove also that if L corresponds to W, there is an isomorphism of topological groups $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}(W/K^{*m}, E_m)$ mapping σ to $(\alpha K^{*m} \mapsto \sigma(\alpha^{1/m})/\alpha^{1/m})$; here $\mathrm{Hom}(W/K^{*m}, E_m)$ has the relative topology in $(E_m)^{W/K^{*m}}$, where each E_m is discrete.

2.18 (**Artin-Schreier theory.**) Let K be a field with algebraic closure $\overline{K}$, and let $p = \mathrm{char}(K) > 0$. Prove that there is a bijective correspondence between the collection of subfields $L \subset \overline{K}$ for which

$$K \subset L \text{ is Galois, } \mathrm{Gal}(L/K) \text{ is abelian, } \forall\, \sigma \in \mathrm{Gal}(K/L) : \sigma^p = \mathrm{id}_L$$

and the collection of additive subgroups $W \subset K$ for which $\wp[K] \subset W$, where $\wp\colon \overline{K} \to \overline{K}$ is defined by $\wp(x) = x^p - x$; this correspondence maps L to $\wp[L] \cap K$ and W to $K(\wp^{-1}[W])$. Prove also that if L corresponds to W, there is an isomorphism of topological groups $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}(W/\wp[K], \mathbb{F}_p)$ mapping σ to $(\alpha + \wp[K] \to \sigma(\beta) - \beta$, where $\wp(\beta) = \alpha)$.

2.19 Let K be a field, K_s its separable closure, m a positive integer not divisible by $\mathrm{char}(K)$ and w the number of m-th roots of unity in K.

(a) Let for $\tau \in \mathrm{Gal}(K_s/K)$ the integer $c(\tau)$ be such that $\tau(\zeta_m) = \zeta_m^{c(\tau)}$, where ζ_m denotes a primitive m-th root of unity. Prove that w is the greatest common divisor of m and all numbers $c(\tau) - 1$, $\tau \in \mathrm{Gal}(K_s/K)$.

(b) (**Schinzel's theorem.**) Let $a \in K$. Prove that the splitting field of $X^m - a$ over K is abelian over K if and only if $a^w = b^m$ for some $b \in K$. [*Hint* for the "only if" part: if $\alpha^m = a \neq 0$, prove that $a^{c(\tau)}/\tau(\alpha) \in K^*$ for all τ.]

In the following two exercises we shall study the Galois group of

$$L = \mathbb{Q}(\sqrt[\infty]{\mathbb{Q}}) = \mathbb{Q}(\alpha \in \overline{\mathbb{Q}} : \exists m \in \mathbb{Z}_{>0} : \alpha^m \in \mathbb{Q})$$

over $\mathbb{Q}$. We write

M = $\mathbb{Q}(\zeta_\infty)$ (see Exercise 2.13(c)),
E_m = (group of m-th roots of unity) $\subset M^*$,
Q = multiplicative group of positive rational numbers.

If A is a multiplicatively written abelian group, we write $A^m = \{a^m : a \in A\}$ for $m \in \mathbb{Z}$.

2.20 (a) Prove that $Q \cap M^{*m} = Q^{m/\gcd(m,2)}$. [*Hint:* Exercise 2.19.]

(b) Let $L_m = M(\alpha \in \overline{\mathbb{Q}} : \alpha^m \in \mathbb{Q})$, for $m \in \mathbb{Z}_{>0}$. Prove that $M \subset L_m$ is Galois, and that there is an isomorphism of topological groups

$$\mathrm{Gal}(L_m/M) \xrightarrow{\sim} \mathrm{Hom}(Q, E_m^{\gcd(m,2)})$$

mapping σ to $(a \mapsto \sigma(a^{1/m})/a^{1/m})$.

(c) Define $E_m \to E_n$ by $\zeta \mapsto \zeta^{m/n}$ for n dividing m, and let $\hat{E} = \varprojlim E_n$ with respect to these maps. Prove that $\hat{E} \cong \hat{\mathbb{Z}}$ as topological groups.

(d) Prove that $M \subset L$ is Galois and that the isomorphisms in (b) combine to yield an isomorphism of topological groups

$$\mathrm{Gal}(L_m/M) \xrightarrow{\sim} \mathrm{Hom}(Q, \hat{E}^2) \ ;$$

here $\mathrm{Hom}(Q, \hat{E}^2)$ has the relative topology in $(\hat{E}^2)^Q$. Prove also that this Galois group is isomorphic to the product of a countably infinite collection of copies of $\hat{\mathbb{Z}}$.

2.21 (a) Prove that there is a function $Q \times (\mathbb{Z}_{>0}) \to L^*$ such that, if the image of (a, n) is denoted by $a^{1/n}$, we have

$$(a^{1/n})^n = a \ , \qquad (ab)^{1/n} = a^{1/n}\, b^{1/n} \ , \qquad (a^{1/m})^{m/n} = a^{1/n}$$

for all $a, b \in Q$ and $n, m \in \mathbb{Z}_{>0}$ with n dividing m.

(b) Let Γ be the semidirect product $\mathrm{Hom}(Q, \hat{E}) \rtimes \hat{\mathbb{Z}}^*$ with the product topology, the action of $\hat{\mathbb{Z}}^*$ on $\mathrm{Hom}(Q, \hat{E})$ being induced by the natural $\hat{\mathbb{Z}}$-module structure on each E_n (cf. Exercise 2.13(a)). Prove that Γ is isomorphic to the group of those automorphisms of the abelian group $\{x \in L^* : \exists m > 0 : x^m \in \mathbb{Q}^*\}$ that are the identity on $\mathbb{Q}^*$. Prove further that there exists a continuous group homomorphism $\phi\colon \mathrm{Gal}(L/\mathbb{Q}) \to \Gamma$ such that the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/\mathbb{Q}) & \xrightarrow{\ \phi\ } & \Gamma \\ \downarrow & & \downarrow \\ \mathrm{Gal}(M/\mathbb{Q}) & \xrightarrow{\ \sim\ } & \hat{\mathbb{Z}}^* \end{array}$$

is commutative; here the vertical maps are the canonical ones and the bottom isomorphism is from Exercise 2.13(c).

(c) Let $H = \{(f, c) \in \Gamma : \forall a \in Q : (f(a) \bmod \hat{E}^2) = \left(\frac{a}{c}\right)\}$ where $\hat{E}/\hat{E}^2$ is identified with $E_2 = \{\pm 1\}$ and the Jacobi symbol $\left(\frac{a}{c}\right)$ is as in Exercise 2.15. Prove that H is a closed subgroup of Γ.

(d) Prove that ϕ yields an isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} H$ of topological groups. [*Hint:* use Exercises 2.16 and 2.20(d).]

(e) Prove that $\mathrm{Gal}(L/M)$ is the closure of the commutator subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, and that $\mathrm{Gal}(L/\mathbb{Q})$ is *not* a semidirect product of $\mathrm{Gal}(M/\mathbb{Q})$ and $\mathrm{Gal}(L/M)$.

2.22 Let K be a field that is complete with respect to a discrete nontrivial valuation, and K_s the separable closure of K. Let K_{unr} be the composite of all $L \subset K_s$ for which $K \subset L$ is finite and unramified, and K_{tr} the composite of all $L \subset K_s$ for which $K \subset L$ is finite and tamely ramified; here "unramified" and "tamely ramified" include separability of the residue class field extension.

(a) Prove that $K \subset K_{\mathrm{unr}}$ is Galois, and $\mathrm{Gal}(K_{\mathrm{unr}}/K) \cong \mathrm{Gal}(k_s/k)$, where k is the residue class field of K and k_s its separable closure.

(b) Prove that $K_{\mathrm{unr}} \subset K_{\mathrm{tr}}$ is Galois, and that $\mathrm{Gal}(K_{\mathrm{tr}}/K_{\mathrm{unr}})$ is isomorphic to $\hat{\mathbb{Z}}$ if $\mathrm{char}(k) = 0$ and to $\hat{\mathbb{Z}}/\mathbb{Z}_p$ if $\mathrm{char}(k) = p > 0$, with $\mathbb{Z}_p$ embedded in $\hat{\mathbb{Z}}$ as in Exercise 1.14.

(c) Prove that $K \subset K_{\mathrm{tr}}$ is Galois, that $\mathrm{Gal}(K_{\mathrm{tr}}/K)$ is a semidirect product of $\mathrm{Gal}(k_s/k)$ and $\hat{\mathbb{Z}}$ or $\hat{\mathbb{Z}}/\mathbb{Z}_p$ (as in (b)), and determine the action of $\mathrm{Gal}(k_s/k)$ on $\hat{\mathbb{Z}}$ or $\hat{\mathbb{Z}}/\mathbb{Z}_p$.

(d) Suppose that $\#k = q < \infty$. Prove that $\mathrm{Gal}(K_{\mathrm{tr}}/K)$ is isomorphic to the profinite completion of the group $\langle a, b : aba^{-1} = b^q \rangle$.

(e) Prove that $K_{\mathrm{tr}} = K_s = \overline{K}$ if $\mathrm{char}(k) = 0$, and that $\mathrm{Gal}(K_s/K_{\mathrm{tr}})$ is a pro-p-group if $\mathrm{char}(k) = p > 0$. (A *pro-p-group* is a projective limit of finite p-groups.)

(f) Prove that $\mathrm{Gal}(K_s/K)$ is a semidirect product of $\mathrm{Gal}(K_{\mathrm{tr}}/K)$ and $\mathrm{Gal}(K_s/K_{\mathrm{tr}})$. [*Hint:* [23, Chapitre II, Proposition 3 and Chapitre I, Proposition 16].]

2.23 (a) Let A be a local ring and $x \in A$ such that $x^2 = x$. Prove that $x = 0$ or $x = 1$.

(b) Prove that any ring isomorphism $\prod_{i=1}^{s} A_i \xrightarrow{\sim} \prod_{j=1}^{t} B_j$, where the A_i and B_j are local rings and $s, t < \infty$, is induced by a bijection $\sigma\colon \{1, 2, \ldots, s\} \xrightarrow{\sim} \{1, 2, \ldots, t\}$ and isomorphisms $A_i \xrightarrow{\sim} B_{\sigma(i)}$, $1 \le i \le s$.

2.24 Let B be a finite dimensional algebra over a field K, and write $B = \prod_{i=1}^{t} B_i$ as in 2.6, where B_i has maximal ideal $\mathfrak{m}_i$. Let $K_i = \{x \in B_i/\mathfrak{m}_i : x \text{ is separable over } K\}$. Prove that the number of K-algebra homomorphisms $B \to \overline{K}$ equals $\sum_{i=1}^{t} [K_i : K]$, and use this to give an alternative proof of 2.7, (iii) $\Rightarrow$ (iv).

2.25 Let B be a free separable algebra over a field K, and write $B = \prod_{i=1}^{t} B_i$ as in 2.7(iv). Let L be any field extension of K. Prove that $B \otimes_K L \cong L^{\dim_K(B)}$ as L-algebras if and only if L contains for each i a subfield containing K that is K-isomorphic to the normal closure of B_i over K.

2.26 Let π be a profinite group, $\pi' \subset \pi$ an open subgroup, and $\rho \subset \pi$ the normalizer of π' in π. Prove that the automorphism group of the π-set π/π' in the category π-**sets** is

isomorphic to ρ/π'. In particular, this automorphism group is isomorphic to π/π' if π' is normal in π.

2.27 Show that under the anti-equivalence of Theorem 2.9 injective maps correspond to surjective maps, surjective maps to injective maps, and fields to *transitive* π-sets (i.e., consisting of exactly one orbit).

2.28 Let $K \subset L$ be a finite Galois extension.

(a) Show that intermediate fields E of $K \subset L$ can be described categorically as equivalence classes of injective (or monomorphic) morphisms $E \xrightarrow{f} L$, two morphisms $E \xrightarrow{f} L$ and $E' \xrightarrow{f'} L$ being equivalent if $f = f'g$ for some isomorphism $E \xrightarrow{g} E'$.

(b) Show how the bijective correspondence between subgroups of $\mathrm{Aut}_K(L)$ and intermediate fields of $K \subset L$ can be deduced from Theorem 2.9.

2.29 Let K be a field, M a Galois extension of K, and B a finite dimensional K-algebra. If $B \otimes_K M \cong M \times M \times \cdots \times M$ as M-algebras we say that M *splits* B. Prove that the category of K-algebras that are split by M is anti-equivalent to $\mathrm{Gal}(M/K)$-**sets.**

3 Galois categories

This section contains an axiomatic characterization of categories that are equivalent to π-**sets** (see 1.10) for some profinite group π. Our axiom system is slightly simpler than that of Grothendieck [9, Exposé V, numéro 4] in that it does not mention "strict" epimorphisms. Our proof of the main result of this section, Theorem 3.5, was influenced by the treatment in [13, Section 8.4]. As an application we prove the topological theorem 1.15.

We now first list the axioms, and explain the terms used afterwards.

3.1 Definition. Let $\mathbf{C}$ be a category and F a covariant functor from $\mathbf{C}$ to the category **sets** of finite sets. We say that $\mathbf{C}$ is a *Galois category* with *fundamental functor* F if the following six conditions are satisfied.

(G1) There is a *terminal object* in $\mathbf{C}$, and the *fibred product* of any two objects over a third one exists in $\mathbf{C}$.

(G2) *Finite sums* exist in $\mathbf{C}$, in particular an *initial object*, and for any object in $\mathbf{C}$ the *quotient* by a finite group of automorphisms exists.

(G3) Any morphism u in $\mathbf{C}$ can be written as $u = u'u''$ where u'' is an *epimorphism* and u' a monomorphism, and any monomorphism $u\colon X \to Y$ in $\mathbf{C}$ is an isomorphism of X with a direct summand of Y.

(G4) The functor F transforms terminal objects in terminal objects and commutes with fibred products.

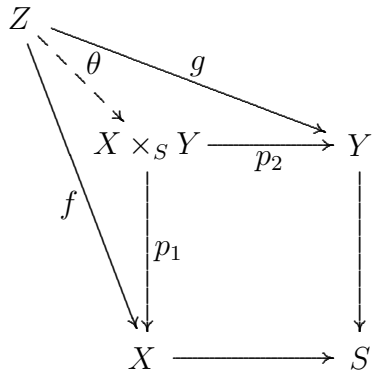
(G5) The functor F commutes with finite sums, transforms epimorphisms in epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.

(G6) If u is a morphism in $\mathbf{C}$ such that $F(u)$ is an isomorphism, then u is a isomorphism.

3.2 Explanation. (G1) A *terminal object* of a category $\mathbf{C}$ is an object Z such that for every object X there exists exactly one morphism $X \to Z$ in $\mathbf{C}$. Clearly, a terminal object is uniquely determined up to isomorphism, if it exists. We denote one by 1. In **sets** the terminal objects are the one-elements sets.

Suppose we are given objects X, Y, S and morphisms $X \to S$ and $Y \to S$ in a category $\mathbf{C}$. The *fibred product* of X and Y over S is an object, denoted by $X \times_S Y$, together with morphisms called *projections* $p_1\colon X \times_S Y \to X,\ p_2\colon X \times_S Y \to Y$, which make a commutative diagram with the given morphisms $X \to S,\ \ Y \to S$, such that given any object Z with morphisms $f\colon Z \to X,\ \ g\colon Z \to Y$ that make a commutative diagram with $X \to S$ and

$Y \to S$, there exists a unique morphism $\theta\colon Z \to X \times_S Y$ such that $f = p_1\theta$ and $g = p_2\theta$.



The fibred product is uniquely determined up to isomorphism, if it exists. We write $X \times Y$ instead of $X \times_1 Y$; this is the *product* of X and Y. In **sets** the fibred product $X \times_S Y$ is the set of all pairs (x, y) in the cartesian product of X and Y for which x and y have the same image in S; if the maps $X \to S,\ Y \to S$ are inclusions this may be identified with the *intersection* of X and Y.

The notions of a terminal object and a fibred product are special cases of the notion of a *left limit*, see Exercises 3.1 and 3.2. Condition G1 implies that **C** has arbitrary finite left limits, see Exercise 3.3.

(G2) Let $(X_i)_{i\in I}$ be a collection of objects of a category **C**. The *sum* of the X_i is an object, denoted by $\coprod_{i\in I} X_i$, together with morphisms $q_j\colon X_j \to \coprod_{i\in I} X_i$ for each $j \in I$, such that for any object Y of **C** and any collection of morphisms $f_j\colon X_j \to Y$, $j \in I$, there is a unique morphism $f\colon \coprod_{i\in I} X_i \to Y$ such that $f_j = fq_j$ for all $j \in I$. The sum is unique up to isomorphism if it exists. In the category of sets the sum of the X_i is their *disjoint union.*

We say that *finite sums* exist in **C** if any *finite* collection of objects has a sum in **C**. This is the case in **sets.** The *empty* collection of objects has a sum if and only if **C** has an *initial object*, i.e., an object, to be denoted by 0, with the property that for every object X there is exactly one morphism $0 \to X$ in **C**. In **sets** the empty set is an initial object.

If I is finite, $I = \{i_1, i_2, \ldots, i_n\}$, we may write $X_{i_1} \amalg X_{i_2} \amalg \cdots \amalg X_{i_n}$ instead of $\coprod_{i\in I} X_i$.

Let X be an object of **C** and G a finite subgroup of the group of automorphisms of X in **C**. The *quotient of X by G* is an object of **C**, denoted by X/G, together with a morphism $p\colon X \to X/G$ satisfying $p = p\sigma$ for all $\sigma \in G$, such that for any morphism $f\colon X \to Y$ in **C** satisfying $f = f\sigma$ for all $\sigma \in G$ there is a unique morphism $g\colon X/G \to Y$ for which $f = gp$. Such a quotient is unique up to isomorphism if it exists. In **sets** we can take X/G to be the set of *orbits* of X under G.

Axiom G2 requires that certain finite right limits exist in **C**; see Exercise 3.4. It follows

immediately from the main result of this section, Theorem 3.5, that in fact arbitrary finite right limits exist in a Galois category.

(G3) Let $f\colon X \to Y$ be a morphism in $\mathbf{C}$. We call f an *epimorphism* if for any object Z and any morphisms $g, h\colon Y \to Z$ with $gf = hf$ we have $g = h$, and a *monomorphism* if for any object Z and any morphisms $g, h\colon Z \to X$ with $fg = fh$ we have $g = h$. In **sets** a map f is an epimorphism if and only if it is surjective, and a monomorphism if and only if it is injective. Since any map is a surjection followed by an injection, a decomposition $u = u'u''$ as in G3 exists in **sets.**

The morphism $u\colon X \to Y$ is called an isomorphism of X with a direct summand of Y if there is a morphism $q_2\colon Z \to Y$ such that Y, together with $q_1 = u\colon X \to Y$ and $q_2\colon Z \to Y$ is the sum of X and Z. Taking Z to be the complement of the image of u we see that in **sets** any monomorphism has this property.

(G4) This condition is equivalent to the condition that F commute with arbitrary finite left limits (given G1); see Exercise 3.6(a). A functor F with this property is called *left exact.*

(G5) This condition is satisfied if F commutes with arbitrary finite right limits, i.e., if F is *right exact*; see Exercise 3.7. Theorem 3.5 implies that any fundamental functor F on a Galois category $\mathbf{C}$ is right exact, but this is not obvious from G5.

3.3 Examples of Galois categories. It is easy to see that the category **sets** is a Galois category, the fundamental functor F being the identity functor. In the same way one verifies that, for a profinite group π, the category π-**sets** of finite sets with a continuous π-action is a Galois category. In this case one takes F to be the forgetful functor π-**sets** $\to$ **sets.**

The main result of this section, Theorem 3.5, asserts that any essentially small Galois category $\mathbf{C}$ is equivalent to π-**sets** for a uniquely determined profinite group π. Here we call $\mathbf{C}$ *essentially small* if it is equivalent to a category whose objects form a set. (Clearly, π-**sets** is essentially small.)

Let K be a field, and let $\mathbf{C}$ be the opposite of the category ${}_K\mathbf{SAlg}$ of free separable K-algebras. From Theorem 2.9 it follows immediately that $\mathbf{C}$ is a Galois category, and from the proof of 2.9 we see that we can take F to be defined by $F(B) = \mathrm{Alg}_K(B, K_s)$, where K_s is a separable closure of K. A direct verification of the axioms G1–G6, depending on 2.7, is outlined in Exercise 3.9.

Further examples will be discussed in 3.6 and 3.7.

3.4 The automorphism group of a fundamental functor. Let $\mathbf{C}$ be a Galois category with fundamental functor F. An automorphism of F is an invertible morphism of functors $F \to F$. Equivalently, an automorphism σ of F is a collection of bijections $\sigma_X\colon F(X) \to$

$F(X)$, one for each object X of $\mathbf{C}$, such that for each morphism $f\colon Y \to Z$ in $\mathbf{C}$ the diagram

$$\begin{array}{ccc} F(Y) & \xrightarrow{F(f)} & F(Z) \\ {\scriptstyle\sigma_Y}\downarrow & & \downarrow{\scriptstyle\sigma_Z} \\ F(Y) & \xrightarrow{F(f)} & F(Z) \end{array}$$

is commutative. Denoting by $S_{F(X)}$ the finite group of permutations of $F(X)$ we can consider the automorphism group $\mathrm{Aut}(F)$ of F as a subgroup

$$\mathrm{Aut}(F) \subset \prod_X S_{F(X)},$$

the product ranging over the objects X of $\mathbf{C}$; it is supposed here that $\mathbf{C}$ is *small*, i.e., that its objects form a set. Let $\prod_X S_{F(X)}$ be endowed with the product topology, each $S_{F(X)}$ being discrete. Then for each morphism $f\colon Y \to Z$ the set $\{(\sigma_X) \in \prod_X S_{F(X)} : \sigma_Z F(f) = F(f)\sigma_Y\}$ is closed, so $\mathrm{Aut}(F)$ is a closed subgroup of $\prod_X S_{F(X)}$. From Exercises 1.10 and 1.11(c) it thus follows that $\mathrm{Aut}(F)$ may be considered as a *profinite group*, as we shall do in the sequel. Since we may replace $\mathbf{C}$ by an equivalent category, the foregoing is also valid if $\mathbf{C}$ is essentially small instead of small.

For any object X of $\mathbf{C}$, the profinite group $\mathrm{Aut}(F)$ acts continuously on the finite set $F(X)$. Let the resulting $\mathrm{Aut}(F)$-**set** be called $H(X)$. If $f\colon Y \to Z$ is any morphism in $\mathbf{C}$, then by the commutativity of the above diagram $F(f)$ is a morphism of $\mathrm{Aut}(F)$-**sets**. Hence putting $H(f) = F(f)$ we see that $H\colon \mathbf{C} \to \mathrm{Aut}(F)$-**sets** is a functor, and that F is the composite of H and the forgetful functor $\mathrm{Aut}(F)$-**sets** $\to$ **sets**.

If we take $\mathbf{C} = \pi$-**sets** for some profinite group π, and F the forgetful functor to **sets**, then one finds that $\mathrm{Aut}(F)$ may be identified with π, and that $H\colon \mathbf{C} \to \mathrm{Aut}(F)$-**sets** is the identity functor; see Exercise 3.11. In the general case we have the following theorem.

3.5 Theorem. *Let* $\mathbf{C}$ *be an essentially small Galois category with fundamental functor* F*. Then we have:*

(a) *the functor* $H\colon \mathbf{C} \to \mathrm{Aut}(F)$-**sets** *defined in* 3.4 *is an equivalence of categories;*

(b) *if* π *is a profinite group such that the categories* $\mathbf{C}$ *and* π-**sets** *are equivalent by an equivalence that, when composed with the forgetful functor* π-**sets** $\to$ π-**sets**, *yields the functor* F*, then* π *is canonically isomorphic to* $\mathrm{Aut}(F)$*;*

(c) *if* F' *is a second fundamental functor on* $\mathbf{C}$*, then* F *and* F' *are isomorphic;*

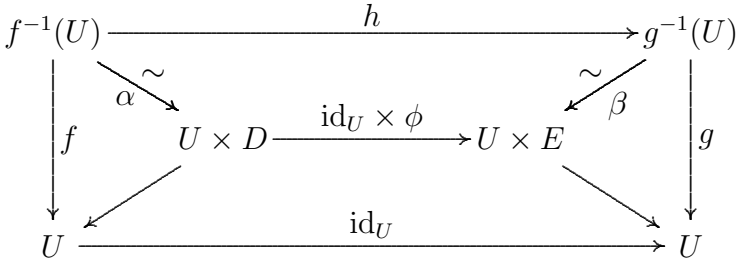
(d) *if* π *is a profinite group such that the categories* $\mathbf{C}$ *and* π-**sets** *are equivalent, then there is an isomorphism of profinite groups* $\pi \cong \mathrm{Aut}(F)$ *that is canonically determined up to an inner automorphism of* $\mathrm{Aut}(F)$.

For the proof of the theorem, see 3.11–3.19.

3.6 Example. Let X be a connected scheme and x a "geometric point" of X, i.e., a morphism $x\colon \operatorname{Spec}\Omega \to X$ for some algebraically closed field Ω. As we shall see in 5.23, there is a functor $\mathbf{FEt}_X \to \mathbf{FEt}_{\operatorname{Spec}\Omega}$ sending Y to $Y \times_X \operatorname{Spec}\Omega$. Composed with the equivalence $\mathbf{FEt}_{\operatorname{Spec}\Omega} \to \mathbf{sets}$ from 2.9, this yields a functor $F_x\colon \mathbf{FEt}_X \to \mathbf{sets}$. We shall prove that $\mathbf{FEt}_X$ is a Galois category with fundamental functor F_x by verifying the axioms G1–G6; see Theorem 5.24. From Theorem 3.5 we shall then deduce the Main theorem 1.11, with $\pi = \operatorname{Aut}(F_x)$. The latter profinite group is denoted by $\pi(X,x)$, the *fundamental group of X in x*. If x' is another geometric point of X, then 3.5(d) implies that $\pi(X,x) \cong \pi(X,x')$ by an isomorphism that is canonical up to an inner automorphism. This is analogous to the situation with the fundamental group that is defined in algebraic topology with homotopy classes of closed paths; see 1.13.

3.7 Finite coverings. Let X be a topological space, $x \in X$, and $\mathbf{C}$ the category of finite coverings of X. Let the functor $F_x\colon \mathbf{C} \to \mathbf{sets}$ send a covering $f\colon Y \to X$ to $f^{-1}(x)$. We shall prove that, if X is connected, $\mathbf{C}$ is a Galois category with fundamental functor F_x, and deduce Theorem 1.15 from 3.5. The basic tool in the verification of axioms G1–G6 is the following lemma.

3.8 Lemma. *Let X, Y, Z be topological spaces, $f\colon Y \to X$ and $g\colon Z \to X$ finite coverings, $h\colon Y \to Z$ a continuous map with $f = gh$, and $x \in X$. Then there exists an open neighborhood U of x in X such that f, g and h are "trivial above U", i.e., such that there exist finite discrete sets D and E, homeomorphisms $\alpha\colon f^{-1}(U) \to U \times D$ and $\beta\colon g^{-1}(U) \to U \times E$ and a map $\phi\colon D \to E$ such that the diagram*



is commutative; here the maps $U \times D \to U$ and $U \times E \to U$ are the projections on the first coordinate.

Proof of 3.8. By the definition of "finite covering" there exist open neighborhoods U' and U'' of x in X, finite discrete sets D and E and homeomorphisms $\alpha\colon f^{-1}(U') \to U' \times D$,

$\beta\colon g^{-1}(U'') \to U'' \times E$ such that the diagrams

$$\begin{array}{ccc} f^{-1}(U') & \xrightarrow{\alpha} & U' \times D \\ & {\scriptstyle f}\searrow \quad \swarrow & \\ & U' & \end{array} \qquad \begin{array}{ccc} g^{-1}(U'') & \xrightarrow{\beta} & U'' \times D \\ & {\scriptstyle g}\searrow \quad \swarrow & \\ & U'' & \end{array}$$

commute. Let now first $U = U' \cap U''$; then these assertions are also valid with U' and U'' replaced by U. Since h maps $f^{-1}(U)$ to $g^{-1}(U)$, there is a continuous map $\beta h \alpha^{-1}\colon U \times D \to U \times E$. It respects the projections to U, so it maps each $(u, d) \in U \times D$ to $(u, \phi_u(d)) \in U \times E$ for some map $\phi_u\colon D \to E$. Let $\phi = \phi_x$. The two obvious maps $U \times D \to D \xrightarrow{\phi} E$ and $U \times D \to U \times E \to E$ combine into a continuous map $U \times D \to E \times E,\ (u, d) \mapsto (\phi(d), \phi_u(d))$, mapping $\{x\} \times D$ to the diagonal in $E \times E$. Since the diagonal is open in $E \times E$ there is an open neighborhood of $\{x\} \times D$ in $U \times D$ that is also mapped to this diagonal, and since D is finite this open neighborhood may be taken of the form $V \times D$, with $V \subset X$ open. Then $\phi = \phi_v$ for all $v \in V$. Replacing U by V one now finds that Lemma 3.8 is proved.

3.9 Finite coverings: verification of the axioms. Let X be a topological space, and $\mathbf{C}$ the category of finite coverings of X. We first verify axioms G1, G2, G3 for $\mathbf{C}$.

(G1) The trivial covering $\mathrm{id}_X\colon X \to X$ is clearly a terminal object of $\mathbf{C}$. If $g\colon Y \to Z$, $h\colon W \to Z$ are morphisms in $\mathbf{C}$, then the fibred product is

$$Y \times_Z W = \{(y, w) \in Y \times W : g(y) = h(w) \text{ in } Z\}\ .$$

It must be shown that this space, with the obvious map to X, is a finite covering of X. Let $x \in X$. There is a neighborhood U of x in X above which the coverings $Y \to X$, $Z \to X$ and the map $g\colon Y \to Z$ are trivial in the sense of Lemma 3.8. Replacing U by a smaller neighborhood, if necessary, we may assume that also the covering $W \to X$ and the map $h\colon W \to Z$ are trivial above U. Then it is straightforward to verify that $p\colon Y \times_Z W \to X$ is trivial above U in the sense that the restriction of p to $p^{-1}(U)$ can be factored into a homeomorphism $p^{-1}(U) \xrightarrow{\sim} U \times E$, for some finite discrete set E, and the projection $U \times E \to U$.

(G2) One takes finite sums in $\mathbf{C}$ by forming disjoint unions in an obvious way. In particular, the unique covering $f\colon Y \to X$ with $Y = \emptyset$ is an initial object in $\mathbf{C}$. Next let $f\colon Y \to X$ be a finite covering and G a finite group of automorphisms of this covering. Then the space Y/G of orbits of Y under G, provided with the quotient topology and with the obvious maps to X, is a quotient of Y by G. It must of course be checked that this is a finite covering of

X. To do this one observes that each $x \in X$ has a neighborhood U in X above which not only the covering $Y \to X$ is trivial but each element of G as well, in the sense of Lemma 3.8.

(G3) For the verification of this axiom we refer to Exercise 3.14.

Next let $F_x \colon \mathbf{C} \to \mathbf{sets}$ be defined as in 3.7. We show that F_x satisfies G4 and G5 for any $x \in X$.

(G4) This is obvious from the explicit descriptions of terminal objects and fibred products in $\mathbf{C}$ and **sets**; see G1 above and 3.2.

(G5) This is likewise obvious (cf. Exercise 3.14(b)).

Finally, assume that X is *connected.* We prove that axiom G6 is satisfied as well.

(G6) Let $h \colon Y \to Z$ be a morphism in $\mathbf{C}$. Then $F_x(h)$ is the restriction of h to the fibres above x, and this map is bijective if and only if the map ϕ from Lemma 3.8 is bijective. Hence from this lemma we see that each of the sets $\{x \in X : F_x(h) \text{ is bijective}\}$ and $\{x \in X : F_x(h)$ is not bijective$\}$ is open in X. Since X is connected, one of the two sets is X and the other is empty. Therefore, if $F_x(h)$ is bijective for at least one $x \in X$ then h is bijective, hence an isomorphism because it is open (Exercises 3.13 and 3.12).

We conclude that, if X is connected, $\mathbf{C}$ is a Galois category with fundamental functor F_x, for any $x \in X$.

3.10 Finite coverings: proof of Theorem 1.15. Let the notation be as in 3.9, with X connected. Since every covering $Y \to X$ is equivalent to one in which the underlying set of Y is a subset of $X \times \mathbb{Z}$, the category $\mathbf{C}$ is essentially small. It is also a Galois category, by 3.9, so by Theorem 3.5(a) it is equivalent to π-**sets** for some profinite group π. Moreover, by 3.5(d) the profinite group π is uniquely determined, up to isomorphism. This proves Theorem 1.15.

As in 3.6 we can speak about $\hat{\pi}(X, x) = \mathrm{Aut}(F_x)$, the fundamental group of X in x, for $x \in X$; and for $x, x' \in X$ we have $\hat{\pi}(X, x) \cong \hat{\pi}(X, x')$ by an isomorphism that is canonical only up to an inner automorphism.

3.11 Proof of Theorem 3.5. Let $\mathbf{C}$ be a Galois category with fundamental functor F. We begin with the proof of Theorem 3.5. Without loss of generality we assume that $\mathbf{C}$ is small (3.4).

3.12 Subobjects and connected components. A *subobject* of an object X of $\mathbf{C}$ is a monomorphism $Y \to X$, two subobjects $Y \to X$, $Y' \to X$ being considered the same if there is an isomorphism $Y \xrightarrow{\sim} Y'$ making the diagram

$$\begin{array}{ccc} Y & \xrightarrow{\sim} & Y' \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

commutative. By Exercise 3.15(b) each subobject $Y \to X$ gives rise to a subset $F(Y) \subset F(X)$. The *intersection* of two subobjects $Y \to X,\ Y' \to X$ is $Y \times_X Y'$, with its natural morphism to X (see Exercise 3.16). By G4 we have $F(Y \times_X Y') = F(Y) \cap F(Y')$ inside $F(X)$; with G6 it thus follows that two objects $Y \to X,\ Y' \to X$ are the same if and only if $F(Y) = F(Y')$ as subsets of $F(X)$.

An object X is called *connected* if it has precisely two distinct subobjects, namely $0 \to X$, where 0 denotes an initial object (see 3.2, G2), and $\mathrm{id}_X \colon X \to X$. Notice that an initial object is not connected. See Exercise 3.17 for the meaning of connectedness in several Galois categories.

If X is not connected then there is a subobject $Y \to X$ with $\emptyset = F(0) \neq F(Y) \neq F(X)$. Using G3 one then finds Z such that X may be identified with $Y \amalg Z$ so that $F(X)$ is, by G5, equal to the disjoint union of $F(Y)$ and $F(Z)$. Arguing by induction on $\#F(X)$ one concludes that *every object of* $\mathbf{C}$ *is the sum of its connected subobjects.* The latter objects are called the *connected components* of the object. Likewise it follows that any subobject of X is the sum of a subset of the set of connected components of X.

3.13 "Prorepresentability" of F. Let A be a connected object of $\mathbf{C}$, and $a \in F(A)$. We claim that for each X *the map*

$$\mathrm{Mor}_{\mathbf{C}}(A, X) \to F(X), \qquad f \mapsto F(f)(a)$$

is injective; here $\mathrm{Mor}_{\mathbf{C}}(A, X)$ is the set of morphisms from A to X. To prove the claim, suppose $f, g \colon A \to X$ are such that $F(f)(a) = F(g)(a)$. Since F commutes with equalizers (Exercise 3.6(a)), the equalizer C of f and g is a subobject of A with $a \in F(C)$. By the connectedness of A this implies that $C = A$, so $f = g$, as required.

Denote by I the set of all pairs (A, a), where A is connected and $a \in F(A)$. Write $(A, a) \geq (B, b)$ if $b = F(f)(a)$ for some $f \in \mathrm{Mor}_{\mathbf{C}}(A, B)$; by the injectivity proved above, this f is unique if it exists. If both $(A, a) \geq (B, b)$ and $(B, b) \geq (A, a)$ in I, with corresponding morphisms $f \colon A \to B,\ g \colon B \to A$, then the uniqueness implies that $gf = \mathrm{id}_A$ and $fg = \mathrm{id}_B$, so that (A, a) and (B, b) are the same up to isomorphism. It follows that $\geq$ is a partial ordering on the set of isomorphism classes of elements of I.

We claim that the resulting partially ordered set is *directed* (1.7). To prove this, let $(A, a), (B, b) \in I$, and let C be the connected component of $A \times B$ for which $F(C)$, considered as a subset of $F(A \times B) \cong F(A) \times F(B)$ (axiom G4), contains the pair (a, b). Then $(C, (a, b))$ precedes both (A, a) and (B, b) in I, as required.

If $(A,a) \geq (B,b)$ in I then the diagram of induced maps

$$\begin{array}{ccc} \mathrm{Mor}_{\mathbf{C}}(B,X) & & \\ \downarrow & \searrow & \\ & & F(X) \\ \downarrow & \nearrow & \\ \mathrm{Mor}_{\mathbf{C}}(A,X) & & \end{array}$$

is commutative for any X, so there is a map

$$\varinjlim_I \mathrm{Mor}_{\mathbf{C}}(A,X) \to F(X);$$

see Exercise 3.18 for the definition of the injective limit $\varinjlim_I$. We claim that this map is *bijective*. Injectivity follows from the injectivity proved above. Further, if $x \in F(X)$ then $x \in F(A)$ for some connected component A of X, and the map $\mathrm{Mor}_{\mathbf{C}}(A,X) \to F(X)$ corresponding to the pair $(A,x) \in I$ sends the canonical monomorphism $A \to X$ to $x \in F(X)$. This implies surjectivity.

If $X \to Y$ is a morphism in $\mathbf{C}$ then the induced maps $\mathrm{Mor}_{\mathbf{C}}(A,X) \to \mathrm{Mor}_{\mathbf{C}}(A,Y)$, for $(A,a) \in I$, combine to a map between the injective limits, and the diagram

$$\begin{array}{ccc} \varinjlim_I \mathrm{Mor}_{\mathbf{C}}(A,X) & \longrightarrow & F(X) \\ \downarrow & & \downarrow \\ \varinjlim_I \mathrm{Mor}_{\mathbf{C}}(A,Y) & \longrightarrow & F(Y) \end{array}$$

is commutative. We conclude that *the functor F is naturally equivalent to the functor* $\varinjlim_I \mathrm{Mor}_{\mathbf{C}}(A,-)$. This is expressed by saying that F is "prorepresentable".

3.14 Galois objects. Let A be connected. Then $\#\mathrm{Aut}_{\mathbf{C}}(A) \leq \#\mathrm{Mor}_{\mathbf{C}}(A,A) \leq \#F(A)$, so $\mathrm{Aut}_{\mathbf{C}}(A)$ is finite. We call A a *Galois object* if the quotient $A/\mathrm{Aut}_{\mathbf{C}}(A)$ (axiom G2) is the terminal object 1. This is the case if and only if the map $F(A)/\mathrm{Aut}_{\mathbf{C}}(A) = F(A)/\mathrm{Aut}_{\mathbf{C}}(A) \to F(1) = 1$ is an isomorphism, so if and only if $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $F(A)$. Then clearly $\#\mathrm{Aut}_{\mathbf{C}}(A) \geq \#F(A)$, so for a connected Galois object A we have $\mathrm{Aut}_{\mathbf{C}}(A) = \mathrm{Mor}_{\mathbf{C}}(A,A)$ and $\#\mathrm{Aut}_{\mathbf{C}}(A) = \#F(A)$, and $\mathrm{Aut}_{\mathbf{C}}(A)$ acts freely and transitively on $F(A)$ (see (1.10)).

Let X be an arbitrary object of $\mathbf{C}$. We claim that there exists $(A,a) \in I$ with A *Galois* such that the injective map $\mathrm{Mor}_{\mathbf{C}}(A,X) \to F(X)$ from 3.13 is bijective.

To construct (A,a), put $Y = X^{F(X)}$, the product of a number of copies of X, one for each element of $F(X)$ (axiom G1). Let a be the element of $F(Y) = F(X)^{F(X)}$ (axiom G4) whose x-th coordinate is x, for $x \in F(X)$, and let A be the connected component of Y for which $a \in F(A)$. We claim that (A,a) has the desired properties.

Denote the composite of the canonical monomorphism $A \to Y$ with the projection on the x-th coordinate $Y = X^{F(X)} \to X$ by p_x, for $x \in F(X)$. Then the map $\mathrm{Mor}_{\mathbf{C}}(A, X) \to F(X)$ sends p_x to x, for $x \in F(X)$, so it is surjective. We knew already that it is injective, so it is bijective, and it follows at the same time that each morphism $A \to X$ is of the form p_x.

Next let a' be another element of $F(A)$. From $\mathrm{Mor}_{\mathbf{C}}(A, X) = \#F(X)$ it follows that the injective map $\mathrm{Mor}_{\mathbf{C}}(A, X) \to F(X)$ induced by (A, a') is also bijective. This means that the coordinates of a', when viewed as an element of $F(Y) = F(X)^{F(X)}$, are precisely all elements of $F(X)$, each occurring once. Hence there is an automorphism σ of $Y = X^{F(X)}$, permuting the factors, such that $F(\sigma)$ maps a to a'. This automorphism transforms the connected component A of Y into a connected component A' of Y, and from $a' \in F(A) \cap F(A')$ (inside $F(Y)$) we see that we must have $A = A'$. We conclude that A has an automorphism sending a to a', so that A is indeed a Galois object.

3.15 Construction of π. Put $J = \{(A, a) \in I : A \text{ is Galois}\}$. We prove that J is a *cofinal* subset of I (Exercise 1.17). Let $(B, b) \in I$. By 3.14 there is a connected Galois object A such that there is a morphism $f\colon A \to B$. By G3 and the connectedness of B the map $F(f)\colon F(A) \to F(B)$ is surjective, so $F(f)(a) = b$ for some $a \in F(A)$. Now $(A, a) \in J$, and $(A, a) \geq (B, b)$, as required. Let $f'\colon A \to B$ be another morphism. By the surjectivity of $F(f)$ there exists $a' \in F(A)$ with $F(f)(a') = F(f')(a)$, and since A is Galois there is $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ with $a' = F(\sigma)(a)$. Then $F(f\sigma)(a) = F(f')(a)$, so $f\sigma = f'$ by the injectivity of $\mathrm{Mor}_{\mathbf{C}}(A, B) \to F(B)$. We conclude that the natural action of $\mathrm{Aut}_{\mathbf{C}}(A)$ on $\mathrm{Mor}_{\mathbf{C}}(A, B)$ is *transitive.*

Since J is cofinal in I the result of 3.13 implies that F is naturally equivalent to the functor $\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A, -)$.

Let $(A, a), (B, b) \in J$ be such that $(A, a) \geq (B, b)$, with corresponding morphism $f\colon A \to B$. For each $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ there is a unique $\tau \in \mathrm{Aut}_{\mathbf{C}}(B)$ for which

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\ A & \xrightarrow{f} & B \end{array}$$

commutes, namely, the automorphism τ with $F(\tau)(b) = F(f\sigma)(a)$. The map $\mathrm{Aut}_{\mathbf{C}}(A) \to \mathrm{Aut}_{\mathbf{C}}(B)$ sending σ to τ in this situation is clearly a group homomorphism. It is surjective, since by the transitivity proved above each τf is of the form $f\sigma$. Thus we obtain a projective system of finite groups with surjective transition maps. We write π for the projective limit $\varprojlim_J \mathrm{Aut}_{\mathbf{C}}(A)$, which is a profinite group.

3.16 A functor to π-sets. Let X be an object of $\mathbf{C}$. For each connected Galois object A, the group $\mathrm{Aut}_{\mathbf{C}}(A)$ acts on $\mathrm{Mor}_{\mathbf{C}}(A, x)$ by $(\sigma, f) \mapsto f\sigma^{-1}$. This action is, for $(A, a) \geq (B, b)$ in J, compatible with the maps $\mathrm{Aut}_{\mathbf{C}}(A) \to \mathrm{Aut}_{\mathbf{C}}(B)$, $\mathrm{Mor}_{\mathbf{C}}(B, X) \to \mathrm{Mor}_{\mathbf{C}}(A, X)$, so it gives rise to a continuous π-action on the finite set $\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A, X) \cong F(X)$.

If $X \to Y$ is a morphism in $\mathbf{C}$ then it is easy to check that the induced map $\varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A, X) \to \varinjlim_J \mathrm{Mor}_{\mathbf{C}}(A, Y)$ is a morphism of π-sets. Hence if we write $H(X)$ for the set $F(X)$ equipped with the π-action just defined, and $H(f) = F(f)$ for a morphism f in $\mathbf{C}$, then H is a functor $\mathbf{C} \to \pi$-**sets** that composed with the forgetful functor π-**sets** $\to$ **sets** yields F. (We shall see in 3.19 that this H is the same one as in 3.4.)

3.17 The effect on connected objects. Let B be a connected object, and let $(A, a) \in J$ be such that $\mathrm{Mor}_{\mathbf{C}}(A, B) \xrightarrow{\sim} F(B)$. In 3.15 we proved that $\mathrm{Aut}_{\mathbf{C}}(A)$ acts transitively on $\mathrm{Mor}_{\mathbf{C}}(A, B)$, so we have an isomorphism of π-sets

$$H(B) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G$$

with H as in 3.16, where $G \subset \mathrm{Aut}_{\mathbf{C}}(A)$ is the subgroup

$$G = \{\sigma \in \mathrm{Aut}_{\mathbf{C}}(A) : f\sigma = f\}$$

for some fixed $f\colon A \to B$.

Since the natural map $\pi \to \mathrm{Aut}_{\mathbf{C}}(A)$ is surjective, the action of π on $H(B)$ is *transitive.* Hence H maps connected objects of the category $\mathbf{C}$ to connected objects of the category π-**sets** (Exercise 3.17(a)).

Since $f\sigma = f$ for all $\sigma \in G$, the morphism $f\colon A \to B$ induces a morphism $g\colon A/G \to B$. We claim that this is an *isomorphism.* To prove this, it suffices to check that $F(g)$ is an isomorphism. In any case $F(g)$ is surjective, since $F(f)$ is. Further $F(A/G) = F(A)/G$ has cardinality $\#(\mathrm{Aut}_{\mathbf{C}}(A)/G)$, because the action of $\mathrm{Aut}_{\mathbf{C}}(A)$ on $F(A)$ is free and transitive. Since also $F(B)$ has cardinality $\#(\mathrm{Aut}_{\mathbf{C}}(A)/G)$ this completes the proof.

3.18 An equivalence of categories. To prove that the functor $H\colon \mathbf{C} \to \pi$-**sets** from 3.16 is an equivalence it suffices to check that (i) each finite π-set is isomorphic to one of the form $H(X)$, for an object X of $\mathbf{C}$; and (ii) for every two objects X, Y of $\mathbf{C}$ the functor H yields a bijective map $\mathrm{Mor}_{\mathbf{C}}(X, Y) \to \mathrm{Mor}_{\pi}(H(X), H(Y))$ (see Exercise 3.20).

We first prove (i). Every finite π-set is isomorphic to a finite sum of *transitive* π-sets, and the functor H preserves finite sums since F does. Hence it suffices to consider a transitive π-set, and any such is of the form $\mathrm{Aut}_{\mathbf{C}}(A)/G$ for some connected Galois object A and some subgroup $G \subset \mathrm{Aut}_{\mathbf{C}}(A)$ (cf. Exercise 1.19). Let $a \in F(A)$. Then the map

$\mathrm{Aut}_{\mathbf{C}}(A) = \mathrm{Mor}_{\mathbf{C}}(A,A) \to F(A)$ sending f to $F(f)(a)$ is bijective, and $F(A)$ with the π-action $(\sigma, F(f)(a)) \mapsto F(f\sigma^{-1})(a)$ is $H(A)$. Thus $H(A)$ is isomorphic to the π-set $\mathrm{Aut}_{\mathbf{C}}(A)$ on which π acts by left multiplication, by $F(f)(a) \mapsto f^{-1}$. Since F is a functor, $\mathrm{Aut}_{\mathbf{C}}(A)$ and its subgroup G act in a second way on $H(A) = F(A)$, namely by $(\sigma, x) \to F(\sigma)(x)$; under the identification of π-sets $H(A) \cong \mathrm{Aut}_{\mathbf{C}}(A)$ just given this is right multiplication by σ^{-1}. We thus see that the quotient $H(A)/G$ in the category π-**sets** is the π-set $\mathrm{Aut}_{\mathbf{C}}(A)/G$. Since the natural map $F(A)/G \to F(A/G)$ is an isomorphism, by G5, the same is true for H, so we have $H(A/G) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G$ in π-**sets**. This proves (i).

To prove (ii), let X, Y be objects of $\mathbf{C}$. The map $\mathrm{Mor}_{\mathbf{C}}(X,Y) \to \mathrm{Mor}_{\pi}(H(X), H(Y))$ to be proved bijective is in any case injective, by Exercise 3.6(b). If $X = \coprod_{i=1}^{s} X_i$ then $\mathrm{Mor}_{\mathbf{C}}(X,Y) \cong \coprod_{i=1}^{s} \mathrm{Mor}_{\mathbf{C}}(X_i, Y)$, by the definition of $\coprod$, and since H preserves finite sums we have an analogous decomposition for $\mathrm{Mor}_{\pi}(H(X), H(Y))$. In this way the question is reduced to the case that X is *connected.* If $X \to Y$ is any morphism, factored as $X \to Z \to Y$ with $X \to Z$ epimorphic and $Z \to Y$ monomorphic, then the connectedness of X implies that Z is connected (Exercise 3.21), so Z is one of the connected components of Y. If we write $Y = \coprod_{j=1}^{t} Y_j$, the Y_j being the connected components of Y, then it easily follows that $\mathrm{Mor}_{\mathbf{C}}(X,Y) \cong \coprod_{j=1}^{t} \mathrm{Mor}_{\mathbf{C}}(X, Y_j)$ for connected X, and since also $H(X)$ is connected (3.17) there is a similar decomposition for $\mathrm{Mor}_{\pi}(H(X), H(Y))$. The question has now been reduced to the case that both X and Y are connected.

Let X and Y be connected. Choosing $(A, a) \in J$ sufficiently large we can write $X = A/G_1$ and $Y = A/G_2$ for certain subgroups $G_1, G_2 \subset \mathrm{Aut}_{\mathbf{C}}(A)$ with $H(X) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G_1$, $H(Y) \cong \mathrm{Aut}_{\mathbf{C}}(A)/G_2$ (see 3.17). Any π-homomorphism $\mathrm{Aut}_{\mathbf{C}}(A)/G_1 \to \mathrm{Aut}_{\mathbf{C}}(A)/G_2$ is of the form $\tau G_1 \mapsto \tau\sigma G_2$ for some uniquely determined $\sigma G_2 \in \mathrm{Aut}_{\mathbf{C}}(A)/G_2$, and for given σG_2 this is a well-defined π-homomorphism if and only if $G_1\sigma \subset \sigma G_2$. Hence $\#\mathrm{Mor}_{\pi}(H(X), H(Y))$ $= \#\{\sigma G_2 \in \mathrm{Aut}_{\mathbf{C}}(A)/G_2 : G_1\sigma \subset \sigma G_2\}$. To count $\mathrm{Mor}_{\mathbf{C}}(X,Y)$ we use that for any $f \in \mathrm{Mor}_{\mathbf{C}}(X,Y)$ there exists $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ for which the diagram

$$\begin{array}{ccc} A & \xrightarrow{h_1} & A/G_1 = X \\ \Big\downarrow{\scriptstyle \sigma} & & \Big\downarrow{\scriptstyle f} \\ A & \xrightarrow{h_2} & A/G_2 = Y \end{array}$$

with natural horizontal maps h_i commutes; namely, choose $a' \in F(A)$ with $F(h_2)(a') = F(fh_1)(a)$, and σ with $F(\sigma)(a) = a'$. We have $h_2\sigma = h_2\sigma' \Leftrightarrow \sigma'\sigma^{-1} \in G_2 \Leftrightarrow G_2\sigma = G_2\sigma'$, so f uniquely determines the coset $G_2\sigma$. Conversely, a given element $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ gives rise to a morphism $f\colon X \to Y$ if and only if $h_2\sigma$ factors via A/G_1, so if and only if $h_2\sigma\tau = h_2\sigma$ for

all $\tau \in G_1$, so if and only if $\sigma G_1 \subset G_2\sigma$. Therefore $\#\mathrm{Mor}_{\mathbf{C}}(X,Y) = \#\{G_2\sigma : \sigma G_1 \subset G_2\sigma\}$, and replacing σ by σ^{-1} we see that this is the same as $\#\mathrm{Mor}_{\pi}(H(X), H(Y))$. This proves (ii).

We have proved that the functor H defined in 3.16 is an equivalence of categories.

3.19 End of proof of Theorem 3.5. We first prove (b). Let π be any profinite group and $H\colon \mathbf{C} \to \pi$-**sets** any equivalence that composed with the forgetful functor $F_1\colon \pi$-**sets** $\to$ **sets** yields F. Then $\mathrm{Aut}(F) \cong \mathrm{Aut}(F_1)$, since H is an equivalence, and $\mathrm{Aut}(F_1) \cong \pi$ by Exercise 3.11. Hence $\pi \cong \mathrm{Aut}(F)$. This proves (b).

To prove (a), we apply (b) to the group π constructed in 3.15 and the functor H defined in 3.16. Then H is an equivalence by 3.18, and composed with the forgetful functor to **sets** it yields F. Hence by (b) we may identify π with $\mathrm{Aut}(F)$, and then H becomes identified with the functor from 3.4 (cf. Exercise 3.11(c)). This implies (a).

To prove (c), let $F'\colon \mathbf{C} \to$ **sets** be a second fundamental functor. We have

$$\varinjlim_{J} \mathrm{Mor}_{\mathbf{C}}(A, -) \cong F, \qquad \varinjlim_{J'} \mathrm{Mor}_{\mathbf{C}}(A, -) \cong F',$$

with J as defined in 3.15 and J' defined similarly for F'. Since all pairs $(A, a) \in J$ with the same A are isomorphic, we may replace J by a subset J_0 containing exactly one pair (A, a) for each connected Galois object A. Similarly, choose $J_0' \subset J'$ such that J_0' contains exactly one pair (A, a') for each connected Galois object A; it should be noted that the definitions of "connected" and "Galois" (3.12 and 3.14) do not refer to a fundamental functor. If $(A, a), (B, b) \in J_0$ and $g\colon A \to B$ is a morphism, then there is a unique $\beta \in \mathrm{Aut}_{\mathbf{C}}(B)$ for which $F(\beta)$ sends $F(g)(a)$ to b. Then $f = \beta g$ satisfies $F(f)(a) = b$, so $(A, a) \geq (B, b)$ in J_0. It follows easily that $(A, a) \geq (B, b)$ in J_0 if and only if the corresponding elements $(A, a'), (B, b')$ of J_0' satisfy $(A, a') \geq (B, b')$; but the morphisms $f, f'\colon A \to B$ with $F(f)(a) = b$ and $F'(f')(a') = b'$ are not necessarily the same. For each $\alpha \in \mathrm{Aut}_{\mathbf{C}}(A)$ there exists $\gamma \in \mathrm{Aut}_{\mathbf{C}}(B)$ for which the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \gamma} \\ A & \xrightarrow{f'} & B \end{array}$$

commutes, with f, f' as above. Mapping α to γ we obtain a projective system of finite non-empty sets $\mathrm{Aut}_{\mathbf{C}}(A)$, with A ranging over the connected Galois objects. By Exercise 1.9(b) the projective limit is non-empty, so we can make a simultaneous choice of $\alpha_A \in \mathrm{Aut}_{\mathbf{C}}(A)$

such that all diagrams

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \alpha_A} & & \downarrow{\scriptstyle \alpha_B} \\ A & \xrightarrow{f'} & B \end{array}$$

as above commute. These automorphisms induce an isomorphism

$$\varinjlim_{J_0} \mathrm{Mor}_{\mathbf{C}}(A, -) \cong \varinjlim_{J_0'} \mathrm{Mor}_{\mathbf{C}}(A, -),$$

so $F \cong F'$. This proves (c).

Finally, we prove (d). Let $H' \colon \mathbf{C} \to \pi\text{-}\mathbf{sets}$ be an equivalence, and F' the composite with the fundamental functor to **sets**. Then $\pi \cong \mathrm{Aut}(F')$ by (b), and since $F' \cong F$ by (c) there is an isomorphism of profinite groups $\mathrm{Aut}(F') \cong \mathrm{Aut}(F)$ that is canonically determined up to an inner automorphism.

This completes the proof of Theorem 3.5.

3.20 Theorem. *Let* $\mathbf{C}$ *and* $\mathbf{C}'$ *be essentially small Galois categories,* $F' \colon \mathbf{C}' \to \mathbf{sets}$ *a fundamental functor and* $G \colon \mathbf{C} \to \mathbf{C}'$ *a functor such that* $F = F'G$ *is a fundamental functor for* $\mathbf{C}$*. Let* $H \colon \mathbf{C} \to \pi\text{-}\mathbf{sets}$ *and* $H' \colon \mathbf{C}' \to \pi'\text{-}\mathbf{sets}$ *be the equivalence from Theorem* 3.5(a)*, with* $\pi = \mathrm{Aut}(F)$*,* $\pi' = \mathrm{Aut}(F')$*. Then there is a natural continuous group homomorphism* $\pi' \to \pi$ *such that the functor* $G' \colon \pi\text{-}\mathbf{sets} \to \pi'\text{-}\mathbf{sets}$ *that endows a* π*-set with the* π'*-action induced by* $\pi' \to \pi$ *gives rise to a commutative diagram*

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{G} & \mathbf{C}' \\ \downarrow{\scriptstyle H} & & \downarrow{\scriptstyle H'} \\ \pi\text{-}\mathbf{sets} & \xrightarrow{G'} & \pi'\text{-}\mathbf{sets}. \end{array}$$

Proof. Each automorphism (σ'_Y) of F', with Y ranging over the objects of $\mathbf{C}'$, gives rise to an automorphism (σ_X) of F, with $\sigma_X = \sigma'_{G(X)}$ for each object X of $\mathbf{C}$. The resulting map $\mathrm{Aut}(F') \to \mathrm{Aut}(F)$ is easily seen to be a continuous group homomorphism (cf. Exercise 3.10) and to have the property stated in the theorem. This proves 3.20.

3.21 Examples. Let X and X' be connected topological spaces, $f \colon X' \to X$ a continuous map, $x' \in X'$ and $x = f(x') \in X$. Denote the categories of finite coverings of X and X' by $\mathbf{C}$ and $\mathbf{C}'$, respectively. Then there is a functor $G \colon \mathbf{C} \to \mathbf{C}'$ with $G(Y) = Y \times_X X' = \{(y, z) \in Y \times X' : y \text{ and } z \text{ have the same image in } X\}$. Using the notation of 3.7 we have $F_{x'}G = F_x$, so

the conditions of 3.20 are satisfied. Hence we find a natural continuous group homomorphism $\hat{\pi}(X', x') \to \hat{\pi}(X, x)$. It follows that $\hat{\pi}$ is a functor from the category of connected topological spaces with base point to the category of profinite groups (cf. Exercise 3.22).

Let K' be a field and K a subfield. Then there is a functor ${}_K\mathbf{SAlg} \to {}_{K'}\mathbf{SAlg}$ sending A to $A \otimes_K K'$. Passing to the opposite categories and defining the fundamental functor F' by $F'(B) = \mathrm{Alg}_{K'}(B, K'_s)$ (cf. 3.3) one finds that the conditions of 3.20 are satisfied. This gives rise to a continuous group homomorphism $\pi' \to \pi$, where π', π are the absolute Galois groups of K', K, respectively. It is easily seen that this is simply the map restricting the action of π' on K'_s to K_s, which may be considered as a subfield of K'_s.

Exercises for Section 3

3.1 (**Left limits and right limits** [12]**.**) A *directed graph* D consists of a set $V = V_D$ of *vertices*, a set $E = E_D$ of *edges*, a *source* map $s = s_D \colon E \to V$ and a *target* map $t = t_D \colon E \to V$; each $e \in E$ is to be thought of as an arrow from $s(e)$ to $t(e)$. Let D be a directed graph and $\mathbf{C}$ a category. A *D-diagram* in $\mathbf{C}$ is a map that assigns to each $v \in V$ an object X_v of $\mathbf{C}$ and to each $e \in E$ a morphism f_e from $X_{s(e)}$ to $X_{t(e)}$ in $\mathbf{C}$. A *morphism* from a D-diagram $((X_v)_{v\in V}, (f_e)_{e\in E})$ to a D-diagram $((Y_v)_{v\in V}, (g_e)_{e\in E})$ is a collection of morphisms $(h_v \colon X_v \to Y_v)_{v\in V}$ in $\mathbf{C}$ such that $h_{t(e)} f_e = g_e h_{s(e)}$ for all $e \in E$.

(a) Show that the D-diagrams in $\mathbf{C}$ form a category. We denote this category by $\mathbf{C}^D$.

(b) Show that there exists a functor $\Gamma \colon \mathbf{C} \to \mathbf{C}^D$ mapping an object X to the *constant D-diagram* with $X_v = X$ for all $v \in V$ and $f_e = \mathrm{id}_X$ for all $e \in E$, and mapping a morphism $h \colon X \to Y$ to the morphism $(h_v)_{v\in V}$ with all $h_v = h$.

(c) A *left limit* of a D-diagram A in $\mathbf{C}$ is an object $\varprojlim A$ of $\mathbf{C}$ such that

$$\mathrm{Hom}_{\mathbf{C}}(-, \varprojlim A) \cong \mathrm{Hom}_{\mathbf{C}^D}(\Gamma(-), A)$$

as functors on $\mathbf{C}$. Prove that $\varprojlim A$ is unique up to isomorphism if it exists, and that the notion of a left limit generalizes that of a projective limit (see 1.7 and Exercise 1.8).

(d) Show that $\mathbf{C}$ admits left limits of all D-diagrams in $\mathbf{C}$ if and only if the functor $\Gamma \colon \mathbf{C} \to \mathbf{C}^D$ has a *right adjoint* $\varprojlim \colon \mathbf{C}^D \to \mathbf{C}$, i.e.,

$$\mathrm{Hom}_{\mathbf{C}}(-, \varprojlim -) \cong \mathrm{Hom}_{\mathbf{C}^D}(\Gamma(-), -) \ .$$

If this right adjoint exists, we say that $\mathbf{C}$ *admits left limits over* D.

(e) A *right limit* of a D-diagram A in $\mathbf{C}$ is an object $\varinjlim A$ of $\mathbf{C}$ such that

$$\mathrm{Hom}_{\mathbf{C}}(\varinjlim A, -) \cong \mathrm{Hom}_{\mathbf{C}^D}(A, \Gamma(-)).$$

Formulate and prove the analogues of the assertions in (c) and (d). If Γ has a left adjoint $\varinjlim\colon \mathbf{C}^D \to \mathbf{C}$ we say that $\mathbf{C}$ *admits right limits over* D.

3.2 (**Left limits in axiom** G1**.**) Let $\mathbf{C}$ be a category.

(a) Prove that $\mathbf{C}$ admits left limits over the empty directed graph (with $V = E = \emptyset$) if and only if $\mathbf{C}$ has a terminal object.

(b) Prove that $\mathbf{C}$ admits left limits over the directed graph  if and only if the fibred product of any two objects over a third one exists in $\mathbf{C}$.

3.3 (**Equalizers and finite left limits.**) Let $\mathbf{C}$ be a category. An *equalizer* of two morphisms $f, g\colon X \to Y$ in $\mathbf{C}$ is a left limit of the D-diagram $f, g\colon X \rightrightarrows Y$, with $D =$  . We say that $\mathbf{C}$ has *equalizers* if it admits left limits over $D =$  . We say that $\mathbf{C}$ has *finite products* if it admits left limits over any D with V finite and $E = \emptyset$. We say that $\mathbf{C}$ has *finite left limits* if it admits left limits over any finite D (i.e., with both V and E finite).

(a) Suppose that $\mathbf{C}$ satisfies G1 (see 3.1), and let $f, g\colon X \to Y$ be morphisms in $\mathbf{C}$. Let $X \times_Y X$ be formed with respect to f and g. Prove that there exists a natural morphism $X \times_Y X \to X \times X$ and a diagonal morphism $X \to X \times X$ such that $X \times_{X\times X} (X \times_Y X)$ is an equalizer of f and g.

(b) Prove that $\mathbf{C}$ satisfies G1 if and only if it has equalizers and finite products, and if and only if it has finite left limits.

3.4 (**Right limits in axiom** G2**.**) Left $\mathbf{C}$ be a category.

(a) Prove that $\mathbf{C}$ admits right limits over the empty directed graph if and only if $\mathbf{C}$ has an initial object.

(b) Prove that the following three assertions are equivalent:

(i) finite sums exist in $\mathbf{C}$;

(ii) any two objects X, Y of $\mathbf{C}$ have a sum $X \amalg Y$ in $\mathbf{C}$, and $\mathbf{C}$ has an initial object;

(iii) $\mathbf{C}$ admits right limits over any directed graph D with V finite and E empty.

(c) Show how the quotient X/G of an object X by a finite subgroup $G \subset \mathrm{Aut}(X)$ can be interpreted as a right limit.

3.5 Let $f\colon X \to Y$ be a morphism in a category $\mathbf{C}$. Prove that f is an epimorphism if and only if Y, together with $\mathrm{id}_Y\colon Y \to Y$ and $f\colon X \to Y$, is a right limit of the diagram $Y \leftarrow X \to Y$ in which both arrows equal f.

3.6 Left $\mathbf{C}$ be a category satisfying G1, and F a covariant functor from $\mathbf{C}$ to the category of sets.

(a) Prove that F satisfies G4 if and only if it commutes with equalizers and with finite products, and if and only if it commutes with arbitrary finite left limits.

(b) Suppose that F satisfies G4 and G6, and let $f, g\colon X \to Y$ be morphisms in $\mathbf{C}$ with $F(f) = F(g)$. Prove that $f = g$.

3.7 Let $\mathbf{C}$ be a category and F a covariant functor from $\mathbf{C}$ to the category of sets. Suppose that F commutes with finite right limits. Prove that F satisfies G4. [*Hint:* Exercises 3.4 and 3.5.]

3.8 Let $\mathbf{C}$ be the category of modules over a ring A, and F a covariant functor from $\mathbf{C}$ to the category of abelian groups. Suppose that F is *additive*, i.e., that for any two A-modules X, Y the map $F\colon \mathrm{Hom}_A(X,Y) \to \mathrm{Hom}(F(X), F(Y))$ is a group homomorphism.

(a) Prove that F commutes with finite products.

(b) Prove that a sequence $0 \to X \to Y \xrightarrow{f} Z$ in $\mathbf{C}$ is exact if and only if X, with the map $X \to Y$ and the zero map $X \to Z$, is an equalizer of f and the zero map $Y \to Z$.

(c) Prove that F, when composed with the forgetful functor to the category of sets, is left exact if and only if for every exact sequence $0 \to X \to Y \to Z$ in $\mathbf{C}$ the sequence $0 \to F(X) \to F(Y) \to F(Z)$ is exact.

3.9 Let K be a field, with algebraic closure $\overline{K}$. In this exercise, A, B and C denote free separable K-algebras.

(a) Prove that if $A \to B$, $A \to C$ are K-algebra homomorphisms, $B \otimes_A C$ is a free separable K-algebra. [*Hint:* 2.7.]

(b) Let G be a finite group of K-algebra automorphisms of A, and extend G by $\overline{K}$-linearity to $A \otimes_K \overline{K}$. Prove that one has $(A \otimes_K \overline{K})^G \cong A^G \otimes_K \overline{K}$ as $\overline{K}$-algebras, and that A^G is a free separable K-algebra. [*Hint:* use a basis of $\overline{K}$ over K.]

(c) Let $f\colon A \to B$ be a K-algebra homomorphism. Prove that $f[A]$ is a free separable K-algebra, and that $f[A] = \{b \in B : b \otimes 1 = 1 \otimes b \text{ in } B \otimes_A B\}$.

(d) Deduce that the opposite of the category of free separable K-algebras is a Galois category, with $F(A) = \mathrm{Alg}_K(A, \overline{K}) \cong \mathrm{Alg}_K(A, K_s)$; here K_s is a separable closure of K.

3.10 Let $\mathbf{C}$ be an essentially small Galois category with fundamental functor F. Prove that a base for the open neighborhoods of id_F in $\mathrm{Aut}(F)$ is given by the sets $\{\sigma \in \mathrm{Aut}(F) : \sigma_X$ is the identity on $F(X)\}$, with X ranging over the objects of $\mathbf{C}$.

3.11 Let π be a profinite group, and F the forgetful functor from π-**sets** to the category **sets** of finite sets.

(a) Prove that an automorphism σ of F is completely determined by the maps $\sigma_{\pi/\pi'} \colon F(\pi/\pi') \to F(\pi/\pi')$, with π' ranging over the open normal subgroups of π. (The action of π on π/π' is induced by left multiplication.)

(b) Let π' be an open normal subgroup of π. Prove that the group of π-**sets**-automorphisms of the π-set π/π' is isomorphic to the group π/π', with $\tau \in \pi/\pi'$ acting as right multiplication by τ^{-1}. Prove also that any set-theoretic map $\pi/\pi' \to \pi/\pi'$ commuting with all π-**sets**-automorphisms of π/π' is given by left multiplication by some element of π/π'.

(c) Conclude that $\mathrm{Aut}(F)$ may be identified with π, and that the functor $H \colon \pi$-**sets** $\to \mathrm{Aut}(F)$-**sets** defined in 3.4 is the identity functor.

3.12 Let X be a topological space, and $f \colon Y \to X$ a finite covering. Prove that f is open and closed.

3.13 Let X, Y, Z be topological spaces, $f \colon Y \to X$ and $g \colon Z \to X$ finite coverings, and $h \colon Y \to Z$ a continuous map with $f = gh$. Prove that h is a finite covering.

3.14 Let X be a topological space, $\mathbf{C}$ the category of finite coverings of X, and $h \colon Y \to Z$ a morphism in $\mathbf{C}$.

(a) Prove that the image of h is open and closed in Z.

(b) Prove that h is injective if and only if it is a monomorphism, and that h is surjective if and only if it is an epimorphism.

(c) Prove that $\mathbf{C}$ satisfies axiom G3.

3.15 Let $\mathbf{C}$ be a category and $F \colon \mathbf{C} \to$ **sets** be a functor such that axioms G1, G4, G6 are satisfied. Let further $f \colon Y \to X$ be a morphism in $\mathbf{C}$.

(a) Prove that f is a monomorphism if and only if the first projection $p_1 \colon Y \times_X Y \to Y$ is an isomorphism.

(b) Prove that f is a monomorphism if and only if $F(f)$ is injective.

3.16 Let $\mathbf{C}$ be a category, $Y \to X \leftarrow X'$ morphisms in $\mathbf{C}$, and suppose that the fibred product $Y \times_X Y'$ exists. Prove: if $Y \to X$ is a monomorphism, then so is $Y \times_X Y' \to Y'$; and if both $Y \to X$ and $Y' \to X$ are monomorphisms, then so is $Y \times_X Y' \to X$.

3.17 (a) Let π be a profinite group and E a finite π-set. Prove that E, as an object of π-**sets**, is connected if and only if the action of π on E is transitive.

(b) Let K be a field and A a free separable K-algebra. Prove that A, as an object of the category opposite to ${}_K\mathbf{SAlg}$, is connected if and only if A is a field.

(c) Let X be a connected topological space and $Y \to X$ a finite covering. Prove that $Y \to X$, as an object of the category of finite coverings of X, is connected if and only if Y is connected as a topological space.

(d) Let X be a connected scheme and $Y \to X$ a finite étale covering. Prove that $Y \to X$, as an object of $\mathbf{FEt}_X$, is connected if and only if the scheme Y is connected. (See Exercise 5.16.)

3.18 (**Injective limits.**) An *injective system* of sets consists of a directed partially ordered set I, a collection of sets $(S_i)_{i\in I}$ and a collection of maps $(f_{ij}\colon S_i \to S_j)_{i,j\in I,\ i\le j}$ satisfying the conditions

$$f_{ii} = (\text{identity on } S_i) \quad \text{for each} \quad i \in I,$$
$$f_{ik} = f_{jk} \circ f_{ij} \quad \text{for all} \quad i,j,k \in I \text{ with } i \le j \le k.$$

Call $x \in S_i$ *equivalent* to $y \in S_j$ if there exists $k \in I$ with $k \ge i$, $k \ge j$ and $f_{ik}(x) = f_{jk}(y)$ in S_k.

(a) Prove that this is an equivalence relation on the disjoint union of the sets S_i. The set of equivalence classes is called the *injective limit* of the system, notation: $\varinjlim S_i$ or $\varinjlim_{i\in I} S_i$.

(b) Prove that the injective limit can be interpreted as a right limit (Exercise 3.1).

(c) Suppose that $I \neq \emptyset$, that all S_i are groups and that all f_{ij} are group homomorphisms. Show that $\varinjlim S_i$ has a natural group structure.

(d) Let I be the set of positive integers, ordered by divisibility. For $n, m \in I$, n dividing m, let $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the group homomorphism mapping $(1 \bmod n)$ to $(m/n \bmod m)$. Prove that $\varinjlim \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}$.

3.19 Describe the connected Galois objects in the category π-**sets**, for a profinite group π. Do the same thing for the category opposite to ${}_K\mathbf{SAlg}$, for a field K.

3.20 Let H be a covariant functor from a category $\mathbf{C}$ to a category $\mathbf{D}$. Prove that H is an equivalence of categories if and only if the following two conditions are satisfied:

(i) every object of $\mathbf{D}$ is isomorphic to one of the form $H(X)$, for an object X of $\mathbf{C}$;

(ii) for any two objects X, Y of $\mathbf{C}$ the functor H yields a bijective map $\mathrm{Mor}_{\mathbf{C}}(X,Y) \to \mathrm{Mor}_{\mathbf{D}}(H(X),H(Y))$.

3.21 Let $X \to Z$ be an epimorphism in a Galois category, and $W \to Z$ a subobject different from $0, Z$. Prove that $W \times_Z X \to X$ is a subobject different from $0, X$.

3.22 Let **Gal** be the category whose objects are pairs $(\mathbf{C}, F)$ where $\mathbf{C}$ is a small Galois category and F a fundamental functor on $\mathbf{C}$. A morphism$(\mathbf{C}, F) \to (\mathbf{C}', F')$ is a functor $G\colon \mathbf{C} \to \mathbf{C}'$ with $F = F'G$. Prove that the assignment $(\mathbf{C}, F) \mapsto \mathrm{Aut}(F)$ extends to a contravariant functor from **Gal** to the category of profinite groups with continuous group homomorphisms. Is this functor an anti-equivalence of categories?

3.23 Let $\pi' \to \pi$ be a homomorphism of profinite groups and $G'\colon \pi$-**sets** $\to \pi'$-**sets** the induced functor (see 3.20).

(a) Prove that $\pi' \to \pi$ is surjective if and only if G' sends connected π-sets to connected π'-sets.

(b) Prove that $\pi' \to \pi$ is injective if and only if for every connected object X' of π'-**sets** there is an object X of π-**sets** and a connected component Y' of $G'(X)$ such that there is a π'-homomorphism $Y' \to X'$.

3.24 Let $\mathbf{C}$ be a category and $F\colon \mathbf{C} \to$ **sets** a covariant functor. Prove that the following two assertions are equivalent:

(i) $\mathbf{C}$ is a Galois category with fundamental functor F;

(ii) for every set S of objects of $\mathbf{C}$ there is a set T of objects of $\mathbf{C}$ with $S \subset T$ such that the category $\mathbf{D}$ whose objects are the elements of T, with the same morphisms as in $\mathbf{C}$, is a small Galois category with fundamental functor $F|\mathbf{D}$.

3.25 Let $\mathbf{C}$ be a Galois category with fundamental functor F, let A be a connected object of $\mathbf{C}$ (cf. 3.12), and $a \in F(A)$. By $\mathbf{C}_A$ we denote the category whose objects are morphisms $f\colon X \to A$ in $\mathbf{C}$, a morphism from $f\colon X \to A$ to $g\colon Y \to A$ in $\mathbf{C}_A$ being a morphism $h\colon X \to Y$ in $\mathbf{C}$ for which $f = gh$.

(a) Define the functor $F_a\colon \mathbf{C}_A \to$ **sets** by sending $f\colon X \to A$ to the subset $F(f)^{-1}(a)$ of $F(X)$. Prove that $\mathbf{C}_A$ is a Galois category with fundamental functor F_a.

(b) Define the functor $G\colon \mathbf{C} \to \mathbf{C}_A$ by $G(X) = (X \times A \to A)$ (the canonical projection). Prove that $F_a G$ is a fundamental functor on $\mathbf{C}$.

(c) Prove that if $\mathbf{C}$ is small the profinite group $\mathrm{Aut}(F_a)$ is isomorphic to an open subgroup of $\mathrm{Aut}(F)$.

(d) Define the functor $J\colon \mathbf{C}_A \to \mathbf{C}$ by $J(X \to A) = X$. Prove that (J, G) is an adjoint pair of functors, i.e.,

$$\mathrm{Mor}_{\mathbf{C}}(J(Y), X) \cong \mathrm{Mor}_{\mathbf{C}_A}(Y, G(X))$$

functorially in X and Y.

3.26 Let $\mathbf{C}$ be the category defined as follows. An *object* of $\mathbf{C}$ is a triple $(D, \lambda, (\sigma_\alpha)_{\alpha<\lambda})$ where D is a finite set, λ an ordinal number and $\sigma_\alpha\colon D \to D$ a map, for each ordinal number $\alpha < \lambda$, such that

$$\begin{aligned} \sigma_\alpha^2 &= \mathrm{id}_D \qquad && \text{for all } \alpha < \lambda\ , \\ \sigma_\alpha &= \mathrm{id}_D \qquad && \text{for almost all } \alpha < \lambda\ , \\ \sigma_\alpha \sigma_\beta &= \sigma_\beta \sigma_\alpha \qquad && \text{for all } \alpha, \beta < \lambda. \end{aligned}$$

A *morphism* from $(D, \lambda, (\sigma_\alpha)_{\alpha<\lambda})$ to $(E, \mu, (\tau_\alpha)_{\alpha<\mu})$ is a map $f\colon D \to E$ for which $f\sigma_\alpha = \tau_\alpha f$ for all $\alpha < \min\{\lambda, \mu\}$; $f\sigma_\alpha = f$ for all α with $\min\{\lambda, \mu\} \le \alpha < \lambda$; and $f = \tau_\alpha f$ for all α with $\min\{\lambda, \mu\} \le \alpha < \mu$.

Let $F\colon \mathbf{C} \to \mathbf{sets}$ be the forgetful functor sending $(D, \lambda, (\sigma_\alpha)_{\alpha<\lambda})$ to D. Prove that $\mathbf{C}$ is a Galois category with fundamental functor F, and that $\mathbf{C}$ is not essentially small.

3.27 Let $\mathbf{C}$ be the category whose objects are quintuples $(S, T, \alpha, \beta, \gamma)$, where S, T are finite sets and $\alpha, \beta, \gamma\colon S \to T$ are bijections, a morphism from $(S, T, \alpha, \beta, \gamma)$ to $(S', T', \alpha', \beta', \gamma')$ being a pair of maps $f\colon S \to S'$, $g\colon T \to T'$ for which $g\alpha = \alpha' f$, $g\beta = \beta' f$, $g\gamma = \gamma' f$.

(a) Prove that $\mathbf{C}$ is an essentially small Galois category, with a suitably defined fundamental functor.

(b) Describe the connected objects of $\mathbf{C}$.

(c) For which profinite group π is $\mathbf{C}$ equivalent to π-**sets**?

4 Projective modules and projective algebras

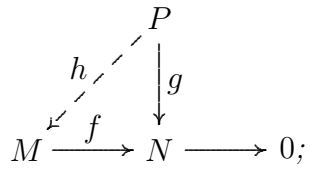
This section contains the affine information needed for the following section. We denote by A a ring.

4.1 Definition. An A-module P is called *projective* if the functor $\mathrm{Hom}_A(P,-)$ on the category of A modules is exact, i.e., if for every exact sequence $M_0 \to M_1 \to M_2$ of A-modules the induced sequence $\mathrm{Hom}_A(P,M_0) \to \mathrm{Hom}_A(P,M_1) \to \mathrm{Hom}_A(P,M_2)$ is exact.

4.2 Theorem. *For any A-module P the following four assertions are equivalent:*

(i) *P is projective;*

(ii) *for every surjective A-homomorphism $f\colon M \to N$ and every A-homomorphism $g\colon P \to N$ there exists an A-homomorphism $h\colon P \to M$ for which $fh = g$:*



(iii) *every exact sequence of A-modules $0 \to M_0 \to M_1 \to P \to 0$ splits (see Exercise 4.2);*

(iv) *there is an A-module Q for which $P \oplus Q$ is a free A-module.*

Proof. (i)⇒(ii) If $M \to N \to 0$ is exact, then $\mathrm{Hom}(P,M) \to \mathrm{Hom}(P,N) \to 0$ is exact, so $g \in \mathrm{Hom}(P,N)$ is the image of some $h \in \mathrm{Hom}(P,M)$.

(ii)⇒(iii) Take $M = M_1,\ \ N = P,\ \ g = \mathrm{id}_P$, and apply Exercise 4.2.

(iii)⇒(iv) Mapping the basis element s of a free module F of sufficiently large (possibly infinite) rank to a collection of generators for P we obtain a surjective A-homomorphism $F \to P$. Calling the kernel Q and applying (iii) to the sequence $0 \to Q \to F \to P \to 0$ one finds that $P \oplus Q \cong F$.

(iv)⇒(i) Since $\mathrm{Hom}_A(A,M) \cong M$, the A-module A is clearly projective. Further, if $(P_i)_{i\in I}$ is any collection of A-modules, then it is easy to prove that $\bigoplus_{i\in I} P_i$ is projective if and only if each P_i is projective (cf. Exercise 4.4). These facts immediately imply (iv)⇒(i).

This proves 4.2.

4.3 Flatness. Recall that an A-module P is called *flat* if the functor $-\otimes_A P$ on the category of A-modules is exact. Clearly A is flat, and replacing "projective" by "flat" in the proof of 4.2, (iv)⇒(i), one finds that direct summands of free modules are flat. We conclude that *projective modules are flat.*

4.4 Examples. (a) Suppose that there are rings A_1, A_2 with $A \cong A_1 \times A_2$. Then each A_i is a projective A-module. If the A_i are non-zero these modules are not free. Every A-module P can be written as $P = P_1 \times P_2$, where P_i is an A_i-module (namely, $P_1 = (1,0) \cdot P$ and $P_2 = (0,1) \cdot P$), and P is projective over A if and only if each P_i is projective over A_i.

(b) If A is a field, then every A-module is free, hence projective. If $A = K[G]$, where K is a field and G a finite abelian group of order not divisible by $\mathrm{char}(K)$, then again every A-module is projective (see Exercise 4.6 or 4.7).

(c) A $\mathbb{Z}$-module is projective if and only if it is free. This is because every subgroup of a free abelian group is free. In this example $\mathbb{Z}$ can be replaced by any principal ideal domain (see Exercise 4.9).

(d) Let A be the ring of integers of an algebraic number field or, more generally, a Dedekind domain. Then a non-zero finitely generated A-module is projective if and only if it is torsionfree, and if and only if it is isomorphic to a module of the form $A^n \oplus I$ for some $n \geq 0$ and some non-zero ideal I of A; moreover, $A^n \oplus I \cong A^{n'} \oplus I'$ if and only if $n = n'$ and I and I' have the same ideal class. See Exercises 4.10 and 4.11 for this. Hence if A has a non-trivial class group then there are projective A-modules that are not free. We remark that projective A-modules that are not finitely generated are free (Exercise 4.12).

(e) Let A be a domain, with field of fractions K. An A-submodule I of K is projective if and only if it is *invertible*, i.e., if and only if $IJ = A$ for some $J \subset K$, where $IJ = \{\sum_{i=1}^{n} x_i y_i : n \in \mathbb{Z},\ n \geq 0,\ x_i \in I,\ y_i \in J\ (1 \leq i \leq n)\}$; see Exercise 4.13.

(f) If $A = K[X_1, X_2, \ldots, X_n]$, where K is a field and $n < \infty$, then every projective A-module is free. This was proved by D. Quillen and A.A. Suslin in 1976, answering a question of Serre from 1955. See [16] for the case of finitely generated modules, and [3] for the other case.

(g) If A is a *local* ring, then every projective A-module is free. This was proved by I. Kaplansky [14]. For finitely generated modules we prove this below (see 4.5), the countably generated case is done in Exercise 4.14, and the general case in Exercise 4.16.

For more information about projective modules, see [4; 16; 21] and the references given there.

4.5 Proposition. *A finitely generated module over a local ring is projective if and only if it is free.*

Proof. Let A be a local ring with maximal ideal $\mathfrak{m}$ and P a finitely generated projective A-module. Let $x_1, x_2, \ldots, x_n \in P$ be such that the $x_i \otimes 1$ form a basis for the $A/\mathfrak{m}$-vector space $P \otimes_A A/\mathfrak{m}$. Let $f\colon A^n \to P$ send the i-th basis vector to x_i. Then $f \otimes \mathrm{id}_{A/\mathfrak{m}}$ is an isomorphism $(A/\mathfrak{m})^n \to P \otimes_A (A/\mathfrak{m})$, so the cokernel M of f, which is a finitely generated

module, satisfies $M = \mathfrak{m}M$. By the lemma of Nakayama [1, Proposition 2.6] this implies that $M = 0$, so f is surjective. By 4.2(iii) we now have $A^n \cong P \oplus \ker(f)$. It follows that $\ker(f)$ is finitely generated and satisfies $\ker(f) = \mathfrak{m} \cdot \ker(f)$. Again applying Nakayama's lemma we conclude that $\ker(f) = 0$, so f is an isomorphism. This proves the "only if" part of 4.5. The "if" part is immediate from 4.2. This proves 4.5.

4.6 Local characterization of projective modules. For $f \in A$ we write $A_f = S^{-1}A$, where $S = \{f^n : n \geq 0\}$, and $M_f = S^{-1}M = M \otimes_A A_f$ for an A-module M. Recall that M is *finitely presented* if there is an exact sequence $A^m \to A^n \to M \to 0$ of A-modules with $m, n < \infty$.

Theorem. *Let A be a ring and P an A-module. The following properties are equivalent:*

(i) *P is a finitely generated projective A-module;*

(ii) *P is finitely presented, and $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module for any maximal ideal $\mathfrak{m}$ of A;*

(iii) *there is a collection $(f_i)_{i \in I}$ of elements of A with $\sum_{i \in I} Af_i = A$, such that for each $i \in I$ the A_{f_i}-module P_{f_i} is free of finite rank.*

Notice that (iii) just means that the sheaf associated to P on $\operatorname{Spec} A$ is locally free of finite rank (see [10, Chapter II, Section 5]). Exercise 4.23 shows that one cannot replace "finitely presented" by "finitely generated" in (ii).

Proof. (ii)⇒(i) Assuming (i) we have $P \oplus Q \cong A^n$ for some Q and some $n < \infty$ (Exercise 4.3). Then Q is finitely generated, so P is finitely presented. From $P_\mathfrak{m} \oplus Q_\mathfrak{m} \cong A^n_\mathfrak{m}$ we see that $P_\mathfrak{m}$ is a finitely generated projective $A_\mathfrak{m}$-module, so $P_\mathfrak{m}$ is free by 4.5.

(ii)⇒(iii) Assume (ii), and let $\mathfrak{m}$ be a maximal ideal of A. Choose isomorphisms $g\colon A^n_\mathfrak{m} \to P_\mathfrak{m}$, $h\colon P_\mathfrak{m} \to A^n_\mathfrak{m}$ that are inverse to each other. By Exercise 4.20, we have $\operatorname{Hom}_{A_\mathfrak{m}}(A^n_\mathfrak{m}, P_\mathfrak{m}) \cong \operatorname{Hom}_A(A^n, P)_\mathfrak{m}$ and $\operatorname{Hom}_{A_\mathfrak{m}}(P_\mathfrak{m}, A^n_\mathfrak{m}) \cong \operatorname{Hom}_A(P, A^n)_\mathfrak{m}$, so $g = g'/s$, $h = h'/t$ for certain A-linear maps $g'\colon A^n \to P$, $h'\colon P \to A^n$ and certain $s, t \in A - \mathfrak{m}$. From $gh = \mathrm{id}_{P_\mathfrak{m}}$, $hg = \mathrm{id}_{A^n_\mathfrak{m}}$ it follows that $ug'h' = ust \cdot \mathrm{id}_P$, $vh'g' = vst \cdot \mathrm{id}_{A^n}$ for certain $u, v \in A - \mathfrak{m}$. With $f = stuv \in A - \mathfrak{m}$, $g'' = tuvg'/f$ $(= g'/s)$, $h'' = suvh'/f$ $(= h'/t)$ we now have isomorphisms $g''\colon A^n_f \to P_f$, $h''\colon P_f \to A^n_f$ over A_f that are inverse to each other. Letting $\mathfrak{m}$ range over all maximal ideals of A, we obtain a collection of f's that is not contained in any maximal ideal and therefore generates A as an A-ideal.

(iii)⇒(i) Writing $1 \in A$ as a linear combination of the f_i we see that we may assume that I is *finite*. For each $i \in I$, choose an isomorphism $g_i\colon A^{n(i)}_{f_i} \to P_{f_i}$ that maps the canonical basis vectors of $A^{n(i)}_{f_i}$ inside the image of P in P_{f_i}, so that g_i is induced by an A-linear map $g'_i\colon A^{n(i)} \to P$. These maps combine to a map $g'\colon A^{\sum_{j \in I} n(j)} \to P$. Applying

Exercise 4.21(a) to the cokernel of g' we see that g' is *surjective.* For each $i \in I$ the map g' induces a map $A_{f_i}^{\sum_{j\in I} n(j)} \to P_{f_i}$ whose kernel is isomorphic to $A_{f_i}^{\sum_{j\neq i} n(j)}$, hence finitely generated. By Exercise 4.21(b) it now follows that the kernel of g' is finitely generated, so P is *finitely presented.* Let $M \to N$ be any surjective map of A-modules. Then the map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$ becomes surjective after tensoring with A_{f_i}, for any $i \in I$; here we use Exercise 4.20 and the fact P_{f_i} is A_{f_i}-projective. Applying Exercise 4.21(a) to the cokernel of $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$ we see that this map is *surjective*, so that P is projective by 4.2(ii).

This completes the proof of the theorem.

4.7 The rank of a projective module. Let P be a finitely generated projective A-module. From Theorem 4.6(iii) it follows that for each $\mathfrak{p} \in \operatorname{Spec} A$ the $A_\mathfrak{p}$-module $P_\mathfrak{p}$ is *free*, and that the function

$$\mathrm{rank}(P) = \mathrm{rank}_A(P) \colon \operatorname{Spec} A \to \mathbb{Z}$$

assigning to $\mathfrak{p}$ the rank of $P_\mathfrak{p}$ over $A_\mathfrak{p}$ is *locally constant*, hence *continuous.* If $\operatorname{Spec} A$ is connected, e.g., if A is a domain, then $\mathrm{rank}(P)$ is *constant* and may be identified with a non-negative integer. We say that P is *faithfully projective* if $\mathrm{rank}(P) \geq 1$, i.e., $\mathrm{rank}(P)(\mathfrak{p}) \geq 1$ for all $\mathfrak{p} \in \operatorname{Spec} A$.

4.8 The trace. Let P be a finitely generated projective A-module, and $P^* = \mathrm{Hom}(P, A)$. For each A-module M, define

$$\phi \colon P^* \otimes_A M \to \mathrm{Hom}_A(P, M)$$

by $\phi(f \otimes m)(p) = f(p) \cdot m$. We claim that ϕ is an *isomorphism* of A-modules. This is clear if $P = A$, since then both modules may be identified with M, and ϕ becomes id_M. Taking direct sums we find that ϕ is also an isomorphism if $P \cong A^n$ for some $n < \infty$, and passing to direct summands one deals with general P.

The *trace*

$$\mathrm{Tr} = \mathrm{Tr}_{P/A} \colon \mathrm{End}_A(P) \to A$$

is now defined to be the composite of the maps

$$\mathrm{End}_A(P) = \mathrm{Hom}_A(P, P) \xrightarrow{\phi^{-1}} P^* \otimes_A P \to A$$

where $P^* \otimes_A P \to A$ maps $f \otimes p$ to $f(p)$.

The trace is an A-linear map, which agrees with the trace defined in 1.1 in the case that $P \cong A^n$; see Exercise 4.35. It follows that the trace defined in 1.1 is independent of the choice of the basis. See Exercise 4.36–4.40 for further properties of the trace.

4.9 Projective algebras. A *finite projective* A-algebra is an A-algebra B that is finitely generated projective when considered as an A-module. For such an algebra we write $[B : A]$ for $\operatorname{rank}_A(B)$; this is a continuous function $\operatorname{Spec} A \to \mathbb{Z}$.

4.10 Proposition. *Let B be a finite projective A-algebra. Then we have:*

(a) *the map $A \to B$ is injective if and only if $[B : A] \geq 1$ (i.e., $[B : A](\mathfrak{p}) \geq 1$ for all $\mathfrak{p} \in \operatorname{Spec} A$);*

(b) *the map $A \to B$ is surjective if and only if $[B : A] \leq 1$, and if and only if the map $B \otimes_A B \to B$ sending $x \otimes y$ to xy is an isomorphism;*

(c) *the map $A \to B$ is an isomorphism if and only if $[B : A] = 1$.*

Proof. (a) "Only if". If $[B : A](\mathfrak{p}) = 0$, then $B_\mathfrak{p} = 0$, so $A_\mathfrak{p} \to B_\mathfrak{p}$ is not injective, and consequently $A \to B$ is not injective either. "If". If $[B : A](\mathfrak{p}) \geq 1$, then the kernel of $A_\mathfrak{p} \to B_\mathfrak{p}$ annihilates the non-zero free $A_\mathfrak{p}$-module $B_\mathfrak{p}$, so must be zero. But if $A_\mathfrak{p} \to B_\mathfrak{p}$ is injective for all $\mathfrak{p}$ then so is $A \to B$.

(b) First suppose that $B \otimes_A B \xrightarrow{\sim} B$. Comparing the ranks we see, using Exercise 4.26, that $[B : A]^2 = [B : A]$, so $[B : A] \leq 1$. Next suppose that $[B : A] \leq 1$. To prove that $A \to B$ is surjective we may assume that A is *local*; then $[B : A]$ is constant. If $[B : A] = 0$ then $B = 0$ and clearly $A \to B$ is surjective. Next suppose that $[B : A] = 1$. Then $\operatorname{End}_A(B)$ is free of rank 1 over A, the identity map of B forming a basis. The map $\psi\colon B \to \operatorname{End}_A(B)$ defined by $\psi(b)(x) = bx$ is injective, and the composed map $A \to B \to \operatorname{End}_A(B)$ is an isomorphism, so $A \to B$ is surjective. Finally, if $A \to B$ is surjective then $B \cong A/\mathfrak{a}$ for some ideal $\mathfrak{a}$ of a, and $B \otimes_A B = B/\mathfrak{a}B = B$.

(c) This is clear from (a) and (b).

This proves 4.10.

4.11 Faithfully projective algebras. An A-algebra B is called *faithfully projective* if it is finite projective with $[B : A] \geq 1$, i.e., if it is faithfully projective as an A-module. See 4.10(a) and Exercise 4.25 for equivalent properties. In particular we see that B is *faithfully flat* over A if it is faithfully projective (see Exercise 4.25, and Exercise 3.16 of [1]).

4.12 Proposition. *Let B be a faithfully flat A-algebra, and P an A-module. Then P is finitely generated projective as an A-module if and only if $P \otimes_A B$ is finitely generated projective as a B-module.*

Proof. The "only if" part is true for any A-algebra B, see Exercise 4.33. To prove the "if" part, assume that $P \otimes_A B$ is a finitely generated projective as a B-module. Choose a finite collection of generators of $P \otimes_A B$ of the form $p \otimes 1$, with $p \in P$. These give rise to an

A-linear map $A^n \to P$ that becomes surjective when tensored with B; so by faithful flatness $A^n \to P$ is already surjective. Let Q be the kernel. Then $0 \to Q \otimes_A B \to B^n \to P \otimes_A B \to 0$ is exact, so $Q \otimes_A B$ is finitely generated projective over B, and applying what we just proved for P to Q we conclude that Q is finitely generated and hence that P is *finitely presented.*

Let M be any A-module. We claim that the natural map

$$Hom_A(P, M) \otimes_A B \to \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B)$$

is an *isomorphism.* If $P \cong A^m$ for some $m < \infty$ this is clear, since both sides may be identified with $(M \otimes_A B)^m$. In the general case we choose an exact sequence $A^m \to A^n \to P \to 0$. Then we have a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_A(P, M) \otimes_A B & \longrightarrow & \mathrm{Hom}_A(A^n, M) \otimes_A B & \longrightarrow & \mathrm{Hom}_A(A^m, M) \otimes_A B \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) & \to & \mathrm{Hom}_B(A^n \otimes_A B, M \otimes_A B) & \to & \mathrm{Hom}_B(A^m \otimes_A B, M \otimes_A B).
\end{array}$$

The top row is exact by right exactness of $\mathrm{Hom}_A(-, M)$ and flatness of B, and the bottom row is exact for the same two reasons in reverse order. By what we just proved the two vertical arrows at the right are isomorphisms. Hence the remaining vertical arrow is an isomorphism, as required.

To prove that P is projective, let now $M \to N$ be a surjective A-linear map. Then $M \otimes_A B \to N \otimes_A B$ is surjective, and since $P \otimes_A B$ is projective it follows that $\mathrm{Hom}_B(P \otimes_A B, M \otimes_A B) \to \mathrm{Hom}_B(P \otimes_A B, N \otimes_A B)$ is surjective. By what we just proved this implies that $\mathrm{Hom}_A(P, M) \otimes_A B \to \mathrm{Hom}_A(P, N) \otimes_A B$ is surjective, so by faithful flatness of B the map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$ is surjective. This proves that P is projective over A.

This proves 4.12.

4.13 Projective separable algebras. Let B be a finite projective A-algebra. The *trace* $\mathrm{Tr}(b)$ or $\mathrm{Tr}_{B/A}(b)$ of an element $b \in B$ is defined to be the trace of the A-linear map $B \to B$ sending x to bx. Clearly $\mathrm{Tr}_{B/A} \colon B \to A$ is A-linear. Define the A-linear map $\phi \colon B \to \mathrm{Hom}_A(B, A)$ by $\phi(x)(y) = \mathrm{Tr}_{B/A}(xy)$ for $x, y \in B$. If ϕ is an isomorphism we call B a *projective separable* A-algebra.

The main properties of projective separable algebras will be developed in the next section, in scheme-theoretic language. It turns out that projective separable algebras correspond exactly to finite étale coverings of an affine scheme; see Proposition 5.6.

We close this section with two propositions about projective separable algebras that will be needed in the next section.

4.14 Proposition. *Let B be an A-algebra, and C a faithfully flat A-algebra such that $B \otimes_A C$ is a projective separable C-algebra. Then B is a projective separable A-algebra.*

Proof. From 4.12, with B and C in the roles of P and B, we see that B is a finite projective A-algebra. To show that the map $\phi\colon B \to \mathrm{Hom}_A(B, A)$ defined above is an isomorphism, it suffices to show that $\phi \otimes \mathrm{id}_C\colon B \otimes_A C \to \mathrm{Hom}_A(B, A) \otimes_A C$ is an isomorphism, because C is faithfully flat over A. As in the proof of 4.12, we may identify $\mathrm{Hom}_A(B, A) \otimes_A C$ with $\mathrm{Hom}_C(B \otimes_A C, C)$, and then $B \otimes_A C \to \mathrm{Hom}_C(B \otimes_A C, C)$ is induced by the trace map (Exercise 4.36). It is an isomorphism because $B \otimes_A C$ is projective separable over C. This proves 4.14.

4.15 Lemma. *Let B be a projective separable A-algebra and $f\colon B \to A$ an A-algebra homomorphism. Then there exist an A-algebra C and an isomorphism $B \cong A \times C$ of A-algebras such that f is the composition of $B \cong A \times C$ with the projection $A \times C \to A$.*

Proof. Since f is A-linear there is a unique $e \in B$ such that $f(x) = \mathrm{Tr}(ex)$ for all $x \in B$. We shall prove that e is an idempotent that gives rise to the desired splitting.

Putting $x = 1$ we see that $\mathrm{Tr}(e) = 1$. Because f is a ring homomorphism and Tr is A-linear we have $\mathrm{Tr}(exy) = f(xy) = f(x)f(y) = f(x)\mathrm{Tr}(ey) = \mathrm{Tr}(f(x)ey)$ for all $x, y \in B$. By the definition of separability this implies that $ex = f(x)e$ for all $x \in B$. This shows that e annihilates $\ker(f)$, so calculating $\mathrm{Tr}(e)$ by means of the exact sequence $0 \to \ker(f) \to B \to A \to 0$ and Exercise 4.38 we see that $\mathrm{Tr}(e) = f(e)$. Hence $f(e) = 1$, and the A-linear map $A \to B$ sending 1 to e yields an isomorphism $A \oplus \ker(f) \to B$ of A-modules. Putting $x = e$ in $ex = f(x)e$ we see that $e^2 = e$. Since e annihilates $\ker(f)$ it follows that the map $A \oplus \ker(f) \xrightarrow{\sim} B$ respects multiplication, if multiplication is defined componentwise on $A \oplus \ker(f)$. Since A and B have unit elements the same is true for $\ker(f)$, so this is an A-algebra.

This proves the lemma.

4.16 Proposition. *Let A be a ring and B a projective separable A-algebra. Consider $B \otimes_A B$ as a B-algebra via the second factor. Then there exist a B-algebra C and a B-algebra isomorphism $B \otimes_A B \xrightarrow{\sim} B \times C$ that, composed with the natural projection $B \times C \to B$, yields the map $B \otimes_A B \to B$ sending $x \otimes y$ to xy.*

Proof. From Exercise 4.47 we see that $B \otimes_A B$ is a projective separable B-algebra. Moreover, the map $f\colon B \otimes_A B \to B$ defined by $f(x \otimes y) = xy$ is a B-algebra homomorphism. The proposition now follows if we apply 4.15 to $f\colon B \otimes_A B \to B$. This proves 4.16.

Exercises for Section 4

4.1 Let $\mathbf{C}$ be the category of modules over a ring A, and F a covariant additive functor from $\mathbf{C}$ to the category of abelian groups (see Exercise 3.8). We call F *exact* if for every exact sequence $X \to Y \to Z$ in $\mathbf{C}$ the sequence $F(X) \to F(Y) \to F(Z)$ is exact. Prove that the following three assertions are equivalent:

(i) F is exact;

(ii) for every exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathbf{C}$ the sequence $0 \to F(X) \to F(Y) \to F(Z) \to 0$ is exact;

(iii) F commutes with arbitrary finite left or right limits.

4.2 Let $0 \to M_0 \to M_1 \to M_2 \to 0$ be a short exact sequence of modules over a ring A. The sequence is said to *split* if there is an isomorphism $M_1 \xrightarrow{\sim} M_0 \oplus M_2$ of A-modules for which the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M_0 & \longrightarrow & M_0 \oplus M_2 & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

(with the obvious maps in the bottom row) is commutative. Prove that the following three assertions are equivalent:

(i) the sequence $0 \to M_0 \to M_1 \to M_2 \to 0$ splits;

(ii) there is an A-linear map $M_1 \to M_0$ such that the composed map $M_0 \to M_1 \to M_0$ is the identity on M_0;

(iii) there is an A-linear map $M_2 \to M_1$ such that the composed map $M_2 \to M_1 \to M_2$ is the identity on M_2.

4.3 Let P be a *finitely generated* module over a ring A. Prove that P is projective if and only if $P \oplus Q \cong A^n$ for some finitely generated A-module Q and some non-negative integer n.

4.4 Let A be a ring, M an A-module, $(P_i)_{i \in I}$ a collection of A-modules, and $P = \bigoplus_{i \in I} P_i$. Prove that $\mathrm{Hom}_A(P, M) \cong \prod_{i \in I} \mathrm{Hom}_A(P_i, M)$ and $P \otimes_A M \cong \bigoplus_{i \in I}(P_i \otimes_A M)$.

4.5 Prove the statements in Example 4.4(a).

4.6 Let K be a field and G a finite abelian group of order not divisible by $\mathrm{char}(K)$. Prove that $K[G]$ is isomorphic to the product of a finite number of fields, and deduce that every $K[G]$-module is projective.

4.7 Let A be a ring and G a finite abelian group for which $\#G \cdot 1 \in A^*$.

(a) Suppose that $f\colon M \to N$ is a homomorphism of $A[G]$-modules, and $g\colon N \to M$ an A-linear map with $fg = \mathrm{id}_N$. Define $g'\colon N \to M$ by $g'(x) = (\#G \cdot 1)^{-1} \cdot \sum_{\sigma \in G} \sigma \cdot g(\sigma^{-1} \cdot x)$. Prove that g' is a homomorphism of $A[G]$-modules and that $fg' = \mathrm{id}_N$.

(b) Let P be an $A[G]$-module. Prove that P is projective as an $A[G]$-module if and only if P is projective when considered as an A-module. (See the following exercise for a converse.)

4.8 Let A be a ring and G a finite abelian group. Consider A as an $A[G]$-module by letting every $\sigma \in G$ act as the identity on A. Prove that A is projective as an $A[G]$-module if and only if $\#G \cdot 1 \in A^*$.

4.9 Let A be a ring with the property that every ideal of A is projective (a *hereditary* ring).

(a) Prove that any submodule of a free A-module is isomorphic to the direct sum of a collection of ideals of A.

(b) Prove that over a principal ideal domain a module is projective if and only if it is free.

4.10 (a) Let A be a ring, and I, J ideals of A with $I + J = A$. Prove that there is an exact sequence $0 \to I \cdot J \to I \oplus J \to A \to 0$ of A-modules, and that $I \oplus J \cong (I \cdot J) \oplus A$.

(b) Prove that every ideal of a Dedekind domain A is projective and that an A-module is projective if and only if it is isomorphic to a direct sum of a collection of ideals of A.

(c) Let M be a finitely generated module over a Dedekind ring A. Prove that M is projective if and only if M is torsionfree (i.e., if $am = 0$ with $a \in A$ and $m \in M$, then $a = 0$ or $m = 0$).

4.11 Let A be a Dedekind domain.

(a) Prove that two fractional A-ideals are isomorphic as A-modules if and only if they belong to the same ideal class.

(b) Let I, J be fractional A-ideals. Prove that the map $I \otimes_A J \to IJ$ sending $x \otimes y$ to xy is an A-module isomorphism. [*Hint:* Localize.]

(c) Let $I_1, I_2, \ldots, I_n, J_1, J_2, \ldots, J_m$ be fractional A-ideals. Prove that $I_1 \oplus I_2 \oplus \ldots \oplus I_n \cong J_1 \oplus J_2 \oplus \ldots \oplus J_m$ as A-modules if and only if $n = m$ and $I_1 I_2 \ldots I_n$ and $J_1 J_2 \ldots J_m$ belong to the same ideal class. [*Hint:* take exterior powers.]

4.12 Let A be a Dedekind domain and $(I_n)_{n=0}^{\infty}$ a sequence of fractional A-ideals. Prove that $\bigoplus_{n=0}^{\infty} I_n \cong \bigoplus_{n=0}^{\infty} A$ as A-modules, and deduce that every projective A-module that is not finitely generated is free.

4.13 Let A be a domain with field of fractions K, and $I \subset K$ an A-submodule.

(a) Prove that I is projective if and only if it is invertible, and that it is free if and only if it is principal. [*Hint:* map a free module onto I.]

(b) Prove that invertible ideals are finitely generated.

(c) Prove that A is a Dedekind domain if and only if all ideals of A are projective.

4.14 Let A be a local ring with residue class field k.

(a) Suppose $a_1, a_2, \ldots, a_n \in A$ are such that none of the a_i belongs to the ideal generated by the others, and let $a = (a_i)_{i=1}^n \in A^n$. Let $f\colon A^n \to A^n$ be an A-linear map with $f(a) = a$. Prove that $f \otimes \mathrm{id}_k$ is the identity mapping on k^n, and that f is invertible.

(b) Let F be a free A-module, P a direct summand of F, and $a \in P$. Prove that P has a free direct summand containing a. [*Hint:* Choose a basis of F on which a has the smallest possible number of non-zero coordinates, say $a_1, a_2, \ldots, a_n$, and apply (a) to a suitable map $A^n \to P \to A^n$.]

(c) Prove that a countably generated projective A-module is free.

4.15 Let A be a ring, I a set, M_i a countably generated A-module for $i \in I$, and $M = \bigoplus_{i\in I} M_i$. Suppose that $M = P \oplus Q$, where $P, Q \subset M$ are A-submodules of M.

(a) Write $i \to j$, for $i, j \in I$, if there exists $x \in M_i$ such that the P-component or the Q-component of x has a non-zero projection on M_j. Prove that for each $i \in I$ the set $D(i) = \{j \in I$: there exist $m \geq 0$ and $i_0, i_1, \ldots, i_m \in I$ with $i = i_0 \to i_1 \to \cdots \to i_m = j\}$ is *countable.*

(b) For $J \subset I$, write $M_J = \bigoplus_{j\in J} M_j \subset M$, $P_J = P \cap M_J$, $Q_J = Q \cap M_J$. Prove that for any $i \in I$ there is a countable subset J of I containing i such that $M_J = P_J \oplus Q_J$, and that for any such subset P_J and Q_J are direct summands of P and Q.

(c) Deduce that P is the direct sum of countably generated modules.
[*Hint:* use transfinite induction.]

4.16 Deduce from 4.14 and 4.15 that any projective module over a local ring is free.

4.17 Let an ideal $\mathfrak{a}$ of a ring A be called *almost nilpotent* if for every sequence $(a_i)_{i=0}^{\infty}$ of elements of $\mathfrak{a}$ there exists n with $\prod_{i=0}^{n} a_i = 0$.

(a) Prove that a nilpotent ideal is almost nilpotent.

(b) Prove that a finitely generated almost nilpotent ideal is nilpotent.

(c) Let $K[X_1, X_2, \dots]$ be the polynomial ring in countably many variables over a field K, and I the ideal generated by $\{X_k \cdot \prod_{i=1}^{n} X_i^{a(i)} : k, n \geq 1,\ a(i) \geq 0\ (1 \leq i \leq n),\ \sum_{i=1}^{n} a(i) \geq k\}$. Prove that $K[X_1, X_2, \dots]/I$ is a local ring whose maximal ideal is almost nilpotent but not nilpotent.

4.18 Let A be a local ring whose maximal ideal $\mathfrak{m}$ is almost nilpotent.

(a) Prove that any A-module M with $\mathfrak{m}M = M$ is zero.

(b) Let F be a free A-module. Prove that a subset of F is an A-basis if and only if it yields an $A/\mathfrak{m}$-basis for $F \otimes_A A/\mathfrak{m}$. Prove also that any generating set for F contains a basis.

4.19 Let A be a local ring whose maximal ideal $\mathfrak{m}$ is *not* almost nilpotent.

(a) Construct a countably generated non-zero A-module M with $M = \mathfrak{m}M$. [*Hint:* Consider a suitable injective limit $A \to A \to A \to \dots$.]

(b) Let $f\colon F \to M$ be A-linear, with F free and M as in (a). Prove that $\ker(f) \cup \mathfrak{m}F$ generates F but does not contain a basis.

4.20 Let M, N be modules over a ring A, with M finitely presented, and let $S \subset A$ be a multiplicative subset. Prove that the obvious map $S^{-1}\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ is an $S^{-1}A$-module isomorphism.

4.21 Let A be a ring, $(f_i)_{i \in I}$ a collection of elements of A with $\sum_{i \in I} Af_i = A$, and M an A-module.

(a) Suppose that $M_{f_i} = 0$ for all $i \in I$. Prove that $M = 0$.

(b) Suppose that $M_{f_i} = 0$ is a finitely generated A_{f_i}-module for each $i \in I$. Prove that M is finitely generated.

4.22 Let $M = \{q \in Q : q \text{ has a squarefree denominator}\}$, considered as a module over $A = \mathbb{Z}$. Prove that $M_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$-free of rank 1 for every prime ideal $\mathfrak{p}$ of A, but that M is not projective over A.

4.23 Let V be an infinite set and $A = \mathbb{F}_2^V$.

(a) Prove that A has a maximal ideal $\mathfrak{n}$ and that is not principal.

(b) Let $M = A/\mathfrak{n}$, with $\mathfrak{n}$ as in (a). Prove that M is finitely generated, that $M_{\mathfrak{m}}$ is $A_{\mathfrak{m}}$-free of rank ≤ 1 for every maximal ideal $\mathfrak{m}$ of A, but that M is not projective.

4.24 Let A be a ring and P a finitely generated projective A-module. Prove that A can be written as the product of finitely many rings, $A = A_1 \times A_2 \times \cdots \times A_n$, such that $P = P_1 \times P_2 \times \cdots \times P_n$ where each P_j is a finitely generated projective A_j-module of constant rank.

4.25 Let A be a ring and P a finitely generated projective A-module. Prove that the following four properties are equivalent:

(i) P is faithfully projective;

(ii) the map $A \to \mathrm{End}_{\mathbb{Z}}(P)$ giving the A-module structure is injective;

(iii) P is *faithful*, i.e., an A-module M is zero if and only if $M \otimes P = 0$;

(iv) P is *faithfully flat*, i.e., a sequence $M_0 \to M_1 \to M_2$ of A-modules is exact if and only if the induced sequence $M_0 \otimes P \to M_1 \otimes P \to M_2 \otimes P$ is exact.

4.26 Let P and P' be finitely generated projective modules over a ring A, and $k \in \mathbb{Z}$, $k \geq 0$. Prove that the A-modules $P \oplus P'$, $P \otimes P'$, $\mathrm{Hom}_A(P, P')$, $P^* = \mathrm{Hom}_A(P, A)$, $\bigwedge^k P$, $P^{\otimes k}$ are finitely generated projective, and that the ranks of these modules are given by

$$\begin{aligned}
&\mathrm{rank}(P \oplus P') = \mathrm{rank}(P) + \mathrm{rank}(P'),\\
&\mathrm{rank}(P \otimes P') = \mathrm{rank}(P) \cdot \mathrm{rank}(P'),\\
&\mathrm{rank}(\mathrm{Hom}_A(P, P')) = \mathrm{rank}(P) \cdot \mathrm{rank}(P'),\\
&\mathrm{rank}(P^*) = \mathrm{rank}(P),\\
&\mathrm{rank}(\textstyle\bigwedge^k P) = \binom{\mathrm{rank}(P)}{k},\\
&\mathrm{rank}(P^{\otimes k}) = \mathrm{rank}(P)^k
\end{aligned}$$

as functions on $\mathrm{Spec}\, A$.

4.27 Let P be a finitely generated A-module such that for each $\mathfrak{p} \in \mathrm{Spec}\, A$ the $A_{\mathfrak{p}}$-module $P_{\mathfrak{p}}$ is free of finite rank $r(\mathfrak{p})$, where $r\colon \mathrm{Spec}\, A \to \mathbb{Z}$ is continuous. Prove that P is finitely generated projective.

4.28 Let P be a finitely generated module over a ring A. Prove that P is projective of rank 1 if and only if P is *invertible*, i.e., if and only if $P \otimes Q \cong A$ for some A-module Q. [*Hint* for the "only if" part: take $Q = P^*$.]

4.29 For a ring A, let $\mathrm{Pic}(A)$ be the set of isomorphism classes of finitely generated projective A-modules of rank 1. Prove that $\mathrm{Pic}(A)$ is an *abelian group* with operation $\otimes_A$, the *Picard group* of A. Express the function $\mathrm{Hom}_A(-,-)\colon \mathrm{Pic}(A) \times \mathrm{Pic}(A) \to \mathrm{Pic}(A)$ in terms of the group operation.

4.30 Let A be a ring. The group K_0A is defined by generators and relations. There is one generator $[P]$ for each finitely generated projective A-module P (up to isomorphism), and one relation $[P \oplus P'] = [P] + [P']$ for each pair P, P' of such modules.

(a) Prove that $[P] = [P']$ if and only if P and P' are *stably isomorphic*, i.e., if and only if $P \oplus A^n \cong P' \oplus A^n$ for some $n \geq 0$.

(b) Prove that $\otimes_A$ induces a multiplication on K_0A that makes K_0A into a commutative *ring* with unit element $[A]$.

(c) Show that there are group homomorphisms $\phi\colon \mathrm{Pic}(A) \to (K_0A)^*$ and $\psi\colon K_0A \to \mathrm{Pic}(A)$ (the latter from an additive group to a multiplicative group) with $\psi\phi = \mathrm{id}_{\mathrm{Pic}(A)}$. [*Hint:* put $\psi([P]) = [\bigwedge^{\mathrm{rank}(P)} P]$, to be defined in a suitable way if $\mathrm{rank}(P)$ is non-constant.]

4.31 Let A be a ring, and H_0A the ring of continuous functions $\mathrm{Spec}\, A \to \mathbb{Z}$.

(a) Prove that $\mathrm{rank}\colon K_0A \to H_0A$ is a ring homomorphism.

(b) Construct a ring homomorphism $\lambda\colon H_0A \to K_0A$ such that $\mathrm{rank} \circ \lambda = \mathrm{id}_{H_0A}$.

(c) Let $\tilde{K}_0A = \ker\lambda$. Prove that $K_0A \cong H_0A \oplus \tilde{K}_0A$. *Remark.* It can be proved that $\tilde{K}_0A$ is the nilradical of K_0A; see [4, Proposition IX.4.6].

4.32 (a) Prove that $\tilde{K}_0A = 0$ if A is a field, or a local ring, or a principal ideal domain, or a semilocal ring (i.e., a ring with only finitely many maximal ideals).

(b) Prove that $\tilde{K}_0A \cong \mathrm{Pic}(A) \cong \mathrm{Cl}(A)$, the ideal class group of A, if A is a Dedekind domain.

4.33 Let A be a ring, B an A-algebra and P a projective A-module. Prove that $P \otimes_A B$ is a projective B-module, and that the diagram

$$\begin{array}{ccc} \mathrm{Spec}\, B & \longrightarrow & \mathrm{Spec}\, A \\ & {\scriptstyle \mathrm{rank}_B(P \otimes_A B)} \searrow \quad \swarrow {\scriptstyle \mathrm{rank}_A(P)} & \\ & \mathbb{Z} & \end{array}$$

commutes if P is finitely generated.

4.34 Prove that any ring homomorphism $f\colon A \to B$ induces a ring homomorphism $K_0A \to K_0B$ via $- \otimes_A B$, and that K_0 is a functor.

4.35 Let P be a free A-module with basis $w_1, w_2, \ldots, w_n$, and define $w_i^* \in P^* = \mathrm{Hom}_A(P, A)$ by $w_i^*(w_j) = 1$ if $i = j$ and $w_i^*(w_j) = 0$ if $i \neq j$.

(a) Prove that P^* is a free A-module with basis $w_1^*, w_2^*, \ldots, w_n^*$.

(b) Let $f\colon P \to P$ be A-linear, $f(w_i) = \sum_{j=1}^{n} a_{ij} w_j$ with $a_{ij} \in A$. Prove that $\phi^{-1}(f) = \sum_{i,j} a_{ij} w_i^* \otimes w_j$, where $\phi\colon P^* \otimes_A P \to \mathrm{Hom}_A(P,P)$ is as in 4.8.

(c) Prove that the traces defined in 1.1 and 4.8 coincide.

4.36 Let A be a ring, B an A-algebra and P a finitely generated projective A-module. Prove that the diagram of natural maps

$$\begin{array}{ccc} \mathrm{End}_A(P) & \xrightarrow{\otimes \mathrm{id}_B} & \mathrm{End}_B(P \otimes_A B) \\ \Big\downarrow{\scriptstyle \mathrm{Tr}_{P/A}} & & \Big\downarrow{\scriptstyle \mathrm{Tr}_{P\otimes_A B/B}} \\ A & \longrightarrow & B \end{array}$$

is commutative.

4.37 Let A be a ring and P a finitely generated projective A-module.

(a) Suppose that P has constant rank n. Prove that $\mathrm{Tr}_{P/A}(\mathrm{id}_P) = n \cdot 1 \in A$.

(b) In the general case, prove that $\mathrm{Tr}_{P/A}(\mathrm{id}_P)$ is the image of $\mathrm{rank}(P)$ under the natural map $H_0 A \to \Gamma(\mathrm{Spec}\, A, \mathcal{O}) \cong A$; here $H_0 A$ is as in Exercise 4.31, the sheaf $\mathcal{O}$ is the natural sheaf of rings on $\mathrm{Spec}\, A$ (see [10, Chapter II, Section 2]), the map $H_0 A \to \Gamma(\mathrm{Spec}\, A, \mathcal{O})$ is induced by the ring homomorphisms $\mathbb{Z} \to A_{\mathfrak{p}}$, and $\Gamma(\mathrm{Spec}\, A, \mathcal{O}) \cong A$ is the isomorphism from [10, Chapter II, Proposition 2.2].

4.38 Let A be a ring, $0 \to P_0 \to P_1 \to P_2 \to 0$ an exact sequence of A-modules in which P_1 and P_2 are finitely generated projective, and $g\colon P_1 \to P_1$ an A-linear map with $g[P_0] \subset P_0$. Denote by h the induced map $P_2 \to P_2$. Prove that P_0 is finitely generated projective and that $\mathrm{Tr}_{P_1/A}(g) = \mathrm{Tr}_{P_0/A}(g \mid P_0) + \mathrm{Tr}_{P_2/A}(h)$.

4.39 Let P and Q be two finitely generated projective A-modules, and $f\colon P \to Q$, $g\colon Q \to P$ two A-linear maps. Prove that $\mathrm{Tr}_{Q/A}(f \circ g) = \mathrm{Tr}_{P/A}(g \circ f)$.

4.40 (a) Let P be a finitely generated projective A-module. Prove that the map $\psi\colon \mathrm{End}_A(P) \to \mathrm{End}_A(P^*)$ defined by $\psi(f)(g) = g \circ f$ is an anti-isomorphism of not necessarily commutative rings, and that $\mathrm{Tr}_{P^*/A}(\psi(f)) = \mathrm{Tr}_{P/A}(f)$.

(b) Let $f\colon P \to P$ and $g\colon Q \to Q$ be endomorphisms of finitely generated projective A-modules P and Q. Prove that $\mathrm{Tr}_{P\otimes Q/A}(f \otimes g) = \mathrm{Tr}_{P/A}(f) \cdot \mathrm{Tr}_{Q/A}(g)$.

4.41 Let $B_1, B_2, \ldots, B_n$ be algebras over a ring A. Prove that $\prod_{i=1}^{n} B_i$ is a finite projective A-algebra if and only if each B_i is a finite projective A-algebra.

4.42 Let A be a ring, B a finite projective A-algebra, and P a finitely generated projective B-module. Prove that P, when considered as an A-module, is finitely generated

and projective. Prove also that the map $\mathrm{Hom}_A(B,A) \otimes_B \mathrm{Hom}_B(P,B) \to \mathrm{Hom}_A(P,A)$ sending $f \otimes g$ to $f \circ g$ is *surjective.*

4.43 Let A be a ring, B a finite projective A-algebra, and C a finite projective B-algebra. Prove that C is a finite projective A-algebra. Can you express $[C : A]$ in terms of $[C : B]$ and $[B : A]$?

4.44 With A, B and C as in the previous exercise, show that $\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$.

4.45 Let $B_1, B_2, \ldots, B_n$ be algebras over a ring A. Prove that $\prod_{i=1}^n B_i$ is a projective separable A-algebra if and only if each B_i is a projective separable A-algebra.

4.46 Let A be a ring, B a projective separable A-algebra and C a projective separable B-algebra. Prove that C is a projective separable A-algebra. [*Hint:* use Exercises 4.42 and 4.44. In 5.12 we shall give a different proof.]

4.47 Let A be a ring, B a projective separable A-algebra and C any A-algebra. Prove that $B \otimes_A C$ is a projective separable C-algebra.

5 Finite étale morphisms

In this section we treat the basic properties of finite étale morphisms, and we prove the Main theorem 1.11.

5.1 Affine morphisms, locally free morphisms. Let $f\colon Y \to X$ be a morphism of schemes. We call f *affine* if there is an open affine cover $\{U_i\}$ of X such that $f^{-1}(U_i)$ is affine for each i or, equivalently, if $f^{-1}(U)$ is affine for every open affine $U \subset X$ (see [10, Chapter II, Exercise 5.17]). Notice that *finite* morphisms are affine. We call f *finite and locally free* if there exists a covering of X by open *affine* subsets $U_i = \operatorname{Spec} A_i$, such that $f^{-1}(U) = \operatorname{Spec} B_i$ is affine for each i, where B_i is an A_i-algebra that is finitely generated and free as an A_i-module.

5.2 Proposition. *Let $f\colon Y \to X$ be a morphism of schemes. Then f is finite and locally free if and only if for each open affine subset $U = \operatorname{Spec} A$ of X the open subscheme $f^{-1}(U)$ of Y is affine, $f^{-1}(U) = \operatorname{Spec} B$, where B is a finite projective A-algebra.*

Proof. The "if" part is clear from Theorem 4.6(iii). To prove the "only if" part, assume that f is finite and locally free, and let $U = \operatorname{Spec} A$ be open affine in X. Then $f^{-1}(U) = \operatorname{Spec} B$ is affine, since f is affine. As in the proof of [10, Chapter II, Proposition 3.2] there is a covering of U by open affine subsets $U_i = \operatorname{Spec} A_{f_i}$ such that for each i we have $f^{-1}(U_i) = \operatorname{Spec} B_{f_i}$, where B_{f_i} is an A_{f_i}-algebra that is finitely generated and free as an A_{f_i}-module. From Theorem 4.6 it now follows that B is a finite projective A-algebra. This proves 5.2.

5.3 The degree. Let $f\colon Y \to X$ be a finite and locally free morphism of schemes. For each open affine set $U = \operatorname{Spec} A$ in X, with $f^{-1}(U) = \operatorname{Spec} B$, there is a continuous rank function $[B : A] : U = \operatorname{Spec} A \to \mathbb{Z}$; see 4.9. Clearly, the functions belonging to different U's agree on their intersection, so they give rise to a continuous function $\operatorname{sp}(X) \to \mathbb{Z}$, where $\operatorname{sp}(X)$ denotes the underlying topological space of X. This function is called the *degree* of Y over X, or of f, and is denoted by $[Y : X]$ or $\deg(f)$. For each integer n the set $\{x \in \operatorname{sp}(X) : [Y : X](x) = n\}$ is open and closed in X. If $[Y : X]$ is constant, it is identified with the unique integer in its image; this occurs, for example, if X is connected.

A morphism $Y \to X$ of schemes is called *surjective* if the map of the underlying topological spaces is surjective.

5.4 Proposition. *Let $f\colon Y \to X$ be a finite and locally free morphism of schemes. Then we have:*

(a) $Y = \emptyset \Leftrightarrow [Y : X] = 0$;

(b) $Y \to X$ *is an isomorphism* $\Leftrightarrow [Y : X] = 1$;

(c) $Y \to X$ *is surjective* $\Leftrightarrow [Y : X] \geq 1 \Leftrightarrow$ *for every open affine subset* $U = \operatorname{Spec} A$ *of* X *we have* $f^{-1}(U) = \operatorname{Spec} B$*, where* B *is a faithfully projective* A*-algebra.*

Proof. We may clearly assume that $X = \operatorname{Spec} A$ is affine. Then $Y = \operatorname{Spec} B$ for some finite projective A-algebra B. Now (a) is trivial, (b) is the same as 4.10(c), and (c) reduces, by 4.10(a), to the statement that $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective if and only if $A \to B$ is injective. "If": since B is finite over A, this immediately follows from [1, Theorem 5.10]. "Only if": if $\mathfrak{p} \in \operatorname{Spec} A$, and $\mathfrak{q} \in \operatorname{Spec} B$ maps to $\mathfrak{p}$, then $B_{\mathfrak{p}} \neq 0$ since $B_{\mathfrak{q}} \neq 0$, so $[B : A](\mathfrak{p}) \neq 0$, and $A \to B$ is injective by 4.10(a). This proves 5.4.

5.5 Finite étale morphisms. We recall from 1.4 that a morphism $f\colon Y \to X$ is called finite étale if there is a covering of X by open affine sets $U_i = \operatorname{Spec} A_i$ such that for each i the open subscheme $f^{-1}(U_i)$ of Y is affine, $f^{-1}(U_i) = \operatorname{Spec} B_i$, where B_i is a free separable A_i-algebra. In particular we see that any finite étale morphism is finite and locally free.

5.6 Proposition. *A morphism* $f\colon Y \to X$ *is finite étale if and only if for each open affine subset* $U = \operatorname{Spec} A$ *of* X *the open subscheme* $f^{-1}(U)$ *of* Y *is affine,* $f^{-1}(U) = \operatorname{Spec} B$*, where* B *is a projective separable* A*-algebra.*

Proof. Clear from 5.2 and the remark that the map $\phi\colon B \to \operatorname{Hom}_A(B, A)$ from 4.13 is an isomorphism if and only if the induced map $B_{\mathfrak{p}} \to \operatorname{Hom}_{A_{\mathfrak{p}}}(B_{\mathfrak{p}}, A_{\mathfrak{p}})$ is an isomorphism for each $\mathfrak{p} \in \operatorname{Spec} A$ (cf. Exercise 4.20). This proves 5.6.

We refer to Exercises 5.1–5.8 for further basic properties of finite locally free and finite étale morphisms, in particular for the fact that these notions are stable under base extension (Exercises 5.5(a) and 5.8).

5.7 Surjective, finite and locally free morphisms. The study of finite étale morphisms is greatly simplified if we make base extensions $W \to X$ that are surjective, finite and locally free, as we shall now see. For an affine description of such morphisms we refer to Exercise 5.9.

5.8 Proposition. *Let* $f\colon Y \to X$ *be an affine morphism of schemes, and* $g\colon W \to X$ *a morphism that is surjective, finite and locally free. Then* $Y \to X$ *is finite étale if and only if* $Y \times_X W \to W$ *is finite étale.*

Proof. The "only if" part is correct for any $W \to X$, by Exercises 5.5(a) and 5.8. To prove the "if" part, let $U = \operatorname{Spec} A$ be an open affine part of X. Since f is affine we have

$f^{-1}(U) = \operatorname{Spec} B$ for some A-algebra B. To prove that f is finite étale it suffices to show that B is projective separable over A. By Exercise 5.9, we have $g^{-1}(U) = \operatorname{Spec} C$ for a faithfully projective A-algebra C. The inverse image of $\operatorname{Spec} C$ under $Y \times_X W \to W$ is $\operatorname{Spec} B \otimes_A C$, by [10, Chapter II, proof of Theorem 3.3]. Since $Y \times_X W \to W$ is finite étale, Proposition 5.6 implies that $B \otimes_A C$ is a projective separable C-algebra. From 4.14 it now follows that B is a projective separable A-algebra. This proves 5.8.

5.9 Totally split morphisms. A morphism $f\colon Y \to X$ of schemes is called *totally split* if X can be written as the disjoint union [10, Chapter II, Exercise 2.12] of schemes X_n, $n \in \mathbb{Z}$, $n \geq 0$, such that for each n the scheme $f^{-1}(X_n)$ is isomorphic to the disjoint union of n copies of X_n with the natural morphism $X_n \amalg X_n \amalg \cdots \amalg X_n \to X_n$. In many cases of interest we have $X = X_n$ for a single n; this must happen, for example, if X is connected. Clearly a totally split morphism is finite étale.

5.10 Theorem. *Let $f\colon Y \to X$ be a morphism of schemes. Then f is finite étale if and only if f is affine and $Y \times_X W \to W$ is totally split for some $W \to X$ that is surjective, finite and locally free.*

Proof. The "if" part is immediate from 5.8. To prove the "only if" part, let $f\colon Y \to X$ be finite étale, and first assume that $[Y : X] = n$ is *constant*. We prove by induction on n the existence of a surjective, finite and locally free morphism $W \to X$ such that $Y \times_X W \to W$ is totally split. If $n = 0$ we can simply take $W = X$. Next suppose that $n > 0$. We claim that the diagonal morphism $Y \to Y \times_X Y$ is both a closed immersion and an open immersion. If $X = \operatorname{Spec} A$ is affine, then also $Y = \operatorname{Spec} B$ is affine, and the splitting $\operatorname{Spec} B \amalg \operatorname{Spec} C \xrightarrow{\sim} \operatorname{Spec} B \otimes_A B$ implied by Proposition 4.16 proves our claim. In the general case we cover X with open affine subsets $U_i = \operatorname{Spec} A_i$, so that Y is covered with open affine subsets $f^{-1}(U_i) = \operatorname{Spec} B_i$ and $Y \times_X Y$ with open affine subsets $\operatorname{Spec} B_i \otimes_{A_i} B_i$, by [10, Chapter II, proof of Theorem 3.3], and our claim follows. We can now write $Y \times_X Y = Y \amalg Y'$. The second projection $Y \times_X Y \to Y$ is finite étale of degree n, by Exercises 5.5 and 5.8. Since $\mathrm{id}_Y\colon Y \to Y$ has rank 1, we see from Exercises 5.3 and 5.8 that the induced morphism $Y' \to Y$ is finite étale of rank $n - 1$. Applying the induction hypothesis we find a morphism $W \to Y$ that is surjective, finite and locally free such that $Y' \times_Y W \to W$ is totally split. We show that the composed morphism $W \to Y \to X$ now satisfies our requirements. Since $Y' \times_Y W \to W$ and $W = Y \times_Y W \to W$ are totally split, the same is true for $Y \times_X W = Y \times_X Y \times_Y W = (Y \amalg Y') \times_Y W = (Y \times_Y W) \amalg (Y' \times_Y W) \to W$. From $[Y : X] \geq 1$ it follows that $Y \to X$ is surjective, so $W \to X$ is also surjective. Finally, $W \to X$ is finite and locally free by Exercise 5.6. This concludes the induction step, and

finishes the proof of the existence of W in the case that the degree $[Y : X]$ is constant.

In the general case we write $X = \coprod_{n=0}^{\infty} X_n$, where $\mathrm{sp}(X_n) = \{x \in \mathrm{sp}(X) : [Y : X](x) = n\}$. Then $Y_n = f^{-1}(X_n) \to X_n$ is finite étale of constant degree n, for each n, so there exist surjective, finite and locally free morphisms $W_n \to X_n$ for which $Y_n \times_{X_n} W_n \to W_n$ is totally split. The combined morphism $W = \coprod_{n=0}^{\infty} W_n \to \coprod_{n=0}^{\infty} X_n = X$ now satisfies our requirements.

This proves 5.10.

5.11 The use of 5.10. Totally split morphisms of constant rank are the scheme theoretic analog of *trivial* finite coverings of a topological space X, i.e., coverings of the form $X \times E \to X$ where E is a discrete finite set. Locally, every finite covering is trivial, and any morphism between finite coverings is locally trivial as well (Lemma 3.8). This fact formed the basis of our proof of the topological Theorem 1.15 in Section 3. In the case of schemes, finite étale morphisms are only "locally trivial" if "locally" is understood in a suitable "Grothendieck topology": finite étale coverings become trivial (= totally split) after a base extension $W \to X$ as in Theorem 5.10. Below we shall see that any morphism $Y_1 \to Y_2$ between totally split morphisms $Y_1 \to X$, $Y_2 \to X$ is locally trivial in a sense analogous to Lemma 3.8; see Lemma 5.14. These facts enable us to reduce many proofs to the case of "trivial" morphisms, in which case straightforward verifications are usually sufficient.

As a first illustration of this technique we prove a result that can in fact be proved directly from the definitions (see Exercises 4.46, 5.6 and 5.8).

5.12 Proposition. *Let $Z \to Y$ and $Y \to X$ be finite étale morphisms of schemes. Then the composed morphism $Z \to X$ is finite étale.*

Proof. First assume that $Y \to X$ is totally split of constant degree: $Y = X \amalg X \amalg \cdots \amalg X$, with n summands. Then $Z = Z_1 \amalg Z_2 \amalg \cdots \amalg Z_n$, where each Z_i is finite étale (Exercises 5.4 and 5.8). By Exercises 5.4 and 5.8 also $Z_1 \amalg Z_2 \amalg \cdots \amalg Z_n \to X$ is finite étale, as required.

The case that $Y \to X$ is totally split of non-constant degree is immediately reduced to the preceding case, again with Exercises 5.4 and 5.8.

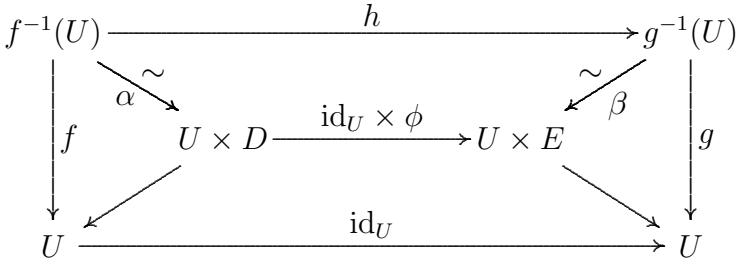
In the general case one chooses $W \to X$ as in Theorem 5.10, so that $Y \times_X W \to W$ is totally split. Since $Z \times_X W \to Y \times_X W$ is finite étale (Exercises 5.5(a) and 5.8), the result already proved implies that $Z \times_X W \to W$ is finite étale. From Proposition 5.8 it now follows that $Z \to X$ is finite étale. This proves 5.12.

5.13 Notation. If X is a scheme and E a finite set of cardinality n, we write $X \times E$ for the disjoint union of n copies of X, one for each element of E; cf. Exercise 5.11. Any map

$\phi\colon D \to E$ of finite sets induces in a natural way a morphism $X \times D \to X \times E$. The morphisms $X \times D \to X \times E$ obtained in this way are easily seen to be finite étale; this follows in fact from Exercises 5.3, 5.4, 5.8 and the remark that the identity morphism $X \times X$ is finite étale.

The following lemma is analogous to Lemma 3.8.

5.14 Lemma. *Let X, Y, Z be schemes, $f\colon Y \to X$ and $g\colon Z \to X$ totally split morphisms, $h\colon Y \to Z$ a morphism with $f = gh$, and $x \in X$. Then there exists an open affine neighborhood U of x in X such that f, g and h are "trivial above U", i.e., such that there exist finite sets D and E, isomorphisms $\alpha\colon f^{-1}(U) \to U \times D$ and $\beta\colon g^{-1}(U) \to U \times E$, and a map $\phi\colon D \to E$ such that the diagram*



is commutative; here $U \times D \to U$, $U \times E \to U$ are the first projections, and $U \times D \to U \times E$ is the morphism induced by ϕ.

Proof. Replacing X by a suitable open neighborhood of x we may assume that $X = \operatorname{Spec} A$ is *affine* and that the totally split morphisms f and g are each of *constant degree*, so that $Y \xrightarrow{\sim} X \times D = \operatorname{Spec} A^D$ and $Z \xrightarrow{\sim} X \times E = \operatorname{Spec} A^E$ for certain finite sets D and E (cf. Exercise 5.11(c)). It must be shown that the A-algebra homomorphism $\psi\colon A^E \to A^D$ corresponding to $h\colon Y \to Z$ is induced by a map $\phi\colon D \to E$, at least above an open affine neighborhood U of x. Since the local ring A_x has no non-trivial idempotents (Exercise 2.23(a)) it follows from Exercise 5.11(d) that the local map $\psi_x\colon A_x^E \to A_x^D$ is induced by a map $\phi\colon D \to E$. Hence ψ and the map $\phi^*\colon A^E \to A^D$ induced by ϕ have the same image in $\operatorname{Hom}_A(A^E, A^D)_x = \operatorname{Hom}_{A_x}(A_x^E, A_x^D)$ (Exercise 4.20). It follows that ψ and ϕ^* yield the same map $A[1/a]^E \to A[1/a]^D$ for some $a \in A$ not belonging to the prime ideal corresponding to x. The open neighborhood $U = \operatorname{Spec} A[1/a]$ of x in $\operatorname{Spec} A$ now satisfies our requirements. This proves Lemma 5.14.

Remark. In a completely analogous way one proves that any $x \in X$ has an open neighborhood U such that each of a given finite set of morphisms between totally split schemes over X is trivial above U, in a sense that is made precise in Exercise 5.12.

The first important consequence of Lemma 5.14 is that morphisms between finite étale coverings are finite étale as well.

5.15 Proposition. *Let $f\colon Y \to X$ and $g\colon Z \to X$ be finite étale morphisms of schemes, and $h\colon Y \to Z$ a morphism with $f = gh$. Then h is finite étale.*

Proof. If f and g are totally split the assertion follows from Lemma 5.14, since any morphism $U \times D \to U \times E$ induced by a map $D \to E$ is finite étale, as we remarked in 5.13. In the general case we choose surjective, finite and locally free morphisms $W_1 \to X$, $W_2 \to X$ such that $Y \times_X W_1 \to W_1$ and $Z \times_X W_2 \to W_2$ are totally split. Then $W = W_1 \times_X W_2 \to W$ is also surjective, finite and locally free (Exercise 5.7), and $Y \times_X W \to W$, $Z \times_X W \to W$ are totally split. Hence by the case already dealt with, $Y \times_X W \to Z \times_X W$ is finite étale. But $Z \times_X W \to Z$ is surjective, finite and locally free (Exercise 5.5), and $Y \times_X W = Y \times_Z (Z \times_X W)$, so applying Proposition 5.8 with $Z \times_X W$ and Z in the roles of W and X we conclude that $Y \to Z$ is finite étale; here we use that $Y \to Z$ is affine (Exercise 5.13). This proves 5.15.

5.16 Proposition. *Let $f\colon Y \to X$, $g\colon Z \to X$ be finite étale and $h\colon Y \to Z$ a morphism with $f = gh$. Then h is an epimorphism in $\mathbf{FEt}_X$ if and only if h is surjective.*

Proof. "Only if". By 5.15, the morphism h is finite and locally free, so $Z_0 = \{z \in Z : [Y : Z](z) = 0\}$ is open and closed in Z (see 5.3), and $Z = Z_0 \amalg Z_1$ where $Z_1 = Z - Z_0$. We have $h^{-1}(Z_0) = \emptyset$, by 5.4(a), and $h\colon Y \to Z_1$ is surjective by 5.4(c). The compositions of h with the two natural morphisms $Z = Z_0 \amalg Z_1 \rightrightarrows Z_0 \amalg Z_0 \amalg Z_1$ are the same, so if h is an epimorphism these two natural morphisms must be the same. Then $Z_0 = \emptyset$ and h is surjective, as required.

"If". Suppose that h is surjective and that $p, q\colon Z \to W$ are morphisms with $ph = qh$, with W finite étale over X. We have to prove that $p = q$, and this can be checked locally, so we may assume that $X = \operatorname{Spec} A$ is *affine.* Then $Y = \operatorname{Spec} B$, $Z = \operatorname{Spec} C$, and $W = \operatorname{Spec} D$ are also affine, and p, q, h correspond to maps $D \rightrightarrows C \to B$ giving the same map $D \to B$. The surjectivity of h implies that $[B : C] \geq 1$ (see 5.4(c)), hence that $C \to B$ is injective (see 4.10(a)). Therefore the two maps $D \rightrightarrows C$ are the same, and $p = q$.

This proves 5.16.

5.17 Proposition. *Let $f\colon Y \to X$, $g\colon Z \to X$ be finite étale and $h\colon Y \to Z$ a morphism with $f = gh$. Then h is a monomorphism in $\mathbf{FEt}_X$ if and only if h is both an open immersion and a closed immersion.*

Proof. The "if"-part is trivial (see Exercise 5.14). Conversely, assume that $h\colon Y \to Z$ is a monomorphism. Then the first projection $Y \times_Z Y \to Y$ is an isomorphism (Exercise 3.15(a)); here it should be noted that $Y \times_Z Y$ is finite étale over Z (Exercises 5.7(a) and 5.8) and hence over X (Proposition 5.12). If $U = \operatorname{Spec} A \subset X$ is open affine, and $f^{-1}(U) = \operatorname{Spec} B$, $g^{-1}(U) = \operatorname{Spec} C$, this yields an isomorphism $B \xrightarrow{\sim} B \otimes_C B$ sending b to $b \otimes 1$, so $[B : C] \leq 1$ by 4.10(b). This proves that $[Y : Z] \leq 1$. Putting $Z_n = \{z \in Z : [Y : Z](z) = n\}$ we therefore have $Z = Z_0 \amalg Z_1$, and from 5.4(a), (b) we see that $h^{-1}(Z_0) = \emptyset$, $h\colon Y \xrightarrow{\sim} Z_1$. This proves 5.17.

5.18 Quotients under group actions. For a scheme X, let $\mathbf{Aff}_X$ be the category of affine morphisms $Y \to X$ (see 5.1), a morphism between affine morphisms being defined as in 1.6. We show that in $\mathbf{Aff}_X$ quotients under finite groups of automorphisms exist. To do this, it is convenient to replace $\mathbf{Aff}_X$ by the anti-equivalent category of quasi-coherent sheaves of $\mathcal{O}_X$-algebras [10, Chapter II, Exercise 5.17]. So let $\mathcal{A}$ be a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, and G a finite group of automorphisms of $\mathcal{A}$. For any open subset $U \subset X$ the set $\mathcal{A}(U)^G$ of G-invariants of $\mathcal{A}(U)$ is a sub-$\mathcal{O}_X(U)$-algebra of $\mathcal{A}(U)$, and it is the kernel of the map $\mathcal{A}(U) \to \bigoplus_{\sigma \in G} \mathcal{A}(U)$ sending $a \in \mathcal{A}(U)$ to $(\sigma(a) - a)_{\sigma \in G} \in \bigoplus_{\sigma \in G} \mathcal{A}(U)$. Using [10, Chapter II, Proposition 5.7] we conclude that the assignment $U \mapsto \mathcal{A}(U)^G$ is a quasi-coherent sheaf of $\mathcal{O}_X$-algebras. We denote this sheaf by $\mathcal{A}^G$. It is straightforward to check that any morphism $f\colon \mathcal{B} \to \mathcal{A}$ of quasi-coherent sheaf $\mathcal{O}_X$-algebras satisfying $\sigma \circ f = f$ for all $\sigma \in G$ factors uniquely via the inclusion morphism $\mathcal{A}^G \to \mathcal{A}$. For the anti-equivalent category $\mathbf{Aff}_X$ this implies that for any affine morphism $f\colon Y \to X$ and any finite group G of automorphisms of $Y \to X$ in $\mathbf{Aff}_X$ the quotient $g\colon Y/G \to X$ exists in $\mathbf{Aff}_X$. The construction makes it also clear that for any open set $U \subset X$ we have $g^{-1}(U) \cong f^{-1}(U)/G$; and if $U = \operatorname{Spec} A$ is open affine, $f^{-1}(U) = \operatorname{Spec} B$, then $g^{-1}(U) = \operatorname{Spec} B^G$.

It is now our purpose to show that $Y/G \to X$ is finite étale if $Y \to X$ is finite étale. To do this we need the following auxiliary result.

5.19 Proposition. *Let $Y \to X$ be an affine morphism, G a finite group of automorphisms of $Y \to X$ in $\mathbf{Aff}_X$, and $W \to X$ a finite and locally free morphism. Then $(Y \times_X W)/G \cong (Y/G) \times_X W$ in $\mathbf{Aff}_W$.*

Proof. It is easy to see that $Y \times_X W \to W$ is affine, and that G induces a finite group of automorphisms of $Y \times_X W \to W$ in $\mathbf{Aff}_W$, so the quotient $(Y \times_X W)/G \to W$ is well-defined. The morphism $g\colon Y \times_X W \to (Y/G) \times_X W$ induced by the natural morphism $Y \to Y/G$ satisfies $g \circ \sigma = g$ for all $\sigma \in G$, so it gives rise to a morphism $(Y \times_X W)/G \to (Y/G) \times_X W$.

We claim that this is an isomorphism. This can be checked locally, so we may assume that $X = \operatorname{Spec} A$ is affine. Then $Y = \operatorname{Spec} B$ and $W = \operatorname{Spec} C$ are affine as well, and C is a finite projective A-algebra. It must be proved that the natural map $B^G \otimes_A C \to (B \otimes_A C)^G$ is an isomorphism. The sequence $0 \to B^G \to B \to \bigoplus_{\sigma \in G} B$ of A-modules, in which the last map sends $b \in B$ to $(\sigma(b) - b)_{\sigma \in G}$, is exact, so by the flatness of C (see 4.3) it gives rise to an exact sequence $0 \to B^G \otimes_A C \to B \otimes_A C \to \bigoplus_{\sigma \in G} B \otimes_A C$. This shows $B^G \otimes_A C \cong (B \otimes_A C)^G$, as required. This proves 5.19.

5.20 Proposition. *Let $Y \to X$ be a finite étale morphism of schemes, and G a finite group of automorphisms of $Y \to X$ in $\mathbf{FEt}_X$. Then the quotient $Y/G \to X$ of $Y \to X$ under G exists in $\mathbf{FEt}_X$.*

Proof. Since finite morphisms are affine, the quotient $g\colon Y/G \to X$ exists in $\mathbf{Aff}_X$. It suffices to show that $Y/G \to X$ is in fact finite étale.

Let it first be assumed that $f\colon Y \to X$ is totally split. By the remark following Lemma 5.14, the space X is covered by open sets U above which both $f^{-1}(U) \to U$ and the action of G on $f^{-1}(U)$ are trivial; that is, we can identify $f^{-1}(U)$ with $U \times D$ for some finite set D, such that the action of G on $U \times D$ is induced by an action of G on D. Denote by D/G the set of orbits of D under G. Then it is readily checked that $U \times (D/G)$ is a quotient of $U \times D$ under G in $\mathbf{Aff}_U$, so $U \times (D/G) \cong f^{-1}(U)/G$. Hence $U \times (D/G) \cong g^{-1}(U)$, so $g^{-1}(U) \to U$ is finite étale. This implies that $g\colon Y/G \to X$ is finite étale.

In the general case we choose a surjective, finite and locally free morphism $W \to X$ for which $Y \times_X W \to W$ is totally split. Then $(Y \times_X W)/G \to W$ is finite étale by the result just proved, and $(Y \times_X W)/G \cong (Y/G) \times_X W$ by 5.19. From 5.8 it now follows that $Y/G \to X$ is finite étale. This proves 5.20.

5.21 Proposition. *Let $Y \to X$ be a finite étale morphism, G a finite group of automorphisms of $Y \to X$ in $\mathbf{FEt}_X$, and $Z \to X$ any morphism of schemes. Then $(Y \times_X Z)/G \cong (Y/G) \times_X Z$ in $\mathbf{FEt}_Z$.*

Proof. As in the proof of 5.19 we have a morphism $(Y \times_X Z)/G \to (Y/G) \times_X Z$. We first prove that this is an isomorphism if $Y = X \times D$ for some finite set D, the action of G being induced by an action of G on D. Then $Y \times_X Z \cong Z \times D$, and $(Y \times_X Z)/G$ and $(Y/G) \times_X Z$ are both isomorphic to $Z \times (D/G)$ (cf. the proof of 5.20), as required. Next we consider the case that $Y \to X$ is totally split. Then X can be covered by open sets U above which both $Y \to X$ and the action of G are trivial, as in the proof of 5.20. Hence by the case just dealt with, the morphism $(Y \times_X Z)/G \to (Y/G) \times_X Z$ is locally an isomorphism, so it is an isomorphism.

In the general case we choose a surjective, finite and locally free morphism $W \to X$ for which $Y_W \to W$ is totally split; here we write $-_W$ for $- \times_X W$. Then the above result implies $(Y_W \times_W Z_W)/G \xrightarrow{\sim} (Y_W/G) \times_W Z_W$. Here $Y_W \times_W Z_W \cong (Y \times_X Z) \times_Z W_Z$, where $W_Z = W \times_X Z \to Z$ is surjective, finite and locally free (Exercise 5.5). Hence by 5.19 we have $(Y_W \times_W Z_W)/G \cong ((Y \times_X Z)/G) \times_Z W_Z$. Again by 5.19 we have $Y_W/G \cong (Y/G)_W$, so $(Y_W/G) \times_W Z_W \cong (Y/G)_W \times_W Z_W \cong ((Y/G) \times_X Z) \times_Z W_Z$. We conclude that the morphism $(Y \times_X Z)/G \to (Y/G) \times_X Z$ becomes an isomorphism after $- \times_Z W_Z$. By Exercises 5.9 and 4.25 it follows that it was already an isomorphism. This proves 5.21.

5.22 Finite étale morphisms: verification of the first three axioms. Let X be a scheme. We show that the category $\mathbf{FEt}_X$ of finite étale coverings of X satisfies the axioms G1, G2, G3 of 3.1.

(G1) The identity morphism $X \to X$ is clearly a terminal object in $\mathbf{FEt}_X$. If $Y \to W \leftarrow Z$ are morphisms of finite étale coverings of X, then $Y \times_W Z \to W$ is finite étale by Exercises 5.7(a) and 5.8, and $Y \times_W Z \to X$ is finite étale by Proposition 5.12. Hence fibred products exist in $\mathbf{FEt}_X$.

(G2) If $Y_i \to X$ is finite étale for $1 \leq i \leq n$, then $\coprod_{i=1}^n Y_i \to X$ is finite étale (Exercises 5.3 and 5.8). Hence finite sums exist in $\mathbf{FEt}_X$. In particular, $\emptyset \to X$ is an initial object. By Proposition 5.20, quotients under finite groups of automorphisms exist.

(G3) Let $h\colon Y \to Z$ be a morphism of finite coverings of X. As in the proof of 5.16 we can write $Z = Z_0 \amalg Z_1$, where the subschemes $Z_0 = \{z \in Z : [Y : Z](z) = 0\}$ and $Z_1 = Z - Z_0$ are open and closed in Z. Then $h^{-1}(Z_0) = \emptyset$, and h factors as $Y \to Z_1 \to Z$. Here $Y \to Z_1$ is surjective, hence an epimorphism (Proposition 5.16), and $Z_1 \to Z_0 \amalg Z_1 = Z$ is a monomorphism by Proposition 5.17. This proves that any morphism in $\mathbf{FEt}_X$ is an epimorphism followed by a monomorphism. Further, by Proposition 5.17 any monomorphism is an isomorphism with a direct summand.

5.23 Finite étale morphisms; the fundamental functor. A *geometric point* of a scheme X is a morphism $x\colon \operatorname{Spec}\Omega \to X$, where Ω is an algebraically closed field. Geometric points exist if X is non-empty (Exercise 5.18), in particular if X is connected. Let X be a scheme and $x\colon \operatorname{Spec}\Omega \to X$ a geometric point of X. If $Y \to X$ is finite étale then so is $Y \times_X \operatorname{Spec}\Omega \to \operatorname{Spec}\Omega$, by Exercises 5.5(a) and 5.8. This gives rise to a functor $H_x\colon \mathbf{FEt}_X \to \mathbf{FEt}_{\operatorname{Spec}\Omega}$ with $H_x(Y) = Y \times_X \operatorname{Spec}\Omega$. The absolute Galois group (see 2.4) of Ω is trivial, so by Theorem 2.9 and the remark following that theorem there is an equivalence of categories $J\colon \mathbf{FEt}_{\operatorname{Spec}\Omega} \to \mathbf{sets}$. Let $F_x = J \circ H_x$ denote the composed functor $\mathbf{FEt}_X \to \mathbf{sets}$; see Exercise 5.19 for an explicit description of F_x. We prove that F_x satisfies axioms G4 and G5 of 3.1, and if X

is connected also axiom G6. Since J is an equivalence we may replace F_x by H_x in each of these axioms.

(G4) Clearly, H_x transforms the terminal object $X \to X$ of $\mathbf{FEt}_X$ into the terminal object $\operatorname{Spec}\Omega \to \operatorname{Spec}\Omega$ of $\mathbf{FEt}_{\operatorname{Spec}\Omega}$. Also $H_x = - \times_X \operatorname{Spec}\Omega$ commutes with fibred products, since this is true for any base change.

(G5) Any base change trivially commutes with finite sums, transforms epimorphisms in epimorphisms by Exercise 5.5(c) and Proposition 5.16, and commutes with passage to the quotient by a finite group of automorphisms by Proposition 5.21. This applies in particular to $H_x = - \times_X \operatorname{Spec}\Omega$.

(G6) Let it now be assumed that X is *connected.* Then for any finite étale covering $Y \to X$ the degree $[Y : X]$ is *constant* (see 5.3). By Exercise 5.5(b) we have $[Y : X] = [H_x(Y) : \operatorname{Spec}\Omega]$. Further we see from the proof of Theorem 2.9 that the anti-equivalence ${}_\Omega\mathbf{SAlg} \to \mathbf{sets}$ sends a separable Ω-algebra of rank n over Ω to a set of cardinality n. Combining this we conclude that $\#F_x(Y) = [Y : X]$ for any finite étale covering $Y \to X$.

To prove (G6), let $h\colon Y \to Z$ be a morphism for which $F_x(h)\colon F_x(Y) \to F_x(Z)$ is bijective. We wish to prove that h is an isomorphism. Factor $Y \to Z$ as in the proof of (G3) into $Y \to Z_1 \to Z_0 \amalg Z_1 = Z$, where $Y \to Z_1$ is surjective. Since $F_x(h)$ is an isomorphism and F_x commutes with finite sums, the map $F_x(Z_1) \to F_x(Z) = F_x(Z_0) \amalg F_x(Z_1)$ is surjective. Therefore $F_x(Z_0) = \emptyset$, so $[Z_0 : X] = 0$, and $Z_0 = \emptyset$ by Proposition (5.4)(a). Hence $Z_1 = Z$, and $Y \to Z$ is surjective. Also $[Y : X] = \#F_x(Y) = \#F_x(Z) = [Z : X]$, and from Exercise 5.20 it now follows that $Y \to Z$ is an isomorphism.

5.24 Theorem. *Let X be a connected scheme, x a geometric point of X, and $F_x\colon \mathbf{FEt}_X \to \mathbf{sets}$ as defined in* 5.23. *Then $\mathbf{FEt}_X$ is a Galois category with fundamental functor F_x.*

Proof. This was done in 5.22 and 5.23. This proves 5.24.

5.25 Proof of the Main theorem 1.11. It is straightforward to verify that $\mathbf{FEt}_X$ is an essentially small category for any scheme X. From Theorems 3.5(a) and 5.24 it thus follows that for connected X the category $\mathbf{FEt}_X$ is equivalent to π-**sets** for some profinite group π. The uniqueness of π follows from 3.5(d).

This finishes the proof of the main theorem.

5.26 The fundamental group. For X, x, F_x as in Theorem 5.24 we write $\pi(X, x) = \operatorname{Aut}(F_x)$, the *fundamental group of X in x*, see 3.6. We show that this is a functor on the category $\mathbf{S}$ whose objects are pairs (X, x) with X a connected scheme and x a geometric point of X, a morphism $(X', x') \to (X, x)$ being a morphism $f\colon X' \to X$ of schemes for

which $f \circ x' = x$. If f is such a morphism, then the functor $G = - \times_X X' \colon \mathbf{FEt}_X \to \mathbf{FEt}_{X'}$ satisfies $F_{x'} \circ G \cong F_x$ (canonically), so from Theorems 5.24 and 3.20 we see that a continuous group homomorphism $\pi(X', x') \to \pi(X, x)$ is induced. It follows that $\pi(-,-)$ is a functor from $\mathbf{S}$ to the category of profinite groups.

Exercises for Section 5

5.1 Let X be a scheme and $d \colon X \to \mathbb{Z}$ any continuous function that assumes only non-negative values. Prove that there is a finite and locally free morphism $Y \to X$ such that $d = [Y : X]$.

5.2 Let $Y \to X$ be a finite and locally free morphism. Prove that the underlying map $\mathrm{sp}(Y) \to \mathrm{sp}(X)$ is open and closed.

5.3 Let $Y_i \to X$ be a morphism of schemes, for $1 \leq i \leq n$, and $Y = Y_1 \amalg Y_2 \amalg \cdots \amalg Y_n \to X$ the induced morphism. Prove that $Y \to X$ is finite and locally free if and only if each $Y_i \to X$ is finite and locally free. Prove also that $[Y : X] = \sum_{i=1}^{n} [Y_i : X]$ if $Y \to X$ is finite and locally free.

5.4 Let $(X_i)_{i \in I}$ be a collection of schemes, and $Y_i \to X_i$ a finite and locally free morphism, for each $i \in I$. Prove that the induced morphism $\coprod_{i \in I} Y_i \to \coprod_{i \in I} X_i$ is finite and locally free, and that each finite and locally free morphism $Y \to \coprod_{i \in I} X_i$ is obtained in this way. Prove also that $[\coprod_{i \in I} Y_i : \coprod_{i \in I} X_i]$ equals $[Y_j : X_j]$ when restricted to $\mathrm{sp}(X_j)$, for each $j \in I$.

5.5 Let $Y \to X$ be a finite and locally free morphism of schemes, and let $W \to X$ be any morphism of schemes.

(a) Prove that $Y \times_X W \to W$ is finite and locally free.

(b) Prove that the diagram

$$\begin{array}{ccc} \mathrm{sp}(W) & \longrightarrow & \mathrm{sp}(X) \\ & \searrow \quad \swarrow & \\ & \mathbb{Z} & \end{array}$$

with the left arrow labeled $[Y \times_X W : W]$ and the right arrow labeled $[Y : X]$, is commutative.

(c) Suppose that $Y \to X$ is surjective. Prove that $Y \times_X W \to W$ is surjective.

5.6 Suppose that $Z \to Y$ and $Y \to X$ are finite and locally free morphisms of schemes. Prove that the composed morphism $Z \to X$ is finite and locally free.

5.7 Let $Y \to X$ and $Z \to X$ be finite and locally free morphisms of schemes.

(a) Prove that $Y \times_X Z \to X$ is finite and locally free.

(b) Prove that $[Y \times_X Z : X] = [Y : X] \cdot [Z : X]$.

(c) Prove that $Y \times_X Z \to X$ is surjective if $Y \to X$ and $Z \to X$ are surjective.

5.8 Do Exercises 5.1–5.7 with everywhere "finite and locally free" replaced by "finite étale".

5.9 Prove that a morphism $Y \to X$ is surjective, finite and locally free if and only if for each open affine subset $U = \operatorname{Spec} A$ of X the open subscheme $f^{-1}(U)$ of Y is affine, $f^{-1}(U) = \operatorname{Spec} B$, where B is a faithfully projective A-algebra (see 4.11).

5.10 Let $Y \to X$ be a finite étale morphism of schemes, and let $W \to X$ be the surjective, finite and locally free morphism constructed in the proof of 5.10 for which $Y \times_X W \to W$ is totally split. Prove that $W \to X$ is finite étale, and express $[W : X]$ in terms of $[Y : X]$.

5.11 If E is a finite set and A is a ring, we write A^E for the ring of functions $E \to A$, with pointwise addition and multiplication.

(a) For a scheme X and a finite set E, prove that $X \times E \cong X \times_{\operatorname{Spec}\mathbb{Z}} (\operatorname{Spec}\mathbb{Z}^E)$ (see 5.13 for the definition of $X \times E$).

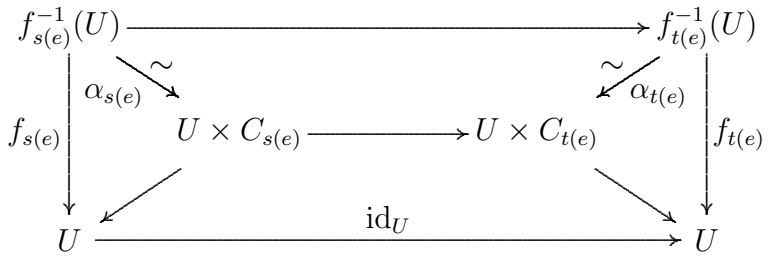
(b) Let X, Y be schemes and E a finite set. Prove that there is a bijection, natural in X, Y and E, from the set $\operatorname{Mor}(X \times E, Y)$ of morphisms $X \times E \to Y$ of schemes to the set of maps $E \to \operatorname{Mor}(X, Y)$.

(c) For a ring A and a finite set E, prove that $(\operatorname{Spec} A) \times E \cong \operatorname{Spec} A^E$.

(d) Suppose that A is a ring that has no non-trivial idempotents, and let E, D be finite sets. Prove that any A-algebra homomorphism $A^E \to A^D$ is induced by a map $D \to E$.

5.12 Let $D = (V, E, s, t)$ be a directed graph as in Exercise 3.1, and suppose that V and E are *finite*. Let further X be a scheme, and let a D-diagram in the category of totally split schemes over X be given; more precisely, let for each $v \in V$ a totally split morphism $f_v \colon Y_v \to X$ be given, and for each $a \in E$ a morphism $h_e \colon Y_{s(E)} \to Y_{t(e)}$ with $f_{t(e)} h_e = f_{s(e)}$. Prove that any $x \in X$ has an open affine neighborhood U such that the diagram is trivial above U, in the sense that there exist finite sets C_v, for $v \in V$, maps $\phi_e \colon C_{s(e)} \to C_{t(e)}$, for $e \in E$, and isomorphisms $\alpha_v \colon f_v^{-1}(U) \xrightarrow{\sim} U \times C_v$ such that for

each $e \in E$ the diagram



is commutative; here $U \times C_{s(e)} \to U$, $U \times C_{t(e)} \to U$ are the first projections, and $U \times C_{s(e)} \to U \times C_{t(e)}$ is the morphism induced by ϕ_e.

5.13 Let $Y \to Z \to X$ be morphisms of schemes such that $Z \to X$ and the composed morphism $Y \to X$ are affine. Prove that $Y \to Z$ is affine.

5.14 Prove that an open immersion is a monomorphism in the category of all schemes.

5.15 Let $f\colon Y \to X$, $g\colon Z \to X$ be finite étale and $h\colon Y \to Z$ a morphism with $f = gh$. Prove:

(a) h is an epimorphism in $\mathbf{FEt}_X$ if and only if $[Y : Z] \geq 1$;

(b) h is a monomorphism in $\mathbf{FEt}_X$ if and only if $[Y : Z] \leq 1$;

(c) h is an isomorphism if and only if it is both an epimorphism and a monomorphism in $\mathbf{FEt}_X$.

5.16 Let X be a connected scheme, and let $Y \to X$ be finite étale. Prove that $Y \to X$ is a connected object of the category $\mathbf{FEt}_X$, in the sense of 3.12, if and only if $\mathrm{sp}(Y)$ is a connected topological space.

5.17 Let $Y \to X$ be an affine morphism, and G a finite group of automorphisms of $Y \to X$ in $\mathbf{Aff}_X$, as in 5.18. Prove that $\mathrm{sp}(Y/G)$ is homeomorphic to the orbit space $\mathrm{sp}(Y)/G$ with the quotient topology.

5.18 Let X be a scheme. Show that giving a geometric point of X is equivalent to giving a point $y \in X$ together with a field homomorphism $k(y) \to \Omega$ from the residue field at y to an algebraically closed field Ω.

5.19 Let X be a scheme and x a geometric point of X. Show that the functor $F_x\colon \mathbf{FEt}_X \to \mathbf{sets}$ defined in 5.23 is naturally equivalent to the functor that sends a covering $f\colon Y \to X$ to the set $\{y\colon \operatorname{Spec}\Omega \to Y : fy = x\}$. [*Hint:* use the explicit description of the anti-equivalence ${}_\Omega\mathbf{SAlg} \to \mathbf{sets}$ from the proof of 2.9.]

5.20 Let $f\colon Y \to X$, $g\colon Z \to X$ be finite étale with $[Y : X] = [Z : X]$, and suppose that $h\colon Y \to Z$ is a surjective morphism with $f = gh$. Prove that h is an isomorphism. [*Hint:* apply 5.14 if f and g are totally split, and make a surjective, finite and locally free base change in the general case.]

5.21 Let $f\colon Y \to X$ be finite étale with X *connected.* Prove that $W \to X$ in 5.10 can be chosen to be finite étale and *connected*, of degree dividing $[Y : X]!$.

5.22 Let X be a scheme, with underlying topological space $\operatorname{sp} X$.

(a) Denote by $\mathbf{C}$ the category of all morphisms $f\colon Y \to X$ that are locally totally split, i.e., for which every $x \in X$ has an open neighborhood U such that $f^{-1}(U) \to U$ is totally split (5.9). Prove that $\mathbf{C}$ is equivalent to the category of finite coverings of $\operatorname{sp} X$.

(b) Suppose that X is connected, and let $\hat{\pi}(\operatorname{sp} X)$ be as in 1.15. Prove that there is a continuous surjective group homomorphism $\pi(X) \to \hat{\pi}(\operatorname{sp} X)$.

5.23 Let X be an irreducible scheme. Prove that every morphism $f\colon Y \to X$ of schemes that is locally totally split (Exercise 5.22(a)) is totally split.

6 Complements

In the preceding sections we studied *finite étale* morphisms, but the notion of an étale morphism has not even been defined. We shall give this definition in the present section, and we shall prove, for locally noetherian X, that a morphism $Y \to X$ is finite étale if and only if it is finite and étale. For general X something stronger than *finite* is needed, see 6.4.

To define étale morphisms we have to define *flat* morphisms and *unramified* morphisms. We only treat those properties of these notions that we need. For a more systematic treatment of flat morphisms, unramified morphisms and étale morphisms we refer to [9; 20].

Similarly, we considered *projective separable* algebras, but a *separable* algebra has not been defined. We give the definition in 6.10, and we prove that an algebra is projective separable if and only if it is projective as a module and separable. For more information on separable algebras, even non-commutative ones, we refer to [7].

In Theorem 6.13 we describe the finite étale coverings of a normal integral scheme. This is applied to the calculation of $\pi(X)$, where $X = \operatorname{Spec} A$ for a Dedekind domain A or $X = \mathbb{P}^1_K$ or $\mathbb{A}^1_K$ for a field K.

For more techniques to calculate the fundamental group we refer to [9] and [22]. A particularly lucid exposition, without proofs, is found in [20, Chapter I, Section 5].

6.1 Flat morphisms. A ring homomorphism $f\colon A \to B$ is called *flat* if B is flat (see 4.3) when regarded as an A-module via f. A morphism $f\colon Y \to X$ of schemes is called *flat* if for every $y \in Y$ the induced ring homomorphism $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.

6.2 Proposition. *Let $f\colon A \to B$ be a ring homomorphism. Then the following four assertions are equivalent:*

(i) *f is flat;*
(ii) *for every prime ideal $\mathfrak{q}$ of B the induced map $A_{f^{-1}[\mathfrak{q}]} \to B_{\mathfrak{q}}$ is flat;*
(iii) *the induced morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ is flat;*
(iv) *for every maximal ideal $\mathfrak{n}$ of B the induced map $A_{f^{-1}[\mathfrak{n}]} \to B_{\mathfrak{n}}$ is flat.*

Proof. (i)⇒(ii) Let $\mathfrak{q} \subset B$ be a prime ideal, $\mathfrak{p} = f^{-1}[\mathfrak{q}] \subset A$ and $S = A - \mathfrak{p}$. If $A \to B$ is flat, then so is $A_{\mathfrak{p}} = S^{-1}A \to S^{-1}B$, by [1, 2.20], and since $S^{-1}B \to B_{\mathfrak{q}}$ is flat [1, 3.6], this shows that (i) implies (ii).

(ii)⇒(iii) This is true by definition.

(ii)⇒(iv) Obvious.

(iv)⇒(i) To prove that $A \to B$ is flat it suffices to prove that for any injective map $M \to N$ of A-modules the induced map $M \otimes_A B \to N \otimes_A B$ is injective [1, 2.19]. So let

$M \to N$ be injective. Then for any maximal ideal $\mathfrak{n}$ of B the map $M \otimes_A A_{f^{-1}[\mathfrak{n}]} \to N \otimes_A A_{f^{-1}[\mathfrak{n}]}$ is injective by flatness of $A \to A_{f^{-1}[\mathfrak{n}]}$. By (iv) it follows that $M \otimes_A B_{\mathfrak{n}} \to N \otimes_A B_{\mathfrak{n}}$ is injective for any $\mathfrak{n}$. Since $B \to B_{\mathfrak{n}}$ is flat, this implies that the kernel K of $M \otimes_A B \to N \otimes_A B$ satisfies $K \otimes_B B_{\mathfrak{n}} = 0$ for all maximal ideals $\mathfrak{n}$ of B. Therefore $K = 0$, as required.

This proves 6.2.

6.3 Proposition. *Let $f\colon Y \to X$ be a morphism of schemes. Then the following four assertions are equivalent:*

(i) *f is flat;*

(ii) *for any pair of open affine subsets $V = \operatorname{Spec} B \subset Y$, $U = \operatorname{Spec} A \subset X$ with $f[V] \subset U$ the induced ring homomorphism $A \to B$ is flat;*

(iii) *there is a covering of Y by open affine subsets $V_i = \operatorname{Spec} B_i$ such that for each i there is an open affine subset $U_i = \operatorname{Spec} A_i \subset X$ with $f[V_i] \subset U_i$ for which the induced ring homomorphism $A_i \to B_i$ is flat;*

(iv) *for every closed point $y \in Y$ the induced ring homomorphism $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.*

Proof. This is a straightforward consequence of 6.2. We leave the proof to the reader.

6.4 Finitely presented morphisms. Let $f\colon Y \to X$ be a morphism of schemes. We recall [10, Chapter II, Section 3] that f is called *finite* if there exists a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$ such that for each i the open subscheme $f^{-1}(U_i)$ of Y is affine, $f^{-1}(U_i) = \operatorname{Spec} B_i$, where B_i is an A_i-algebra that is finitely generated as an A_i-module. Replacing "finitely generated" by "finitely presented" (see 4.6) we obtain the definition of a *finitely presented morphism*; see Exercise 6.3 for an equivalent definition.

Over a noetherian ring, every finitely generated module is finitely presented. Hence if X is locally noetherian, "finitely presented" is the same as "finite".

Warning. Since in most of the literature on the subject all schemes are supposed to be locally noetherian, the above terminology is not commonly used, and if it is used it does not necessarily refer to the same notion.

We shall prove that, for finitely presented morphisms, "flat" is equivalent to "locally free". We need a lemma.

6.5 Lemma. *Let P be a module over a ring A. Then P is finitely generated and projective if and only if P is finitely presented and flat.*

Proof. The "only if"-part we know from Section 4 (see 4.6(ii) and 4.3). To prove the "if"-part, let first P be a finitely presented A-module and M a flat A-module, and write

$P^* = \mathrm{Hom}_A(P, A)$. We claim that the map

$$\phi\colon P^* \otimes_A M \to \mathrm{Hom}_A(P, M)$$

defined in 4.8 by $\phi(f \otimes m)(p) = f(p)m$, is an isomorphism. If $P = A^n$ for some $n < \infty$ this is clear, as in 4.8. In the general case one chooses an exact sequence

$$A^m \to A^n \to P \to 0$$

with $m, n < \infty$, and one considers the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & P^* \otimes_A M & \longrightarrow & A^{n*} \otimes_A M & \longrightarrow & A^{m*} \otimes_A M \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_A(P, M) & \longrightarrow & \mathrm{Hom}_A(A^n, M) & \longrightarrow & \mathrm{Hom}_A(A^m, M). \end{array}$$

The first row is exact since the functor $-^* = \mathrm{Hom}(-, A)$ is left exact and M is flat, and the second row is exact since $\mathrm{Hom}(-, M)$ is left exact. We have just seen that the last two vertical arrows are isomorphisms. Hence the remaining vertical arrow is also an isomorphism. This proves our claim.

Let now P be finitely presented and flat. Applying the above result to $M = P$ we find an element

$$\sum_{i=1}^{t} f_i \otimes p_i \in P^* \otimes_A P$$

such that $\phi\left(\sum_{i=1}^{t} f_i \otimes p_i\right) = \mathrm{id}_P$, i.e.,

$$\sum_{i=1}^{t} f_i(x)p_i = x \quad \text{for all} \quad x \in P.$$

Hence the A-linear maps

$$\begin{aligned} f\colon P \to A^t, &\quad f(x) = (f_i(x))_{i=1}^t, \\ g\colon A^t \to P, &\quad g((a_i)_{i=1}^t) = \sum_{i=1}^{t} a_i p_i \end{aligned}$$

satisfy $gf = \mathrm{id}_P$, so g is surjective and the sequence $0 \to \ker g \to A^t \to P \to 0$ splits. Therefore P is finitely generated projective. This proves 6.5.

Remark. Finitely generated flat modules need not be projective: see Exercise 6.5(b).

6.6 Proposition. *Let $f\colon Y \to X$ be a morphism of schemes. Then f is finite and locally free if and only if it is finitely presented (as in* 6.4*) and flat.*

Proof. This is clear from Proposition 5.2, Exercise 6.3 and Lemma 6.5. This proves 6.6.

6.7 Unramified morphisms. Let $f\colon Y \to X$ be a morphism that is locally of finite type [10, Chapter II, Section 3], and $y \in Y$. The morphism f is said to be *unramified at y* if $\mathcal{O}_{Y,y}/\mathfrak{m}_x\mathcal{O}_{Y,y}$ is a finite separable field extension of $\mathcal{O}_{X,x}/\mathfrak{m}_x$, where $x = f(y) \in X$. See Exercise 6.6 for a reformulation of this definition for affine schemes, and Exercise 6.7 for the relation to number theory.

A morphism $f\colon Y \to X$ is said to be *unramified* if it is locally of finite type and unramified at all $y \in Y$.

6.8 Étale morphisms. A morphism $f\colon Y \to X$ is said to be *étale* if it is flat and unramified.

6.9 Proposition. *A morphism $f\colon Y \to X$ of schemes is finite étale (see* 1.4*) if and only if it is finitely presented (see* 6.4*) and étale (see* 6.8*).*

Remark. It follows that, for X locally noetherian, finite étale is equivalent to finite and étale. This is not true in general, see Exercise 6.8.

Proof of 6.9. By 6.6, finitely presented and étale is equivalent to finite and locally free and unramified. Since finite étale morphisms are also finite and locally free, and all notions are local on X, it suffices to prove the following assertion. Let B be an algebra over a ring A, and suppose that B is finitely generated and free as an A-module. Then B is separable over A (see 1.2) if and only if $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified.

First we reduce the problem to the case that A is a field. By definition, B is separable over A if and only if the map $\phi\colon B \to \operatorname{Hom}_A(B, A)$ defined in 1.2 is an isomorphism. Using Exercises 4.36 and 6.9 one sees that this is the case if and only if for each $\mathfrak{p} \in \operatorname{Spec} A$ the analogously defined map $B \otimes_A k(\mathfrak{p}) \to \operatorname{Hom}_{k(\mathfrak{p})}(B \otimes_A k(\mathfrak{p}), k(\mathfrak{p}))$ is an isomorphism, where $k(\mathfrak{p})$ denotes the residue class field of $\mathfrak{p}$; in other words, if and only if $B \otimes_A k(\mathfrak{p})$ is separable over $k(\mathfrak{p})$ for every $\mathfrak{p} \in \operatorname{Spec} A$.

Likewise, it is straightforward to see from the definition that $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified if and only if $\operatorname{Spec} B \otimes_A k(\mathfrak{p}) \to \operatorname{Spec} k(\mathfrak{p})$ is unramified for every $\mathfrak{p} \in \operatorname{Spec} A$. Thus the problem has now been reduced to the case that A is a field.

Let A be a field. Then we can write $B = \prod_{i=1}^{t} B_i$, where each B_i is a local ring with a nilpotent maximal ideal (Theorem 2.6). It is easy to see that the B_i are in fact the localizations of B at all $\mathfrak{q} \in \operatorname{Spec} B$. Hence from 6.7 we see that $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified if

and only if each B_i is a finite separable field extension of A. By 2.7, this is equivalent to B being separable over A, as required.

This proves 6.9.

The above proposition shows that our notion of "finite étale" agrees with the one found in the literature [20].

6.10 Separable algebras. Let A be a ring and B an A-algebra. The ring homomorphism $B \otimes_A B \to B$ sending $x \otimes y$ to xy makes B into a $B \otimes_A B$-algebra and hence into a $B \otimes_A B$-module. The A-algebra B is said to be *separable* if B is projective as a $B \otimes_A B$-module.

6.11 Proposition. *Let B be an algebra over a ring A. Then B is projective separable (see* 4.13*) over A if and only if B is projective as an A-module and separable as an A-algebra (see* 6.10*).*

Proof. "Only if". Let B be projective separable over A . Then B is projective as an A-module by definition. Further, the isomorphism $B \otimes_A B \cong B \times C$ from 4.16 shows that B is projective as a $B \otimes_A B$-module, so separable as an A-algebra.

"If". Assume that B is projective as an A-module and separable as an A-algebra. First we show that B is *finitely generated* as an A-module.

Since B is projective over $B \otimes_A B$, there is a $B \otimes_A B$-linear map $f\colon B \to B \otimes_A B$ for which the composed map $B \to B \otimes_A B \to B$ is the identity on B. Let $e = f(1)$. Writing e as a finite sum of elements of the form $x \otimes y$, with $x, y \in B$, we see that there exists a finitely generated sub-A-module N of B such that $e \in \text{image}(N \otimes N \to B \otimes B)$.

Because B is projective as an A-module we can embed B as a direct summand in a free A-module F. Then $B \otimes B$ is a direct summand of $F \otimes F$. Since N is finitely generated, we can select a finitely generated free direct summand M of F with $N \subset M$. Then e, considered as an element of $F \otimes F$, belongs to $M \otimes M$; we show that in fact the whole image of f is contained in $M \otimes M$.

Let $b \in B$. Then $f(b) = f((b \otimes 1) \cdot 1) = (b \otimes 1) \cdot e \in (B \otimes 1) \cdot \text{image}(N \otimes N \to B \otimes B) = \text{image}(B \otimes N \to B \otimes B) \subset F \otimes M$. Similarly we have $f(b) \in M \otimes F$. But M is a direct summand of F, so $f(b) \in (F \otimes M) \cap (M \otimes F) = M \otimes M$.

This proves that $f[B] \subset M \otimes M$. It follows that the composite of the natural maps $M \otimes M \to F \otimes F \to B \otimes B \to B$ is *surjective*. Since $M \otimes M$ is finitely generated as an A-module this implies that B is finitely generated as well.

To finish the proof of 6.11 we must now show that B is separable over A in the sense of 4.13. We briefly indicate two different ways of doing this, leaving the details to the reader.

As in the proof of 6.9 we may assume that A is a field, using Exercise 6.11. Next, using Theorem 2.7, we may assume that A is algebraically closed and, using Theorem 2.6 and Exercise 6.12, that B is a local ring. Then $B \otimes_A B$ is also a local ring (Exercise 6.13), so the projective $B \otimes_A B$-module B is free (Proposition 4.5). Calculating dimensions over A one finds that $B = A$, as required.

The second method follows the lines of the proof of Theorem 5.10. First one reduces the problem to the case that B has constant rank (cf. Exercise 4.24) and one argues by induction on the rank. The hypothesis that B is $B \otimes_A B$-projective leads to a splitting $B \otimes_A B = B \times C$ as in Proposition 4.16, where C is a separable B-algebra (by Exercises 6.11, 6.12). By the induction hypothesis, C is a projective separable B-algebra, so the same is true for $B \otimes_A B$. One can now apply 4.14 to conclude the proof.

This proves 6.11.

Proposition 6.11 shows that our terminology agrees with the terminology used in the literature [7].

6.12 Normal integral schemes. Recall that a scheme is *normal* if all of its local rings are integrally closed domains.

Let X be a normal integral scheme. We shall describe all finite étale coverings $Y \to X$ of X. Any such Y can be written, in a unique way, as the disjoint union of finitely many *connected* schemes Y_i, where each $Y_i \to X$ is finite étale (see 3.12 and Exercise 5.16). It will therefore suffice to describe all finite étale coverings $Y \to X$ that are connected.

Denote by K the function field of X [10, Chapter II, Exercise 3.6]. Then $\mathcal{O}_X(U)$ may be considered as a subring of K, for every nonempty open set $U \subset X$. Let L be a finite separable field extension of K. For an open set $U \subset X$, $U \neq \emptyset$, let $\mathcal{A}(U)$ be the integral closure of $\mathcal{O}_X(U)$ in L and $\mathcal{A}(\emptyset) = \{0\}$. It is readily verified that $\mathcal{A}$ is a quasi-coherent sheaf of $\mathcal{O}_X$-algebras. By [10, Chapter II, Exercise 5.17] it therefore gives rise to an affine morphism $Y \to X$ with $Y = \operatorname{Spec} \mathcal{A}$. The scheme Y is called the *normalization* of X in L. We say that X is *unramified* in L if $Y \to X$ is unramified (see 6.7).

6.13 Theorem. *Let X be a normal integral scheme with function field K, and let L be a finite separable field extension of K such that X is unramified in L. Then the normalization of X in L is a connected finite étale covering of X. Moreover every connected finite étale covering of X arises in this way.*

Proof. We first prove the last statement of the theorem, asserting that every connected finite étale covering of X arises in the way described. We begin with a lemma concerning the affine situation.

6.14 Lemma. *Let A be a domain that is integrally closed inside its field of fractions K, and let B be a projective separable A-algebra. Then there are finite separable field extensions $L_1, L_2, \ldots, L_t$ of K such that there is an isomorphism $B \otimes_A K \cong \prod_{i=1}^t L_i$ of K-algebras. Moreover, this isomorphism induces an isomorphism $B \cong \prod_{i=1}^t B_i$, where B_i denotes the integral closure of A in L_i.*

Proof. Since $B \otimes_A K$ is a separable K-algebra, Theorem 2.7 implies that $B \otimes_A K \cong \prod_{i=1}^t L_i$ with $K \subset L_i$ a finite separable field extension for $1 \leq i \leq t$. The map $B \to B \otimes_A K$ is injective, because $A \to K$ is injective and B is flat over A. Hence B may be considered as a subring of $\prod_{i=1}^t L_i$. Since B is finitely generated as an A-module it is integral over A, so $B \subset \prod_{i=1}^t B_i$, with B_i as in the lemma. To prove that equality holds, let $x \in \prod_{i=1}^t B_i$. Then for each $y \in B$ we have $xy \in \prod_{i=1}^t B_i$, and since A is integrally closed this implies, by Exercises 6.17 and 6.18, that $\mathrm{Tr}(xy) \in A$, where $\mathrm{Tr} = \mathrm{Tr}_{B \otimes K/K}$. The map $B \to A$ sending y to $\mathrm{Tr}(xy)$ is A-linear, so by the definition of separability (see 4.13) there exists $x' \in B$ with $\mathrm{Tr}(xy) = \mathrm{Tr}_{B/A}(x'y)$ for all $y \in B$. Then $\mathrm{Tr}(xy) = \mathrm{Tr}(x'y)$ for all $y \in B \otimes_A K$, by K-linearity, and since $B \otimes_A K$ is separable over K this implies that $x = x' \in B$, as required. This proves 6.14.

Continuing the proof of Theorem 6.13, let X be a normal integral scheme with function field K, and $f\colon Y \to X$ a connected finite étale covering. Let $U = \operatorname{Spec} A$ be an open non-empty affine subset of X, and $f^{-1}(U) = \operatorname{Spec} B \subset Y$. Then the conditions of 6.14 are satisfied, so B is a product of finitely many domains. Consequently $f^{-1}(U)$ is the union of open irreducible subsets [10, Chapter II, Proposition 3.1], and all local rings of $f^{-1}(U)$ are domains. Taking the union over U we see that the same two statements are valid for Y. By Exercise 6.14 we can write Y as the *disjoint* union of open irreducible subsets; but Y is connected, so it must itself be irreducible. Its local rings are domains, so by [10, Chapter II, Proposition 3.1] the scheme Y is integral. Let L be its function field. To prove that Y is the normalization of X in L it suffices to prove, for any non-empty open affine subset $U = \operatorname{Spec} A$ of X, that $f^{-1}(U) = \operatorname{Spec} B$, where B is the integral closure of A in L; but this is immediate from Lemma 6.14, with $t = 1$. Finally, X is unramified in L by 6.9. This proves the last statement of 6.13.

Before proving the first statement of 6.13 we treat two lemmas.

6.15 Proposition. *Let C be a separable algebra of rank n over a field K, with $\#K \geq n$. Then there exists $\gamma \in C$ with $C = K[\gamma]$.*

Proof. By 2.7(iv) we can write $C = \prod_{i=1}^t C_i$, where each C_i is a finite separable field extension of K. We proceed by induction on t, the case $t = 0$ being trivial. For $t > 0$, we have

$C = C' \times C_t$, where $C' = \prod_{i=1}^{t-1} C_i$ can be written as $C' = K[\gamma']$. Then $C' \cong K[X]/gK[X]$ for some polynomial $g \in K[X]$ with $\deg g = [C' : K] = n - [C_t : K] < n$. By the theorem of the primitive element we can write $C_t = K[\alpha]$. Using that $\#K \geq n$ we can choose $a \in K$ with $g(a + \alpha) \neq 0$. Then the irreducible polynomial f of $a + \alpha$ over K is relatively prime to g, so the kernel of the K-algebra homomorphism $K[X] \to C$ mapping X to $\gamma = (\gamma', a + \alpha) \in C' \times C_t = C$ is generated by $f \cdot g$. Comparing dimensions we see that the map is surjective, so $K[\gamma] = C$. This proves 6.15.

Exercise 6.19 shows that the bound in 6.15 is sharp.

6.16 Lemma. *Let A be a local domain that is integrally closed in its field of fractions K. Denote the maximal ideal of A by $\mathfrak{m}$. Let L be a finite separable field extension of K, and assume that the integral closure B of A in L is finitely generated as an A-module. Assume furthermore that $B/\mathfrak{m}B$ is a separable $A/\mathfrak{m}$-algebra. Then B is free of rank $[L : K]$ as an A-module.*

Proof. Write $n = [B/\mathfrak{m}B : A/\mathfrak{m}]$. We begin by proving $n \leq [L : K]$. To do this, we first assume $\#A/\mathfrak{m} \geq n$. Then 6.15, applied to $C = B/\mathfrak{m}B$, implies $B/\mathfrak{m}B = (A/\mathfrak{m})[\beta \bmod \mathfrak{m}B]$ for some $\beta \in B$. Since A is integrally closed in K, the irreducible polynomial of β over K belongs to $A[X]$, and it has degree $\leq [L : K]$. Therefore $(\beta \bmod \mathfrak{m}B)$ is a zero of a polynomial in $(A/\mathfrak{m})[X]$ with leading coefficient 1 and degree $\leq [L : K]$. It follows that one has $[B/\mathfrak{m}B : A/\mathfrak{m}] \leq [L : K]$.

Next we assume $\#A/\mathfrak{m} < n$. Choose a positive integer t with $(\#A/\mathfrak{m})^t \geq n$ and $\gcd(t, [L : K]) = 1$. Since $A/\mathfrak{m}$ is finite, there exist irreducible polynomials of every degree in $(A/\mathfrak{m})[X]$, so we can choose a polynomial $f \in A[X]$ with leading coefficient 1 and degree t such that $(f \bmod \mathfrak{m}[X]) \in (A/\mathfrak{m})[X]$ is irreducible. Put $A' = A[X]/fA[X]$. Then A' is free of rank t as an A-module, and $A'/\mathfrak{m}A'$ is the finite field of cardinality $(\#A/\mathfrak{m})^t$, so A' is local and $\operatorname{Spec} A' \to \operatorname{Spec} A$ is unramified at $\mathfrak{m}$. From Exercise 6.10 we now see that A' is a projective separable A-algebra. (This also follows from Exercise 1.6(b).) Since f is irreducible in $A[X]$ it is irreducible in $K[X]$, so $K' = A' \otimes_A K = K[X]/fK[X]$ is a field. From 6.14 it follows that A' is the integral closure of A in K'. Put $B' = A' \otimes_A B$ and $L' = A' \otimes_A L \cong L[X]/fL[X]$. The condition $\gcd(t, [L : K]) = 1$ implies that f is irreducible in $L[X]$, so L' is a field. Since B' is a projective separable B-algebra (Exercise 4.47) it is the integral closure of B in L' (Lemma 6.14). It is therefore also the integral closure of A' in L'. We have now proved that $A', K', \mathfrak{m}A', L', B'$ satisfy the conditions of 6.16, and in addition we have

$$\#A'/\mathfrak{m}A' \geq n = [B/\mathfrak{m}B : A/\mathfrak{m}] = [A' \otimes_A (B/\mathfrak{m}B) : A' \otimes_A (A/\mathfrak{m})] = [B'/\mathfrak{m}B' : A'/\mathfrak{m}A'].$$

Hence by the first part of the proof we have $n \leq [L' : K'] = [L : K]$, as required.

Let $\beta_1, \beta_2, \ldots, \beta_n \in B$ be such that the $(\beta_i \bmod \mathfrak{m}B)$ span $B/\mathfrak{m}B$ as an $A/\mathfrak{m}$-vector space. Then by Nakayama's lemma the β_i span B as an A-module, since B is supposed to be a finitely generated A-module. It follows that $\beta_1, \beta_2, \ldots, \beta_n$ span L as a K-vector space (Exercise 6.20). But $n \leq [L : K]$, so we must have $n = [L : K]$, and $\beta_1, \beta_2, \ldots, \beta_n$ are linearly independent over K. We conclude that B is free of rank $[L : K]$ over A, as required. This proves 6.16.

To prove 6.13, let X be a normal integral scheme, K its function field, L a finite separable field extension of K, and Y the normalization of X in L. Suppose that the morphism $f\colon Y \to X$ is unramified. We claim that f is finite étale and that Y is connected.

Let $U = \operatorname{Spec} A$ be an open affine subset of X. Then $f^{-1}(U) = \operatorname{Spec} B$, where B is the integral closure of A in L. The map $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective [1, Theorem 5.10], and Exercise 6.21 now implies that Y is connected.

Next we prove that $Y \to X$ is finite. If X is locally noetherian this is true for the normalization of X in any finite separable field extension of K, see Exercise 6.22. In the general case we use that $Y \to X$ is unramified and hence locally of finite type, as follows. Since $Y \to X$ is affine, it is quasi-compact [10, Chapter II, Exercises 3.2 and 5.17(b)], and since it is also locally of finite type it is actually of finite type [10, Chapter II, Exercise 3.3(a)]. Hence if A and B are as above, B is a finitely generated A-algebra [10, Chapter II, Exercises 3.3(c)] and since B is integral over A it must be a finitely generated A-module (Exercise 6.23). This proves that $Y \to X$ is finite.

To prove that $Y \to X$ is finite étale it suffices, by Propositions 6.6 and 6.9, to show that B is projective as an A-module, with A and B still as above. Lemma 6.16 implies that $B_{\mathfrak{p}}$ is projective of rank $[L : K]$ as an $A_{\mathfrak{p}}$-module, for every $\mathfrak{p} \in \operatorname{Spec} A$. From Exercise 4.27 it thus follows that B is projective over A, as required.

This completes the proof of Theorem 6.13.

6.17 Corollary. *Let X be a normal integral scheme, K its function field, $\overline{K}$ an algebraic closure of K, and M the composite of all finite separable field extensions L of K with $L \subset \overline{K}$ for which X is unramified in L. Then the fundamental group $\pi(X)$ is isomorphic to the Galois group* $\operatorname{Gal}(M/K)$.

Proof. We note that $K \subset M$ is Galois, so that it makes sense to speak about $\operatorname{Gal}(M/K)$.

The natural morphism $\operatorname{Spec} K \to X$ induces a functor $G\colon \mathbf{FEt}_X \to \mathbf{FEt}_{\operatorname{Spec} K}$, by $G(Y) = Y \times_X \operatorname{Spec} K$. One readily checks that, if L is as in Theorem 6.13, this functor sends the normalization of X in L to $\operatorname{Spec} L$. Theorem 6.13 therefore implies that the image of G is contained in the full subcategory of $\mathbf{FEt}_{\operatorname{Spec} K}$ whose objects are of the form $\operatorname{Spec} B$, where

B is a finite dimensional K-algebra that is split by M (see Exercises 2.25 and 2.29). This category is equivalent to $\mathrm{Gal}(M/K)$-sets, by Exercise 2.29. By Theorem 3.20, the functor G induces a continuous group homomorphism $\mathrm{Gal}(M/K) \to \pi(X)$.

By Theorem 6.13, the functor G sends connected objects to connected objects, so by Exercise 3.23(a) the map $\mathrm{Gal}(M/K) \to \pi(X)$ is surjective. To prove that it is injective we use the criterion of Exercise 3.23(b). Let X' be a connected object of the subcategory of $\mathbf{FEt}_{\mathrm{Spec}\, K}$ described above. Then $X' = \mathrm{Spec}\, L$ for some finite field extension L of K contained in M, so there are finite field extensions $L_1, L_2, \ldots, L_t$ of K contained in M such that X is unramified in each L_i and such that L is contained in the composite field extension $L_1 \cdot L_2 \cdot \ldots \cdot L_t$. Denote by Y_i the normalization of X in L_i. Then $Y = Y_1 \times Y_2 \times \cdots \times Y_t$ belongs to $\mathbf{FEt}_X$, and one has $G(Y) = \mathrm{Spec}\,(L_1 \otimes_K L_2 \otimes_K \ldots \otimes_K L_t)$. The natural surjective map $L_1 \otimes_K L_2 \otimes_K \ldots \otimes_K L_t \to L_1 \cdot L_2 \cdot \ldots \cdot L_t$ sending $x_1 \otimes x_2 \otimes \ldots \otimes x_t$ to $x_1 x_2 \ldots x_t$ shows that $\mathrm{Spec}(L_1 \cdot L_2 \cdot \ldots \cdot L_t)$ is a connected component of $G(Y)$, and the inclusion $L \subset L_1 \cdot L_2 \cdot \ldots \cdot L_t$ yields a morphism $\mathrm{Spec}(L_1 \cdot L_2 \cdot \ldots \cdot L_t) \to \mathrm{Spec}\, L$ in $\mathbf{FEt}_{\mathrm{Spec}\, K}$. Hence the condition of Exercise 2.23(b) is satisfied, and $\mathrm{Gal}(M/K) \to \pi(X)$ is injective.

We have proved that the map $\mathrm{Gal}(M/K) \to \pi(X)$ is bijective, so it is an isomorphism of profinite groups (see 1.8). This proves 6.17.

6.18 Dimension one. We apply 6.13 and 6.17 to the case that the normal integral scheme X is *locally noetherian of dimension one.* Then for each closed point $x \in X$ the local ring $\mathcal{O}_{X,x}$ is a discrete valuation ring [1, Theorem 9.3]. In this situation the proof of 6.13 becomes much simpler (Exercise 6.22); in particular, Lemma 6.16 can be dispensed with. The field M in 6.17 is the largest extension of K within a fixed separable closure of K in which all valuations induced by the closed points $x \in X$ are unramified, see Exercises 6.7 and 6.26.

Many examples given in 1.12 are of the above type. If $X = \mathrm{Spec}\, \mathbb{Z}_p$ for some prime number p, then $K = \mathbb{Q}_p$, and M is the maximal unramified extension of K. It is well known that $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$ (cf. [26, Section 3-2]), so 6.17 implies that $\pi(\mathrm{Spec}\, \mathbb{Z}_p) \cong \hat{\mathbb{Z}}$. If $X = \mathrm{Spec}\, A[1/a]$, where A is the ring of algebraic integers in an algebraic number field K, and $a \in A$, $a \neq 0$, then the closed points $x \in X$ are in one-to-one correspondence with the non-zero prime ideals of A that do not divide a. The field M is the maximal algebraic extension of K that is unramified at these primes. This yields the description $\pi(\mathrm{Spec}\, A[1/a]) \cong \mathrm{Gal}(M/K)$ announced in 1.12. From Theorem 6.13 and Exercise 6.25 we also see that the finite étale coverings $Y \to \mathrm{Spec}\, A[1/a]$ are precisely given by $Y = \coprod_{i=1}^{t} \mathrm{Spec}\, B_i$, where $t \geq 0$ and where for each i the ring B_i is the integral closure of $A[1/a]$ in a finite extension K_i of K that is contained in M.

In particular we can take $A = \mathbb{Z}$, $a = 1$, so that $X = \mathrm{Spec}\, \mathbb{Z}$. Minkowski's theorem that

the discriminant of any algebraic number field $L \neq \mathbb{Q}$ exceeds 1 in absolute value implies that any such L ramifies at some prime number. Therefore $M = \mathbb{Q}$, and $\pi(\operatorname{Spec} \mathbb{Z})$ is trivial.

6.19 Valuations on $K(t)$. Let K be a field. The examples $X = \mathbb{P}^1_K$ and $X = \mathbb{A}^1_K$ given in 1.16 are also of the type described in 6.18. To treat these we need some facts on algebraic function fields of one variable, which may be found in [6].

Let t be transcendental over K. For every irreducible polynomial $f \in K[t]$ with leading coefficient 1, the map $v_f \colon K(t)^* \to \mathbb{Z}$ defined by $v_f(f^n g/h) = n$, for $n \in \mathbb{Z}$, $g, h \in K[t] - fK[t]$, is an exponential valuation on $K(t)$ that is trivial on K. The same is true for the map $v_\infty \colon K(t)^* \to \mathbb{Z}$ defined by $v_\infty(g/h) = \deg h - \deg g$, for $g, h \in K[t] - \{0\}$. Every non-trivial exponential valuation on $K(t)$ that is trivial on K is equivalent to exactly one of the valuations just defined.

Let v be one of these valuations, F a finite separable field extension of $K(t)$, and w an extension of v to F. We recall that w is said to be *tamely ramified* over v if the residue class field extension $\overline{K(t)}_v \subset \overline{F}_w$ is separable and the ramification index $e(w/v)$ is not divisible by $\operatorname{char}(\overline{F}_w)$ $(= \operatorname{char}(K))$. If moreover $e(w/v) = 1$, then w is *unramified over* v. Finally, v is said to be tamely ramified, or unramified, in F if every w extending v is tamely ramified, or unramified.

6.20 Proposition. *Let K be a field, t transcendental over K, and F a finite separable extension of $K(t)$ such that every element of $F - K$ is transcendental over K. Suppose that the valuation v_∞ defined above is tamely ramified in F, and that all valuations v_f defined above are unramified in F. Then $F = K(t)$.*

Proof. Let v and w be as above, and let $K(t)_v$ and F_w denote the completions. The *differential exponent* $m(w)$ of w (with respect to $K(t)$) is defined to be the largest integer m with the property that any $x \in F_w$ with $e(w/v)w(x) \geq -m$ satisfies $v(\operatorname{Tr}_{F_w/K(t)_v}(x)) \geq 0$ (see [6, Chapter IV, Section 8]; observe that $e(w/v)w$ is the *normalized* valuation equivalent to w, i.e., it has value group $\mathbb{Z}$). We have

$$m(w) \geq e(w/v) - 1$$
$$m(w) = e(w/v) - 1 \Leftrightarrow w \text{ is tamely ramified over } v$$

(see [6, Chapter IV, Theorem 7]), and therefore

$$m(w) = 0 \Leftrightarrow w \text{ is unramified over } v.$$

For almost all pairs v, w we have $m(w) = 0$.

To every F as in the proposition is attached a non-negative integer g_F, the *genus* of F, see [6, Chapter II, Section 1]. By Hurwitz's formula [6, Chapter VI, Section 2, Corollary 2 to Theorem 2] we have

$$2g_F - 2 = [F : K(t)](2g_{K(t)} - 2) + \sum m(w)[\overline{F}_w : K],$$

the sum ranging over all w as above, with $\overline{F}_w$ denoting the residue class field. We notice that the hypothesis that every element of $F - K$ be transcendental over K is needed for this formula. Using the ramification hypotheses of 6.20 and the fact that $g_{K(t)} = 0$ (see [6, Chapter II, Section 2]) we find from Hurwitz's formula

$$2g_F - 2 = -2[F : K(t)] + \sum (e(w/v_\infty) - 1)f(w/v_\infty),$$

the sum now ranging over the valuations w of F extending v_∞, and $f(w/v_\infty)$ denoting the residue class field degree $[\overline{F}_w : \overline{K}_{v_\infty}] = [\overline{F}_w : K]$. The well-known formula $\sum e(w/v_\infty)f(w/v_\infty)$ $= [F : K(t)]$ (see [6, Chapter IV, Theorem 1]) now yields

$$-2 \leq 2g_F - 2 < -2[F : K(t)] + [F : K(t)] = -[F : K(t)],$$

so $[F : K(t)] = 1$ and $F = K(t)$. This proves 6.20.

6.21 Corollary. *Let K be a field, t transcendental over K, and F a finite separable extension of $K(t)$. Suppose that v_∞ is tamely ramified in F, and that all v_f are unramified in F. Then $F = L(t)$ for some finite separable extension L of K.*

Proof. Let $L = \{x \in F : x \text{ is algebraic over } K\}$. Then t is transcendental over L. Applying 6.20 to the extension $L(t) \subset F$ we see that $L(t) = F$. Since $K(t) \subset L(t) = F$ is finite separable the same is true for $K \subset L$. This proves 6.21.

6.22 The fundamental group of $\mathbb{P}^1_K$. Let K be a field, and $X = \mathbb{P}^1_K$ the projective line over K. The discussion in 6.18 applies to X, the function field of X being $K(t)$, with t transcendental over X, and the valuations of $K(t)$ corresponding to the closed points of X are the valuations v_f, v_∞ defined in 6.19. If F is a finite separable field extension that is unramified at all these valuations, then 6.21 implies that $F \subset K_s(t)$, where K_s denotes a separable closure of K. Conversely it is easy to see that $K(t) \subset K_s(t)$ is unramified at all these valuations. Therefore the field M from 6.17 equals $K_s(t)$, and by 6.17 we have $\pi(\mathbb{P}^1_K) \cong \mathrm{Gal}(K_s(t)/K(t)) \cong \mathrm{Gal}(K_s/K) \cong \pi(\mathrm{Spec}\, K)$. In particular $\pi(\mathbb{P}^1_K)$ is trivial if K is separably closed.

6.23 The fundamental group of $\mathbb{A}^1_K$. Again let K be a field, and $X = \mathbb{A}^1_K = \operatorname{Spec} K[t]$ the affine line over K, with t transcendental over K. The function field of X is $K(t)$, and the valuations of $K(t)$ corresponding to the closed points of X are the valuations v_f defined in 6.19.

Suppose that $\operatorname{char} K = 0$. Then every valuation of $K(t)$ that is trivial on K, in particular v_∞, is tamely ramified in any finite extension $K(t) \subset F$. Hence using 6.21 we find, as in 6.22, that the field M from 6.17 again equals $K_s(T)$. Consequently $\pi(\mathbb{A}^1_K) \cong \pi(\operatorname{Spec} K)$ if K has characteristic zero.

If $\operatorname{char} K = p > 0$ the natural map $\pi(\mathbb{A}^1_K) \to \pi(\operatorname{Spec} K)$ is still surjective, but it is not injective (see Exercise 6.28). In particular $\pi(\mathbb{A}^1_K)$ is non-trivial if K is a separably closed field of non-zero characteristic.

6.24 Finite rings. Let A be a finite ring, and suppose that $\operatorname{Spec} A$ is *connected.* Then A is a local ring with a nilpotent maximal ideal $\mathfrak{m}$, by [1, Chapter 8]. Let k denote its residue class field. We claim that $\pi(\operatorname{Spec} A) \cong \pi(\operatorname{Spec} k) \cong \hat{\mathbb{Z}}$.

The ring homomorphism $A \to k$ induces a continuous group homomorphism $\pi(\operatorname{Spec} k) \to \pi(\operatorname{Spec} A)$. If B is an A-algebra for which $\operatorname{Spec} B \otimes_A k$ is connected, then $\operatorname{Spec} B$ is connected, by Exercise 6.32. Hence by Exercise 3.23(a) the map $\pi(\operatorname{Spec} k) \to \pi(\operatorname{Spec} A)$ is surjective. Next let $\operatorname{Spec} \ell$ be a connected object of $\mathbf{FEt}_{\operatorname{Spec} k}$. Then $\ell \cong k[X]/fk[X]$ for some separable irreducible $f \in k[X]$. Choose $g \in A[X]$ with $(g \bmod \mathfrak{m}[X]) = f$, and such that the leading coefficient of g is a unit. Then $B = A[X]/gA[X]$ is free as an A-module, and $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified. Hence $\operatorname{Spec} B$ belongs to $\mathbf{FEt}_{\operatorname{Spec} A}$, and $B \otimes_A k \cong \ell$. From Exercise 3.23(b) it now follows that $\pi(\operatorname{Spec} k) \to \pi(\operatorname{Spec} A)$ is injective. This proves that $\pi(\operatorname{Spec} A) \cong \pi(\operatorname{Spec} k)$. In 2.5 we have already seen that $\pi(\operatorname{Spec} k) \cong \hat{\mathbb{Z}}$.

Exercises for Section 6

6.1 A module M over a domain A is called *torsionfree* if for every non-zero $a \in A$ and every non-zero $x \in M$ one has $ax \neq 0$.

(a) Prove that a flat module over a domain is torsionfree.

(b) Let A be a Dedekind domain. Prove that any torsionfree A-module can be written as an injective limit of finitely generated projective A-modules, and that an A-module is flat if and only if it is torsionfree.

6.2 Prove Proposition 6.3.

6.3 Let $f\colon Y \to X$ be a morphism of schemes. Prove that f is finitely presented (as in 6.4) if and only if for every open affine subset $U = \operatorname{Spec} A \subset X$ the open subscheme $f^{-1}[U] \subset Y$ is affine, $f^{-1}[U] = \operatorname{Spec} B$, where B is an A-algebra that is finitely presented as an A-module.

6.4 Let M be a module over a ring A. Prove that M is a flat A-module if and only if $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module for every maximal ideal $\mathfrak{m}$ of A, and if and only if $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for every prime ideal $\mathfrak{p}$ of A.

6.5 Let $A = \mathbb{F}_2^V$, where V is a set.

(a) Prove that $A_{\mathfrak{p}} \cong \mathbb{F}_2$ for every prime ideal $\mathfrak{p}$ of A, and that every A-module is flat.

(b) Suppose that V is infinite. Prove that there is a finitely generated flat A-module that is not projective. [*Hint:* Exercise 4.23.]

6.6 Let A be a ring, B a finitely generated A-algebra, and $\mathfrak{q} \in \operatorname{Spec} B$. Prove that the morphism $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ is unramified at $\mathfrak{q}$ if and only if $\mathfrak{p} = f(\mathfrak{q})$ generates the maximal ideal of $B_{\mathfrak{q}}$ and the residue class field $k(\mathfrak{q})$ is a finite separable extension of $k(\mathfrak{p})$.

6.7 Let A be a Dedekind domain and B the integral closure of A in a finite separable field extension of the field of fractions of A. Let further $\mathfrak{q}$ be a maximal ideal of B, and $\mathfrak{p} = A \cap \mathfrak{q}$. Prove that $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified at $\mathfrak{q}$ if and only if the ramification index $e(\mathfrak{q}/\mathfrak{p})$ equals 1 and $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$, i.e., if and only if $\mathfrak{q}$ is unramified over $\mathfrak{p}$ in the sense of algebraic number theory.

6.8 Let $A = \prod_{i \in I} k_i$ be the product of an infinite collection $(k_i)_{i \in I}$ of fields, and $\mathfrak{a} = \{(x_i)_{i \in I} \in A : x_i = 0 \text{ for almost all } i \in I\}$. Prove that the morphism $\operatorname{Spec} A/\mathfrak{a} \to \operatorname{Spec} A$ is finite and étale, but not finite étale.

6.9 Let A be a ring, M and N two finitely generated free A-modules, and $f\colon M \to N$ an A-linear map. Prove that f is an isomorphism if and only if for each $\mathfrak{p} \in \operatorname{Spec} A$ the induced map $M \otimes_A k(\mathfrak{p}) \to N \otimes_A k(\mathfrak{p})$ is an isomorphism.

6.10 Prove that a morphism $f\colon Y \to X$ of schemes is finite étale if and only if it is finitely presented (see 6.4), flat, and unramified at every *closed* point $y \in Y$.

6.11 Let A be a ring, B a separable A-algebra (see 6.10), and C an A-algebra. Prove that $B \otimes_A C$ is a separable C-algebra.

6.12 Let A be a ring and $B_1, B_2, \ldots, B_n$ algebras over A. Prove that $\prod_{i=1}^n B_i$ is a separable A-algebra if and only if each B_i is a separable A-algebra.

6.13 Let K be an algebraically closed field and B a finite dimensional K-algebra that is a local ring. Prove that the residue class field of B is K, and that $B \otimes_K B$ is a local ring.

6.14 Let X be a topological space that can be written as the union of open irreducible subsets. Prove that X can be written as the *disjoint* union of open irreducible subsets.

6.15 Let A be a noetherian ring for which $\operatorname{Spec} A$ is connected, and suppose that $A_{\mathfrak{p}}$ is a domain for all $\mathfrak{p} \in \operatorname{Spec} A$. Prove that A is a domain. [*Hint:* if $\mathfrak{a} \cdot \mathfrak{b} = 0$ for all non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of A, choose $\mathfrak{a}, \mathfrak{b}$ as large as possible and prove that $\mathfrak{a} + \mathfrak{b} = A$.]

6.16 Let X be a locally noetherian scheme all of whose local rings are domains. Prove that X is the disjoint union of a collection of integral schemes. [*Hint:* use Exercises 6.14 and 6.15.]

6.17 Let A be a domain that is integrally closed in its field of fractions K, and let x be an element of an extension field of K. Prove that x is integral over A if and only if the irreducible polynomial of x over K has coefficients in A.

6.18 Let K be a field, L a finite extension field of K, and $x \in L$. Let $\sum_{i=0}^{n} a_i X^i$ be the irreducible polynomial of x over K, with $a_n = 1$. Prove that $\operatorname{Tr}_{L/K}(x) = -[L : K(x)] \cdot a_{n-1}$.

6.19 Let K be a finite field and C the K-algebra $K^{\#K+1}$. Prove that there does not exist $\gamma \in C$ with $C = K[\gamma]$.

6.20 Let A be a domain with field of fractions K, and L an algebraic field extension of K. Prove that for every $x \in L$ there exists $a \in A$, $a \neq 0$, such that ax is integral over A.

6.21 Let $f\colon Y \to X$ be a continuous surjective map from a topological space Y to a connected topological space X, and assume that every $x \in X$ has an open neighborhood U for which $f^{-1}(U)$ is connected. Prove that Y is connected.

6.22 Let X be a locally noetherian normal integral scheme with function field K, and L a finite separable field extension of K. Prove that the normalization Y of X in L is finite over X. [*Hint:* use [1, Proposition 5.17].] Prove also that Y is locally free of degree $[L : K]$ over X if X has dimension one. [*Hint:* Exercise 4.10(c).]

6.23 Let A be a ring and B a finitely generated A-algebra that is integral over A. Prove that B is finitely generated as an A-module.

6.24 Let X be a normal integral scheme with function field K, and L_1, L_2 two finite separable field extensions of K within a given algebraic closure of K. Prove: if X is unramified in L_1 and in L_2, then X is unramified in $L_1 \cdot L_2$ and in every subextension of $K \subset L_1$. [*Hint:* use 6.17 and its proof.]

6.25 Let X, K, M be as in 6.17, and L a finite field extension of K contained in M. Prove that X is unramified in L.

6.26 Let X be a connected scheme. Prove that the following properties are equivalent:

(a) X is locally noetherian, and every local ring of X is a discrete valuation ring or a field;

(b) there is a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$, where each A_i is a Dedekind domain or a field;

(c) for each open affine subset $U = \emptyset$ of X we have $U = \operatorname{Spec} A$, where A is a Dedekind domain or a field.

6.27 Let X be a connected locally noetherian normal scheme of dimension one, K its function field (cf. Exercise 6.16), and K_s a separable closure of K. For each closed point $x \in X$ let w_x be a valuation on K_s extending the valuation on K corresponding to x (see 6.18), and let I_x be the inertia group of w_x in $\operatorname{Gal}(K_s/K)$. Prove that $\pi(X) \cong \operatorname{Gal}(K_s/K)/N$, where N is the closure of the normal subgroup of $\operatorname{Gal}(K_s/K)$ generated by all groups I_x.

6.28 Let $K[t]$ be the polynomial ring in one variable over a field K of non-zero characteristic p, and let $f \in K[t] - \{0\}$ have degree not divisible by p. Prove that $X = \operatorname{Spec} K[t]$ is unramified in the p-th degree extension $K(t, u)$ of $K(t)$ defined by $u^p - u = f$. Deduce that the natural map $\pi(\mathbb{A}^1_K) \to \pi(\operatorname{Spec} K)$ is not injective.

6.29 Let K be a separably closed field with $\operatorname{char}(K) = p > 0$. Prove that $\pi(\mathbb{A}^1_K)$ is topologically generated by its p-Sylow subgroups [23, Chapitre I, numéro 1.4].

6.30 Prove that $\pi(\operatorname{Spec} \mathbb{Z}[1/2])$ is topologically generated by its 2-Sylow subgroups. Prove that $\pi(\operatorname{Spec} \mathbb{Z}[1/p])$ is *not* topologically generated by its p-Sylow subgroups if p is an odd prime.

6.31 Prove that $\pi(\operatorname{Spec} \mathbb{Z}[X])$ and $\pi(\mathbb{P}^1_{\mathbb{Z}})$ are trivial.

6.32 Let B be a ring and $I \subset B$ a nilpotent ideal. Prove that the set of idempotents of B maps bijectively to the set of idempotents of B/I, under the natural map $B \to B/I$.

6.33 Let p be a prime number and $n \in \mathbb{Z}$, $n > 0$. Prove that the ring homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ induces an isomorphism $\pi(\operatorname{Spec} \mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} \pi(\operatorname{Spec} \mathbb{Z}_p)$.

6.34 Let A be a complete local ring with residue class field k. Prove that $\pi(\operatorname{Spec} A) \cong \pi(\operatorname{Spec} k)$.

6.35 Prove that $\pi(\operatorname{Spec} \mathbb{Z}[\mathrm{i}])$ and $\pi(\operatorname{Spec} \mathbb{Z}[(1 + \sqrt{-3})/2])$ are trivial.

6.36 (a) Let K be a totally imaginary number field with class number h, ring of integers A, and discriminant Δ over $\mathbb{Q}$. Suppose that for every totally imaginary number field L with $[L:\mathbb{Q}] \geq 60 \cdot h \cdot [K:\mathbb{Q}]$ the discriminant Δ_L of L over $\mathbb{Q}$ satisfies $|\Delta_L|^{1/[L:\mathbb{Q}]} > |\Delta_K|^{1/[K:\mathbb{Q}]}$. Prove that $\pi(\operatorname{Spec} A)$ is a finite solvable group. [*Hint:* use class field theory, see Exercise 1.23.]

(b) Prove that $\pi(\operatorname{Spec} \mathbb{Z}[\zeta_{20}])$ is trivial, where ζ_{20} denotes a primitive 20-th root of unity. [*Hint:* use (a) and the results of [25, Chapter 11].]

(c) Prove that $\pi(\operatorname{Spec} \mathbb{Z}[\sqrt{-5}])$ has order two, and that $\pi(\operatorname{Spec} \mathbb{Z}[(1+\sqrt{-163})/2])$ is trivial.

6.37 Let A_0, A_1, A_2 be local rings with maximal ideals $\mathfrak{m}_0, \mathfrak{m}_1, \mathfrak{m}_2$, and $f_i \colon A_i \to A_2$ $(i = 0, 1)$ ring homomorphisms that are *local* (i.e., $f_i[\mathfrak{m}_i] \subset \mathfrak{m}_2$ or, equivalently, $f_i^{-1}(\mathfrak{m}_2) = \mathfrak{m}_i$). Put $A = A_0 \times_{A_2} A_1 = \{(a_0, a_1) \in A_0 \times A_1 : f_0(a_0) = f_1(a_1)\}$.

(a) Prove that A is a local ring.

(b) Let B be a free separable A-algebra, and put $B_i = B \otimes_A A_i$, for $i = 0, 1, 2$. Suppose that there are isomorphisms $B_i \cong A_i \times A_i \times \cdots \times A_i$ of A_i-algebras, for $i = 0, 1$. Prove that for some $n \geq 0$ isomorphisms $B_i \cong A_i^n$ of A_i-algebras can be chosen, for $i = 0, 1, 2$, such that the diagram of natural maps

$$\begin{array}{ccccc} B_0 & \longrightarrow & B_2 & \longleftarrow & B_1 \\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr \\ A_0^n & \longrightarrow & A_2^n & \longleftarrow & A_1^n \end{array}$$

is commutative.

(c) With the hypotheses of (b), prove that $B \cong A \times A \times \cdots \times A$ as A-algebras.

6.38 Let A be the ring $\{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \bmod 6\}$.

(a) Describe $\operatorname{Spec} A$.

(b) Prove that every finite étale covering of $\operatorname{Spec} A$ is locally totally split (see Exercise 5.22(a)). [*Hint:* use Exercise 6.37 and the fact that $\pi(\mathbb{Z})$ is trivial.]

(c) Prove that $\pi(\operatorname{Spec} A) \cong \hat{\mathbb{Z}}$. [*Hint:* Exercise 5.22(a).]

(d) Let $n \in \mathbb{Z}$, $n > 0$. Prove that up to isomorphism there exists exactly one projective separable A-algebra B of rank n over A for which $\operatorname{Spec} B$ is connected. Give an explicit description of this algebra.

6.39 Let A be the group ring of the cyclic group of order 6 over $\mathbb{Z}$.

(a) Prove that A is isomorphic to a subring of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}[(1+\sqrt{-3})/2] \times \mathbb{Z}[(1+\sqrt{-3})/2]$ of index $2^3 \cdot 3^2$, and describe $\operatorname{Spec} A$.

(b) Prove that $\pi(\operatorname{Spec} A) \cong \hat{\mathbb{Z}}$.

6.40 Prove that $\pi(\operatorname{Spec} \mathbb{Z}[\sqrt{-3}])$ is cyclic of order two (cf. Exercise 1.29).

Bibliography

The numbers at the end of each entry indicate the pages on which it is referred to.

1. M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley, Reading, 1969; 5, 5, 21, 56, 58, 70, 83, 83, 83, 91, 92, 95, 97.
2. M. Barr, Abstract Galois theory, I. *Journal Pure & Applied Algebra* **19** (1980), 21–42; II, ibidem **25** (1982), 227–247 (I wish to thank I. Moerdijk for pointing out this reference); 2.
3. H. Bass, Big projective modules are free. *Illinois Journal of Mathematics* **7** (1963), 24–31; 55.
4. H. Bass, *Algebraic K-theory*. Benjamin, New York (1968); 55, 66.
5. J.W.S. Cassels, A. Fröhlich (editors), *Algebraic number theory. Proceedings of an instructional conference*, Academic Press, London (1967); 5, 8, 15.
6. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*. American Mathematical Society, Providence (1951); 93, 93, 93, 94, 94, 94, 94.
7. F. DeMeyer, E. Ingraham, *Separable algebras over commutative rings. Lecture Notes in Mathematics* **181**, Springer-Verlag, Berlin (1971); 83, 88.
8. C. Godbillon, *Éléments de topologie algébrique*. Hermann, Paris (1971); 2, 10, 10.
9. A. Grothendieck, *Séminaire de géométrie algébrique, 1: Revêtements étales et groupe fondamental. Lecture Notes in Mathematics* **224**, Springer-Verlag, Berlin (1971); 5, 5, 11, 33, 83, 83.
10. R. Hartshorne, *Algebraic geometry*. Springer-Verlag, New York (1977); 1, 5, 7, 11, 11, 56, 67, 67, 69, 69, 71, 71, 71, 75, 75, 84, 86, 88, 88, 89, 89, 91, 91, 91.
11. E. Hewitt, K. A. Ross, *Abstract harmonic analysis*, I. Springer-Verlag, Berlin (1963); 15.
12. P. J. Higgins, *Notes on categories and groupoids*. Van Nostrand Reinhold, London (1971); 5, 47.
13. P. T. Johnstone, *Topos theory*. Academic Press, London (1977); 33.
14. I. Kaplansky, Projective modules. *Annals of Mathematics* **68** (1958), 372–377; 55.
15. I. Kaplansky, *Fields and rings*, second edition. University of Chicago Press, Chicago (1972); 26.
16. T. Y. Lam, *Serre's conjecture. Lecture Notes in Mathematics* **635**, Springer-Verlag, Berlin (1978); 55, 55.
17. S. Lang, *Algebraic number theory*. Addison-Wesley, Reading (1970); 5, 15.
18. A. R. Magid, *The separable Galois theory of commutative rings*. Marcel Dekker, New York (1974); 5.

19. W. S. Massey, *Algebraic topology: an introduction*, fourth printing. Springer-Verlag, New York (1977); 2, 2, 10, 10.
20. J. S. Milne, *Étale cohomology*. Princeton University Press, Princeton (1980); 5, 11, 11, 83, 83, 87.
21. J. Milnor, *Introduction to algebraic K-theory*. Princeton University Press, Princeton (1971); 55.
22. J. P. Murre, *Lectures on an introduction to Grothendieck's theory of the fundamental group*. Tata Institute of Fundamental Research, Bombay (1967); 5, 11, 83.
23. J-P. Serre, *Cohomologie galoisienne*, quatrième édition, *Lecture Notes in Mathematics* **5**, Springer-Verlag, Berlin (1973); 31, 98.
24. J-P. Serre, *Arbres, amalgames,* SL_2. *Astérisque* **46**, Société Mathématique de France, Paris (1977); 13.
25. L. C. Washington, *Introduction to cyclotomic fields*. Springer-Verlag, New York (1982); 99.
26. E. Weiss, *Algebraic number theory*. McGraw-Hill, New York (1963); 5, 92.

List of symbols

$\#$	cardinality of a set
$\amalg$	sum in a category, disjoint union 34
$\times$	product 34
$\times_S$	fibred product over S 33
$/$	quotient (of object by group of automorphisms) 34
$[:]$	degree of a field extension
$[:]$	rank of an algebra 58
$[:]$	degree of a morphism of schemes 69
$\mathbf{C}$	category
sets	category of finite sets
π-**sets**	category of finite sets with continuous π-action 9
$\mathbf{FEt}_X$	category of finite étale coverings of a scheme X 7
${}_K\mathbf{SAlg}$	category of free separable K-algebras
$\mathbf{Aff_X}$	category of affine morphisms to a scheme X 75
$\mathbb{Z}$	ring of rational integers
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
$\mathbb{F}_q$	finite field of q elements
$\mathbb{Z}_p$	ring of p-adic integers 9
$\mathbb{A}^1_K$	affine line over K [10, p. 74]
$\mathbb{P}^1_K$	projective line over K [10, p. 77]
$\pi(X)$	fundamental group of a pathwise connected topological space X 2
$\pi(X)$	fundamental group of a connected scheme X 9
$\hat{\pi}(X)$	profinite fundamental group of a connected topological space X 10
$\pi(X,x)$	fundamental group in a point x of a pathwise connected topological space X 10
$\pi(X,x)$	fundamental group in a geometric point x of a connected scheme X 37
$\hat{\pi}(X,x)$	profinite fundamental group in a point x of a connected topological space X 39

K_s	separable closure of a field K	20
$\overline{K}$	algebraic closure of a field K	
$\overline{F}$	residue class field of a field F	92
F_v	completion of a field F at a valuation v	93
A^*	group of units of a ring A	
P^*	dual $\mathrm{Hom}(P, A)$ of a projective A-module P	57
$\overline{G}$	profinite completion of a group G	8
E^G	set of G-invariants of a G-set E	9
A^E	ring of functions from a finite set E to a ring A	80
A^m	subgroup of m-th powers in a multiplicative group A	29
A^n	product of n copies of a ring A	
$A_{\mathfrak{p}}$	localization of a ring A at the prime ideal $\mathfrak{p}$	
$\sqrt{0}$	nilradical of a ring	21
X_h	complex analytic space associated to a variety X [10, p. 493]	11
$\mathcal{O}_{Y,y}$	local ring in point y of scheme Y [10, p. 72]	83
$\mathrm{Alg}_K(B, K_s)$	set of K-algebra homomorphisms $B \to K_s$	23
$\mathrm{Aut}(L)$	automorphism group of L	17
$\mathrm{Aut}_K(L)$	group of K-automorphisms of field L	17
$\mathrm{Aut}(F)$	automorphism group of a fundamental functor F	36
$\mathrm{char}(K)$	characteristic of a field K	
$\deg f$	degree of a polynomial f	
$\deg f$	degree of a morphism f between schemes	69
$\mathrm{End}_A P$	module of A-endomorphisms of an A-module P	57
$\mathrm{Gal}(L/K)$	Galois group of a field extension L over K	17
$\mathrm{Hom}_A(M, N)$	module of A-module homomorphisms from M to N	
$\mathrm{index}[\ :\ ]$	index of a subgroup in a group	
$\varprojlim$	projective limit	8
$\mathrm{Mor}_{\mathbf{C}}(A, X)$	set of morphisms in $\mathbf{C}$ from A to X	40
$\mathrm{Mor}_\pi(E, K_s)$	set of morphisms of π-sets $E \to K_s$	23
$\mathrm{rank}_A(M)$	rank of module M over A	6
$\mathrm{sp}(X)$	underlying topological space of a scheme X	
$\mathrm{Spec}\, A$	spectrum of a ring A	
$\mathrm{Tr}(f)$	trace of an A-module endomorphism f	6
$\mathrm{Tr}(f)$	trace of an element b of an A-algebra B	6
$\mathrm{Tr}_{P/A}(f)$	trace of an A-endomorphism f of a projective A-module P	57
$\mathrm{Tr}(C)$	trace of a matrix C	12

Index

Page numbers in *italics* refer to definitions.