Galois Theory for Schemes

H. W. Lenstra, Jr.

Department of Mathematics
University of California
Berkeley, California 94720–3840

Second printing 1997

First printing 1985
(by the Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam)

Table of Contents

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 most fundamental properties of schemes. The first five sections of Hartshorne's book [10], Chapter II, contain more than we need.

The main theory of Galois theory for schemes classifies the *finite étale coverings* 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 $f : Y \to X$ a continuous map. We call $f : Y \to X$ 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 $f : f^{-1}(U) \to U$ 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 $f : Y \to X$ to a covering $g : Z \to X$ is a continuous map $h : Y \to Z$ for which $f = gh$.

$$\begin{array}{ccc} Y & \xrightarrow{h} & Z \\ f \searrow & & \swarrow g \\ & X & \end{array}$$

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 only wishes to classify the *finite* coverings of X. For this it suffices that X is *connected*, i.e. has 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 $f : Y \to X$ 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 $g \in \mathbb{C}[\mathbb{U}, \mathbb{V}]$ 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 $f : C \to \mathbb{C}$ 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 $u \in \mathbb{C} - \{-100/27,\ 9\}$. From this it can be deduced that f becomes a covering if points with $u = -100/27$ or $u = 9$ are removed; i.e., if $X = \mathbb{C} - \{-100/27,\ 9\}$ and $Y = f^{-1}[X] \subset C$ then $f : Y \to X$ 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 Spec A, where $A = \mathbb{C}[U, ((27U + 100)(U - 9))^{-1}]$, and Y corresponds to Spec B, where $B = A[V]/gA[V]$. The morphism Spec $B \to$ 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 Spec A. Its local ring is the field of fractions $Q(A) = \mathbb{C}(U)$ of A, and the fibre of Spec $B \to$ Spec A over ξ is the spectrum of $Q(B)$. That is a cubic field extension of $Q(A)$, so Spec $Q(B) \to$ Spec $Q(A)$ is not a "trivial covering", and Spec $B \to$ Spec A is not "trivial" in a neighborhood of ξ.

Figure 2

It *is* true that Spec $B \to$ 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 $u \in$ 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 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 for the topological definition To illustrate this we write, for a subfield $K \subset \mathbb{C}$

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

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 $u < -100/27$ the degree is one The algebraic definition, however, takes the "invisible points" into account, and Spec $B_{\mathbb{R}} \to$ Spec $A_{\mathbb{R}}$ is a finite étale covering that has everywhere degree 3 (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 $u = 1/n$ has none, for $n \in \mathbb{Z}$, $n \neq 0$ The morphism Spec $B_K \to$ 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 the 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 $(w_i)_{i \in I}$ of M is called a *basis* of M (over A) if for every $x \in M$ there is a unique collection $(a_i)_{i \in I}$ 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 $(w_i)_{i \in I}$, then the cardinality $\#I$ only depends 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 $f : M \to M$ be A-linear. Then

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

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 only depends on f, and not on the choice of the basis (see 4.8, or Exercise 1.2). It is easily checked that the map $\mathrm{Tr} : \mathrm{Hom}_A(M, M) \to A$ is 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 $m_b : B \to B$ 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 $\mathrm{Tr}: B \to A$ 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 $\phi : B \to \mathrm{Hom}_A(B, A)$ 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 is 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 $n \geqq 0$ 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,a nd $t \geqq 0$, see Theorem 2 7. Further examples are found in Exercises 1.5 and 1.6.

1.4 Finite étale morphism

A morphism $f : Y \to X$ of schemes is *finite étale* if there exists a covering of X by open affine subsets $U_i = \text{Spec } A_i$, such that for each i the open subscheme $f^{-1}(U_i)$ of Y is affine, and equal to Spec B_i, where B_i is a free separable A_i-algebra. In this situation we also say that $f : Y \to X$ 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 $U = \text{Spec } A$ of X the open subscheme $f^{-1}(U)$ of Y is affine, $f^{-1}(U) = \text{Spec } B$, 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 $X \coprod X \coprod \cdots \coprod X$ 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 $X = \text{Spec } \mathbb{Z}$ there are no others (see 1.12 and 6.18). If $X = \text{Spec } K$, where K is a field, the finite étale coverings $Y \to X$ are precisely given by $Y = \coprod_{i=1}^{t} \text{Spec } B_i$, with B_i and t as in 1.3. If $X = \text{Spec } A$, 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 $Y = \coprod_{i=1}^{t} \text{Spec } A_i$, where $t \geqq 0$ 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 $f : Y \to X$ to a finite étale covering $g : Z \to X$ is a morphism of schemes $h : Y \to Z$ 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 $\underline{FEt}_X$.

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 $k \geqq i$ and $k \geqq j$. 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 $(f_{ij} : S_i \to S_j)_{i,j \in I,\ i \geqq j}$ satisfying the conditions

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

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

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

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, $(\pi_i)_{i \in I}$, $(f_{ij})_{i,j \in I,\ i \geqq j}$ 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 homomorphismwith 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 homomorphismis 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 $N \geqq N' \Leftrightarrow N \subset N'$. 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 $N \geqq N'$) being the canonical homomorphisms. Hence $\hat{G} = \lim_{\leftarrow} G/N$ is a profinite group, and it is called the *profinite completion* of G. In particular we have

$$\hat{\mathbb{Z}} = \lim_{\substack{\leftarrow \\ n>0}} \mathbb{Z}/n\mathbb{Z} \ ,$$

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 $n \geqq m$), is a projective system, and

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

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 $f : E \to E'$ 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 $\underline{FEt}_X$ 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 $X = \text{Spec } \mathbb{Z}$ there are no other finite étale coverings of X is thus expressed by the group $\pi(\text{Spec } \mathbb{Z})$ being *trivial*. The same is true for $\pi(\text{Spec } K)$, where K is an algebraically closed field. More generally, if K is an arbitrary field, then $\pi(\text{Spec } K)$ 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, $\pi(\text{Spec } K) \cong \hat{\mathbb{Z}}$ if K is a finite field (see 2.5).

Next let $X = \text{Spec } A$, 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 $\pi(\text{Spec } A[\frac{1}{a}])$ 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 $\pi(\text{Spec } \mathbb{Z}_{(p)}) \cong \hat{\mathbb{Z}}$, 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 only considering *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 nonsingular 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 to calculate 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 $\pi(\mathbb{P}^1_K) = \pi(\text{Spec } K)$, where $\mathbb{P}^1_K$ denotes the projective line over K. If moreover $\text{char}(K) = 0$, then also $\pi(\mathbb{A}^1_K) = \pi(\text{Spec } K)$, 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 $(w_\imath)_{\imath \in I}$.

(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

$$v_\imath = \sum_{\jmath=1}^{n} a_{\imath\jmath} w_\jmath \in M \qquad (1 \leqq \imath \leqq n)$$

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

(b) The trace $\mathrm{Tr}(C)$ of an $n \times n$-matrix $C = (c_{\imath\jmath})_{1 \leqq \imath,\jmath \leqq n}$ over A is defined by $\mathrm{Tr}(C) = \sum_{\imath=1}^{n} c_{\imath\imath}$. Prove that

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

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 $A \Leftrightarrow \det(\mathrm{Tr}(w_\imath w_\jmath))_{1 \leqq \imath,\jmath \leqq n}) \in A^*$.

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 $A\left[\frac{1}{\Delta}\right]$ is a free separable $\mathbb{Z}\left[\frac{1}{\Delta}\right]$-algebra.

1.6 (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 $\underline{FEt}_X$ is equivalent to a suitably defined "product category" $\underline{FEt}_{X'} \times \underline{FEt}_{X''}$.

1.8 Let $S = \lim_{\leftarrow} S_i$ be a projective limit as in 1.7, and define for each $j \in I$ the projection map $f_j : S \to S_j$ 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 $i \leqq j$;

(ii) if T is a set and $(g_j : T \to S_j)_{j \in I}$ is a collection of maps satisfying $f_{ij} \circ g_i = g_j$ (for all $i, j \in I$ with $i \leqq j$) then there is a unique map $g : T \to S$ 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 $(f'_j : S' \to S_j)_{j \in I}$ a collection of maps satisfying the analogues of (i),(ii), then there is a unique bijection $f' : S' \to S$ such that $f'_j = f_j \circ f'$ for all $j \in I$.

1.9 Let the notation be as in 1.7, and $S = \lim_{\leftarrow} S_i$.

(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 $\phi : i \to \mathbb{Z}$, and let $f_{ij} : S_i \to S_j$ (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 $\pi = \lim_{\leftarrow} \pi_i \subset \prod_{i \in I} \pi_i$ be a profinite group, with all π_i finite groups, and $f_j : \pi \to \pi_j$ 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 $\Leftrightarrow$ π' 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 $i \geqq j$.

(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$f : G \to \hat{G}$ for which $f[G]$ is dense in $\hat{G}$.

(b) Prove: if G is a free group, then the natural map $f : G \to \hat{G}$ 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 $u \in \mathbb{Z}_p^*$, $n \in \mathbb{Z},\ n \geqq 0$;

(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 $\mathbb{Z}_{10} = \varprojlim_{n\geqq 1} \mathbb{Z}/10^n\mathbb{Z}$.

(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 $v : \mathbb{Z}_{10} \to \mathbb{R}$ 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 $b \in \mathbb{Z}$, $b \geqq 0$, 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 (1). Compute c_n for $1 \leqq n \leqq 10$.

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

(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 that $\hat{\mathbb{Z}} \cong \varprojlim_{n>0} \mathbb{Z}/n!\mathbb{Z}$.

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 $\chi : R \to \mathbb{R}/\mathbb{Z}$ 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 $f : E \to E'$ 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 morphismfrom (E, σ, τ) to (E', σ', τ') being a map $f : E \to E'$ satisfying $f\sigma = \sigma' f$ and $f\tau = \tau' f$.

1.22 Let p be a prime number. Prove that $\pi(\mathrm{Spec}\ \mathbb{Z}[\frac{1}{p}])$ 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 $\{A\alpha : \alpha \in K^*,\ \sigma(\alpha) > 0$ for every field homomorphism$\sigma : K \to \mathbb{R}\}$. Let $\pi = \pi(\mathrm{Spec}\ A)$, 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 that $\hat{\pi}(X) \cong \hat{\mathbb{Z}}$.

1.26 (a) Let π be a profinite group such that $x^2 = 1$ for all $x \in \pi$. Prove that $\pi \cong (\mathbb{Z}/2\mathbb{Z})^{\mathbf{n}}$ 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 that $\hat{G} \cong (\mathbb{Z}/2\mathbb{Z})^{2^{\mathbf{k}}}$ 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 $\#X \geqq \#\mathbb{R}$. 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 $\beta = (X \mod X^4 + X^2 + 1) \in B$. 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 $\prod_{n \geqq 1} \mathbb{Z}/p^n\mathbb{Z}$, and $\pi' \subset \pi$ the closure of the subgroup generated by $(1 \mod p^n)_{n=1}^{\infty}$.

(a) Prove that $\pi' \cong \mathbb{Z}_p$ 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 1.1 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 $\bar{K}$ 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 $\bar{K}$ 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 $\bar{K}$, and that $\alpha \in \bar{K}$ 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 $\bar{K}$ 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 $\bar{K}$ 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 equivalent 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 $\mathrm{Gal}(L/K) \cong \varprojlim_{E \in I} \mathrm{Gal}(E/K)$.

Remark. The projective limit, in the final assertion, is defined with respect to the natural restriction maps $\mathrm{Gal}(E/K) \to \mathrm{Gal}(E'/K)$, 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 $\bar{K}$ is an algebraic closure of E_0, the K-isomorphism $\rho : E_0 \xrightarrow{\sim} E_0$ can be extended to a K-isomorphism $\sigma : \bar{K} \xrightarrow{\sim} \bar{K}$. 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 intermediate fields of $K \subset L$ correspond bijectively to the closed subgroups of G. More precisely, the maps $\{E : E$ is a subfield of L containing $K\}\{H : H$ 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

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

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 that $H = J$. The inclusion $H \subset J$ is obvious. Conversely, let $\sigma \in J$. In order to prove that $\sigma \in H$ 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

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

This map is also surjective, since each $\tau : E \xrightarrow{\sim} \tau[E] \subset L$, $\tau|K = \mathrm{id}_K\}$, 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 $\tau : E \to L$ 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 index $[G : H]$ field homomorphisms $\tau : E \to L$ with $\tau|K = \mathrm{id}_K$. It follows that for any *finite* extension $K \subset E'$ with $E' \subset E$ there are at most index $[G : H]$ field homomorphisms $\tau : E' \to L$ with $\tau|K = \mathrm{id}_K$, since any such τ can be extended to E. Hence $[E' : K] \leqq \mathrm{index}[G : H]$ 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 iff 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 $\tau : E \to L$ 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 $\bar{K}$ an algebraic closure of K. The *separable closure* K_s of K is defined by

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

This is a subfield of $\bar{K}$, and $K_s = \bar{K}$ if and only if K is perfect; in particular, $K_s = \bar{K}$ 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 isomorphism classes of finite separable extension fields E of K and conjugacy classes of open subgroups of the absolute Galois group of K.

2.5 Example

Let $\mathbb{F}_q$ be a *finite field*, with algebraic closure $\bar{\mathbb{F}}_q$. The only finite extensions of $\mathbb{F}_q$ in $\bar{\mathbb{F}}_q$ are the fields $\mathbb{F}_{q^n} = \{\alpha \in \bar{\mathbb{F}}_q : \alpha^{q^n} = \alpha\}$ for $n \in \mathbb{Z}$, $n \geq 1$. Each $\bar{\mathbb{F}}_{q^n}$ is Galois over $\mathbb{F}_q$, with $\mathrm{Gal}(\bar{\mathbb{F}}_{q^n}/\bar{\mathbb{F}}_q) \cong \mathbb{Z}/n\mathbb{Z}$, 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 $\mathbb{F}_q$ is isomorphic to $\hat{\mathbb{Z}}$, with $1 \in \mathbb{Z}$ corresponding to $F \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. The closure of the subgroup generated by F is equal to the whole group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. This is expressed by saying that F is a *topological generator* of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

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 $t \in \mathbb{Z}_{\geqq 0}$ 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 $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_n$ are distinct maximal ideals of B, then by the Chinese remainder theorem the natural map $B \to \prod_{i=1}^{n} B/\mathcal{M}_i$ is surjective, so $n \leqq \dim_K B$. This shows that B has only finitely many maximal ideals, say $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_t$. The intersection $\bigcap_{i=1}^{t} \mathcal{M}_i$ 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 $\prod_{i=1}^{t} \mathcal{M}_i^N = 0$ for N sufficiently large. The $\mathcal{M}_i$ are pairwise relatively prime, so the same is true for the $\mathcal{M}_i^N$, and the Chinese remainder theorem therefore gives an isomorphism $B \xrightarrow{\sim} \prod_{i=1}^{t} B/\mathcal{M}_i^N$. Here $B_i = B/\mathcal{M}_i^N$ is local, since $\mathcal{M}_i/\mathcal{M}_i^N$ 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 $\bar{K}$ and B a finite dimensional K-algebra. Denote by $\bar{B}$ the $\bar{K}$-algebra $B \otimes_K \bar{K}$. Then the following four assertions are equivalent:*

(i) *B is separable over K;*

(ii) *$\bar{B}$ is separable over $\bar{K}$;*

(iii) *$\bar{B} \cong \bar{K}^n$ as $\bar{K}$-algebras, for some $n \geqq 0$;*

(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) $\Rightarrow$ (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 $\bar{K}$-basis for $\bar{B}$. It follows that the diagram

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

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

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

(ii) $\Rightarrow$ (iii). Applying 2.6 to $\bar{K}, \bar{B}$ we see that $\bar{B} \cong \prod_{j=1}^u C_j$ for certain local $\bar{K}$-algebras C_j with nilpotent maximal ideals $\mathcal{M}_j$. Since $\bar{B}$ is separable over $\bar{K}$ it clearly follows that each C_j is separable over $\bar{K}$. Let j be fixed, and let $\phi : C_j \to \bar{K}$ be any $\bar{K}$-linear function. By 1.2 there exists $c \in C_j$ with $\phi(x) = \mathrm{Tr}(cx)$ for all $x \in C_j$. Taking $x \in \mathcal{M}_j$ and observing that nilpotent maps have trace zero (over a field), we see that $\mathcal{M}_j \subset \ker \phi$. This is true for each ϕ, so $\mathcal{M}_j = \{0\}$ and C_j is a *field.* Since C_j is finite over $\bar{K}$ and $\bar{K}$ algebraically closed we conclude that $C_j = \bar{K}$, 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 $\bar{B}_i \cong \bar{K}[X]/(f_i)$, and since f_i splits into distinct linear factors $X - \alpha_{ij}$ in $\bar{K}[X]$ the Chinese remainder theorem now implies that $\bar{B}_i \cong \Pi_j \bar{K}[X]/(X - \alpha_{ij}) \cong \bar{K}^{\deg(f_i)}$. 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 $\bar{K}$ we find an injective map $\bar{K}[X]/(f_b) \to \bar{B}$. Thus by (iii) it follows that $K[X]/(f_b)$ has no non-zero nilpotent elements, which means that f_b is a separable polynomial. In particular, if b is nilpotent the $X^n \in (f_b)$ 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) $\Rightarrow$ (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_1. 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 are anti-equivalent.*

Remark. It is clear from the definition in 1.4 that $K^{\mathbf{SAlg}}$ is anti-equivalent to $\mathbf{FEt}_{\mathrm{Spec}\ K}$. So Theorem 2.9 is exactly the case $X = \mathrm{Spec}\ K$ 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 $F : {}_K\mathbf{SAlg} \to \pi\text{-}\mathbf{sets}$ are $G : \pi\text{-}\mathbf{sets} \to {}_K\mathbf{SAlg}$ 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 $\theta_B : B \to GF(B)$, one for each object B of ${}_K\mathbf{SAlg}$, such that for any morphism$f : B \to C$ in ${}_K\mathbf{SAlg}$, the diagram

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

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 $g : B \to K_s$ is such a homomorphismand $\sigma \in \pi$, then $\sigma \circ g : B \to K_s$ 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 $\pi_i \subset \imath$ an open subgroup (see 2.4), for each $\imath$. Then $\mathrm{Alg}_K(B, K_s)$ may be identified with the disjoint union of the sets $\mathrm{Alg}_K(K_s^{\pi}, K_s)$, for $1 \leqq \imath \leqq t$. Here $\mathrm{Alg}_K(K_s^{\pi}, K_s)$ 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 $f : B \to C$ be a morphismin ${}_K\mathbf{SAlg}$, i.e. a K-algebra homomorphismfrom a free separable K-algebra B to a free separable K-algebra C. Then we define $F(f) : F(C) \to F(B)$ by $F(f)(g) = g \circ f$, for a K-algebra homomorphism$g : C \to K_s$. This is evidently a morphismof π-sets, and it is now straightforward to verify that F is a contravariant functor ${}_K\mathbf{SAlg} \to \pi$-*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 $E = \prod_{i=1}^{t} E_i$. Then $G(E)$ may be identified with the product of the K-algebras $G(E_i)$, for $1 \leqq \imath \leqq t$. 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 morphismof π-sets $g : \pi/\pi_i \to K_s$ 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 $f : E \to D$ is a morphismof π-sets then $G(f) : G(D) \to G(E)$, $G(f)(g) = g \circ f$, is a morphismof K-algebras, and this makes G into a contravariant functor $\pi\text{-}sets \to {}_K\mathbf{SAlg}_t$.

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

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

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 $f : B \to C$ is a morphismin ${}_K\mathbf{SAlg}$ then the diagram

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

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

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

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 isomorphismfor all B, and GF is naturally equivalent to the identify functor of ${}_K\mathbf{SAlg}$.

The proof that FG is naturally equivalent to the identity functor of $\pi\text{-}sets$ is completely analogous. For a finite π-set E, one defines

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

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 morphismof π-sets, and if $f : E \to D$ is a morphismof π-sets then by a calculation similar to the above one the diagram

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

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 isomorphismof profinite groups $\mathrm{Gal}(L/K) \cong \lim_{\underset{E \in I}{\leftarrow}} \mathrm{Gal}(E/K)$. (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 $\#H \leqq 2$ 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 $\bar{\mathbb{F}}_q$. For a Steinitz number a, let $\mathbb{F}_{q^a}$ be the set of all $x \in \bar{\mathbb{F}}_q$ 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 $\mathbb{F}_q \subset \bar{\mathbb{F}}_q$. [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 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 $\mathrm{index}[G : H] = \mathrm{index}[G : HB']$ 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 groups of unity in $\bar{\mathbb{Q}}^*$. Prove that the map $\hat{\mathbb{Z}}^* \to \mathrm{Aut}(E)$ induced by (a) is an isomorphismof 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 isomorphismof topological groups.

(d) Prove that there are isomorphisms

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

of topological groups.

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

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

(for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{\mathbb{Q}}), a \in \mathbb{Q}^*$) is an isomorphismof topological groups, if $\mathrm{Homo}(\mathbb{Q}, \{\pm 1\})$ 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 $(n_\imath)_{\imath=0}^{\infty}$ of integers $n_\imath$ for which

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

Define the Jacobi symbol $\left(\begin{array}{c} a \\ n \end{array} \right) \in \{\pm 1\}$ by $(\frac{a}{n}) \in \{\pm 1\}$ by $(\frac{a}{n}) = \lim_{\imath \to \infty} (\frac{b}{n_\imath})/(\frac{c}{n_\imath})$, where $(\frac{b}{n_\imath}), (\frac{c}{n_\imath})$ are the ordinary Jacobi symbols. Prove that this is well-defined

and independent of the choices made. Prove also that the map $\mathbb{Q}^* \times \hat{\mathbb{Z}}^* \to \{\pm 1\}$, $(a, n) \mapsto (\frac{a}{n})$, 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 $\mathbb{Q}(\sqrt{\overline{\mathbb{Q}}})/\mathbb{Q}(\zeta_\infty)$, 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 homomorphismsending $a \in \mathbb{Q}^*$ to $(\frac{a}{n})$.

2.17 **(Kummer theory.)** Let K be a field with algebraic closure $\bar{K}$ 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 $L \subset \bar{K}$ for which

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

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 isomorphismof topological groups $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}(W/K^{*m}, E_m)$ 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 $\bar{K}$ and let $p = \mathrm{char}(K) > 0$. Prove that there is a bijective correspondence between the collection of subfields $L \subset \bar{K}$ for which

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

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

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) 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

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

over $\mathbb{Q}$. We write

M = $\mathbb{Q}(\zeta_\infty)$ (see Exercise 2.13(c)),
E_m = {group of m-th roots of unity} $\subset M^*$,
$\mathbb{Q}$ = 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 $L_m = M\{\alpha \in \bar{\mathbb{Q}} : \alpha^m \in \mathbb{Q})$, for $m \in \mathbb{Z}_{>\not\vdash}$. Prove that $M \subset L_m$ is Galois, and that there is an isomorphismof 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 isomorphismof topological groups

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

here $\mathrm{Homo}(Q, \hat{E}^2)$ 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 $Q \times (\mathbb{Z}_{>\not\vdash}) \to \mathbb{L}^*$ 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 $\mathrm{Homo}(Q, \hat{E}) \rtimes \hat{\mathbb{Z}}^*$ with the product topology, the action of $\hat{\mathbb{Z}}^*$ on $\mathrm{Homo}(Q, \hat{E})$ 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 homomorphismϕ : $\mathrm{Gal}(L/\mathbb{Q}) \to \Gamma$ 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 isomorphismis from Exercise 2.13(c).

(c) Let $H = \{(f, c) \in \Gamma : \forall a \in Q : (f(a) \mod \hat{E}^2) = \left(\frac{a}{c}\right)\}$ 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 $K \subset K_{unr}$ is Galois, and $\mathrm{Gal}(K_{unr}/K) \cong \mathrm{Gal}(k_s/k)$, where k is the residue class field of K and k_s its separable closure.

(b) Prove that $K_{unr} \subset K_{tr}$ is Galois, and that $\mathrm{Gal}(K_{tr}/K_{unr})$ 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 $K \subset K_{tr}$ is Galois, that $\mathrm{Gal}(K_{tr}/K)$ 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 $\mathrm{Gal}(K_{tr}/K)$ is isomorphic to the profinite completion of the group $\langle a, b : aba^{-1} = b^q \rangle$.

(e) Prove that $K_{tr} = K_s = \bar{K}$ if $\mathrm{char}(k) = 0$, and that $\mathrm{Gal}(K_s/K_{tr})$ 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 $\mathrm{Gal}(K_{tr}/K)$ and $\mathrm{Gal}(K_s/K_{tr})$. [*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 $\sigma : \{1, 2, \ldots, s\} \xrightarrow{\sim} \{1, 2, \ldots, t\}$ and isomorphisms $A_i \xrightarrow{\sim} B_{\sigma(i)}$, $1 \leqq i \leqq s$.

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 $B \to \bar{K}$ 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 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,a nd $\rho \subset \pi$ the normalizer of π' in π. Prove that the automorphismgroup of the π-set π/π' in the category of π-*sets* is isomorphic to ρ/π'. In particular, this automorphismgroup 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 $B \otimes_K M \cong M \times M \times \ldots \times M$ 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 $u : X \to Y$ 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* $p_1 : X \times_S Y \to X$, $p_2 : X \times_S Y \to Y$, which make a

commutative diagram with the given morphisms $X \to S$, $Y \to S$, such that given any object Z with morphisms $f : Z \to X$, $g : Z \to Y$ that make a commutative diagram with $X \to S$ and $Y \to S$, there exists a unique morphism $\theta : Z \to X \times_S Y$ such that $f = p_1\theta$ and $g = p_2\theta$.

$$\begin{array}{ccc} & Z & \\ & \swarrow \quad \searrow & \\ X \times_S Y & \xrightarrow[p_2]{} & Y \\ \downarrow p_1 & & \downarrow \\ X & \longrightarrow & S \end{array}$$

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 $\mathbf{C}$ has arbitrary finite left limits, see Exercise 3.3.

(G2) Let $(X_i)_{i \in I}$ be a collection of objects of a category $\mathbf{C}$. The *sum* of the X_i is an object, denoted by $\coprod_{i \in I} X_i$, together with morphisms $q_j : X_j \to \coprod_{i \in I} X_i$ for each $j \in I$, such that for any object Y of $\mathbf{C}$ and any collection of morphisms $f_j : X_j \to Y$, $j \in I$, there is a unique morphism $f : \coprod_{i \in I} X_i \to Y$ 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 $\mathbf{C}$ if any *finite* collection of objects has a sum in $\mathbf{C}$. This is the case in *sets*. The *empty* collection of objects has a sum if and only if $\mathbf{C}$ 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 $\mathbf{C}$. In **sets** the empty set is an initial object.

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

Let X be an object of $\mathbf{C}$ and G a finite subgroup of the group of automorphisms of X in $\mathbf{C}$. The *quotient* of X *by* G is an object of $\mathbf{C}$, denoted by X/G, together with a morphism $p : X \to X/G$ satisfying $p = p\sigma$ for all $\sigma \in G$, such that for any morphism $f : X \to Y$ in $\mathbf{C}$ satisfying $f = f\sigma$ for all $\sigma \in G$ there is a unique morphism $g : X/G \to Y$ for which $g = gp$. 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 $\mathbf{C}$; 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 $f : X \to Y$ be a morphism in $\mathbf{C}$. We call f an *epimorphism* if for any object Z and any morphisms $g, h : Y \to Z$ with $gf = hf$ we have $g = h$, and a *monomorphism* if for any object Z and any morphisms $g, h : Z \to X$ 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 $u : X \to Y$ is called an isomorphism of X with a direct summand of Y if there is a morphism $q_2 : Z \to Y$ such that Y, together with $q_1 = u : X \to Y$ and $q_2 : Z \to Y$ 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 commutes 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 $\sigma_X : F(X) \to F(X)$, one for each object X of $\mathbf{C}$, such that for each morphism $f : Y \to Z$ 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 $Aut(F)$ of F as a subgroup

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

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 $\Pi_X \, S_{F(X)}$ be endowed with the product topology, with each $S_{F(X)}$ discrete. Then for each morphism $f : Y \to Z$ the set $\{(\sigma_X) \in \Pi_X \, S_{F(X)} : \sigma_Z F(f) = F(f)\sigma_Y\}$ is closed, so $Aut(F)$ is a closed subgroup of $\Pi_X \, S_{F(X)}$. From Exercises 1.10 and 1.11(c) it thus follows that $Aut(F)$ 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 $Aut(F)$ acts continuously on the finite set $F(X)$. Let the resulting $Aut(F)$-**set** be called $H(X)$. If $f : Y \to Z$ is any morphism in C then by the commutativity of the above diagram $F(f)$ is a morphism of $Aut(F)$-**sets**. Hence putting $H(f) = F(f)$ we see that $H : \mathbf{C} \to Aut(F)$-**sets** is a functor, and that F is the composite of H and the forgetful functor $Aut(F)-$**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 $Aut(F)$ may be identified with π, and that $H : \mathbf{C} \to Aut(F)$-**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* $H : \mathbf{C} \to Aut(F)$-**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** $\to$ **sets**, *yields the functor* F, *then* π *is canonically isomorphic to* $Aut(F)$;

(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 $\pi \cong Aut(F)$ that is canonically determined up to an inner automorphism of $Aut(F)$.*

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 $x : \operatorname{Spec} \Omega \to X$ 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 $F_x : \mathbf{FEt}_X \to \mathbf{sets}$. 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 isomorphismthat 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 $F_x : \mathbf{C} \to \mathbf{sets}$ send a covering $f : Y \to X$ 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, $f : Y \to X$ and $g : Z \to X$ finite coverings, $h : Y \to Z$ 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 $\alpha : f^{-1}(U) \to U \times D$ and $\beta : g^{-1}(U) \to U \times E$*

and a map $\phi : D \to E$ such that the diagram

$$\begin{array}{ccccc} f^{-1}(U) & & \xrightarrow{h} & & g^{-1}(U) \\ & \alpha \searrow\!\sim & & & \vert g \\ \big\downarrow f & U \times D & \xrightarrow{\mathrm{id}_U \times \phi} & & U \times E \\ & \swarrow & & \downarrow & \\ U & & \xrightarrow[\mathrm{id}_U]{} & U & \end{array}$$

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 $\alpha : f^{-1}(U') \to U' \times D$, $\beta : g^{-1}(U'') \to U'' \times E$ such that the diagrams

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

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 $\beta h \alpha^{-1} : U \times D \to U \times E$. 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 $\phi_u : D \to E$. 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 $\mathrm{id}_X : X \to X$ is clearly a terminal object of $\mathbf{C}$. If $g : Y \to Z$, $h : W \to Z$ 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 $g : Y \to Z$ 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 $h : W \to Z$ are trivial above U. Then it is straightforward to verify that $p : Y \times_Z W \to X$ 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 $f : Y \to X$ with $Y = \emptyset$ is an initial object in $\mathbf{C}$. Next let $f : Y \to X$ 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 $F_x : \mathbf{C} \to \mathbf{sets}$ 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 $h : Y \to Z$ 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 $\{x \in X : F_x(h) \text{ is not bijective}\}$ 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 isomorphismthat is only canonical 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 $\mathrm{id}_X : X \to X$. 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 $Y \coprod Z$ 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 $\mathrm{Mor}_{\mathbf{C}}(A, S)$ is the set of morphisms from A to X. To prove the claim, suppose $f, g : A \to X$ 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 $(A, a) \geqq (B, b)$ 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 $(A, a) \geqq (B, b)$ and $(B, b) \geqq (A, a)$ in I, with corresponding morphisms $f : A \to B$, $g : B \to A$, 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 $\geqq$ 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 $\mathrm{Mor}_{\mathbf{C}}(A, X)$ is commutative for any X, so there is a map

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

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

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

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

3.14 Galois objects.

Let A be connected. Then $\#\mathrm{Aut}_{\mathbf{C}}(A) \leqq \#\mathrm{Mor}_{\mathbf{C}}(A, A) \leqq F(A)$, 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 $\#\mathrm{Aut}_{\mathbf{C}}(A) \geqq \#F(A)$, 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 $f : A \to B$. By G3 and the connectedness of B the map $F(f) : F(A) \to F(B)$ is surjective, so $F(f)(a) = b$ for some $a \in F(A)$. Now $(A, a) \in J$, and $(A, a) \geqq (B, b)$, as required. Let $f' : A \to B$ 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 $(A, a) \geqq (B, b)$, with corresponding morphism $f : A \to B$. For each $\sigma \in \mathrm{Aut}_{\mathbf{C}}(A)$ there is a unique $\tau \in \mathrm{Aut}_{\mathbf{C}}(B)$ for which

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

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 $(A, a) \geqq (B, b)$ 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 $\mathbf{C} \to \pi\text{-}\mathbf{sets}$ that composed with the forgetful functor $\pi\text{-}\mathbf{sets} \to \mathbf{sets}$ 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 $f : A \to B$.

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 $f : A \to B$ induces a morphism $g : A/G \to B$. 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 $H : \mathbf{C} \to \pi$-**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 $\mathrm{Mor}_{\mathbf{C}}(X,Y) \to \mathrm{Mor}_{\mathbf{C}}(X,Y)$ 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 $\mathrm{Mor}_{\mathbf{C}}(X,Y)$. 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

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

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 $f : X \to Y$ 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 $H : \mathbf{C} \to \pi\text{-}\mathbf{sets}$ any equivalence that composed with the forgetful functor $F_1 : \pi\text{-}\mathbf{sets} \to \mathbf{sets}$ 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 $F' : \mathbf{C} \to \mathbf{sets}$ 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. 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 $g : A \to B$ 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 $(A, a) \geqq (B, b)$ in J_0. It follows easily that $(A, a) \geqq (B, b)$ in J_0 if and only if the corresponding elements $(A, a'), (B, b')$ of J_0' satisfy $(A, a') \geqq (B, b')$; but the morphisms $f, f' : A \to B$ 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

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

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

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

as above commute. These automorphisms induce an isomorphism $\lim_{\to J_0} \mathrm{Mor}_{\mathbf{C}}(A,-) \cong \lim_{\to J_0'} \mathrm{Mor}_{\mathbf{C}}(A,-)$, so $F \cong F'$. This proves (c).

Finally, we prove (d). Let $H' : \mathbf{C} \to \pi\text{-}\mathbf{sets}$ 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,* $F : \mathbf{C}' \to \mathbf{sets}$ *a fundamental functor and* $G : \mathbf{C} \to \mathbf{C}'$ *a functor such that* $F = F'G$ *is a fundamental functor for* $\mathbf{C}$. *Let* $H : \mathbf{C}' \to \pi\text{-}\mathbf{sets}$ *and* $H' : \mathbf{C}' \to \pi\ \mathbf{sets}$ *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* $G' : \pi\text{-}\mathbf{sets} \to \pi'\text{-}\mathbf{sets}$ *that endows a* π*-set with the* π'*-action induced by* $\pi' \to \pi$ *gives rise to a commutative diagram*

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

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, $f : X' \to X$ 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 $G : \mathbf{C} \to \mathbf{C}'$ 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 $s = S_D : E \to V$ and a *target* map $t = t_D : E \to V$; 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 $(h_v : X_v \to Y_v)_{v\in V}$ 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 $\Gamma : \mathbf{C} \to \mathbf{C}^D$ 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 $e \in A$, and mapping a morphism $h : X \to Y$ 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 on all D-diagrams in $\mathbf{C}$ if and only if the functor $\Gamma : \mathbf{C} \to \mathbf{C}^D$ has a *right adjoint* $\varprojlim : \mathbf{C}^D \to \mathbf{C}$, 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 $\varinjlim : \mathbf{C}^D \to \mathbf{C}$ 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 $\bullet \longrightarrow \bullet \longleftarrow \bullet$ 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 $f, g : X \to Y$ in $\mathbf{C}$ is a left limit of the D-diagram $f, g : X \rightrightarrows Y$, with $D = \curvearrowright$. We say that $\mathbf{C}$ has *equalizers* if it admits left limits over $D = \curvearrowright$. 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 V and E finite).

(a) Suppose that $\mathbf{C}$ satisfies G1 (see 3.1), and let $f, g : X \to Y$ 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 $X \coprod Y$ 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 $f : X \to Y$ be a morphism in a category $\mathbf{C}$. Prove that f is an epimorphism if and only if Y, together with $\mathrm{id}_Y : Y \to Y$ and $f : X \to Y$, 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 $f, g : X \to Y$ 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 $F : \mathrm{Hom}_A(X,Y) \to \mathrm{Hom}(F(X), F(Y))$ 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 $\bar{K}$. 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 $\bar{K}$-linearity to $A \otimes_K \bar{K}$. Prove that $(A \otimes_K \bar{K})^G \cong A^G \otimes_K \bar{K}$ and $\bar{K}$-algebras, and that A^G is a free separable K-algebra. [*Hint*: use a basis of $\bar{K}$ over K.]

(c) Let $f : A \to B$ 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 $F(A) = \mathrm{Alg}_K(A, \bar{K}) \cong \mathrm{Alg}_K(A, K_s)$; 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 $\{\sigma \in \mathrm{Aut}(F) : \sigma_X \text{ is the identity on } F(X)\}$, with X ranging over the objects of $\mathbf{C}$.

3.11 Let π be a profinite group, and F the fundamental 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 $\sigma_{\pi/\pi'} : F(\pi/\pi') \to F(\pi/\pi')$, 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 on 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 $H : \pi\text{-}\mathbf{sets} \to \mathrm{Aut}(F)\text{-}\mathbf{sets}$ defined in 3.4 is the identity functor.

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

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

3.14 Let X be a connected topological space, $\mathbf{C}$ the category of finite coverings of X, and $h : Y \to Z$ 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 $F : \mathbf{C} \to \mathbf{sets}$ be a functor such that axioms G1, G4, G6 are satisfied. Let further $f : Y \to X$ be a morphism in $\mathbf{C}$.

(a) Prove that f is a monomorphism if and only if the first projection $p_1 : Y \times_X Y \to Y$ 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 $(f_{ij} : S_i \to S_j)_{i,j\in I,\ i\leqq j}$ satisfying the conditions

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

Call $x \in S_i$ *equivalent* to $y \in S_j$ if there exists $k \in I$ with $k \geqq i$, $k \geqq j$ 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 mod n) to (m/n mod 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 aH 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 $G : \mathbf{C} \to \mathbf{C}'$ 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 $G' : \pi\text{-}\mathbf{sets} \to \pi'\text{-}\mathbf{sets}$ 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 p'-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 $F : \mathbf{C} \to \mathbf{sets}$ 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 $f : X \to A$ in $\mathbf{C}$, a morphism from $f : X \to A$ to $g : Y \to A$ in $\mathbf{C}_A$ being a morphism $h : X \to Y$ in $\mathbf{C}$ for which $f = gh$.

(a) Define the functor $F_a : \mathbf{C}_A \to \mathbf{sets}$ by sending $f : X \to A$ 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 $G : \mathbf{C} \to \mathbf{C}_A$ 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 $J : \mathbf{C}_A \to \mathbf{C}$ 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.