3
Infinitary Galois theory

Convention *In this chapter, all fields, rings and algebras we consider are commutative and have a unit.*

In this chapter, we develop Galois theory for an arbitrary Galois extension of fields $K \subseteq L$, not necessarily finite dimensional.

3.1 Finitary Galois subextensions

Given a Galois extension of fields $K \subseteq L$, we are interested in the intermediate field extensions $K \subseteq M \subseteq L$, with $K \subseteq M$ a finite dimensional Galois extension of fields. This is what we call a "finite dimensional Galois subextension" of $K \subseteq L$.

Proposition 3.1.1 *Let $K \subseteq L$ be a Galois extension of fields. Consider $l \in L$ with minimal polynomial $p(X) \in K[X]$, admitting in L the roots $l_1, \ldots, l_n$. Then $K \subseteq K(l_1, \ldots, l_n)$ is a finite dimensional Galois extension of fields.*

Proof $K(l_1, \ldots, l_n)$ is finite dimensional over K by proposition 2.1.10. It is the union, in the category of K-algebras, of the subalgebras $K(l_i)$, for all i. Each l_i admits $p(X)$ as minimal polynomial, thus by proposition 2.2.5

$$\begin{aligned}
&\#\mathsf{Hom}_K\big(K(l_i), K(l_1, \ldots, l_n)\big) \\
&\qquad = \#\mathsf{Hom}_K\left(\frac{K[X]}{\langle p(X)\rangle}, K(l_1, \ldots, l_n)\right) \\
&\qquad = \text{number of roots of } p(X) \text{ in } K(l_1, \ldots, l_n) \\
&\qquad = \text{degree of } p(X)
\end{aligned}$$

$$= \dim_K K(l_i).$$

This proves by theorem 2.3.3 that $K(l_1, \dots, l_n)$ splits $K(l_i)$. By lemma 2.3.5, $K(l_1, \dots, l_n)$ splits $K(l_1) \cup \cdots \cup K(l_n) = K(l_1, \dots, l_n)$, which proves by proposition 2.3.2 that $K \subseteq K(l_1, \dots, l_n)$ is a Galois extension. □

Proposition 3.1.2 *Let $K \subseteq L$ be a Galois extension of fields and $K \subseteq M \subseteq L$ an intermediate field extension, with M finite dimensional over K. Every K-homomorphism of fields $f\colon M \longrightarrow M$ extends to a K-homomorphism $g\colon L \longrightarrow L$.*

Proof We recall that a field L is algebraically closed when every polynomial in $L[X]$ has a root in L, thus by induction, factors in $L[X]$ as a product of polynomials of degree 1. We shall use freely the fact that every field K has an algebraic closure $\overline{K}$, which contains in particular all algebraic extensions of K. Moreover, every field homomorphism $f\colon K \longrightarrow M$ extends to a homomorphism $\overline{f}\colon \overline{K} \longrightarrow \overline{M}$ between the algebraic closures, and when f is an isomorphism, so is $\overline{f}$ (see [71]).

Using the previous notation, from the assumption we get an isomorphism $\overline{f}\colon \overline{M} \longrightarrow \overline{M}$ extending f. Since L is algebraic over K, we get $K \subseteq L \subseteq \overline{M}$ and it remains to prove that $\overline{f}(L) \subseteq L$. Given $l \in L$ with minimal polynomial $p(X) \in K[X]$, we have

$$p\big(\overline{f}(l)\big) = \overline{f}\big(p(l)\big) = \overline{f}(0) = 0$$

since f, and thus also $\overline{f}$, fix the coefficients of $p(X)$. Thus $\overline{f}(l)$ is a root of $p(X)$ and, since $K \subseteq L$ is a Galois extension, $\overline{f}(l) \in L$. □

Corollary 3.1.3 *Let $K \subseteq L$ be a Galois extension of fields. One has*

$$K = \big\{l \in L \big| \forall f \in \mathsf{Gal}\,[L : K] \quad f(l) = l\big\} = \mathsf{Fix}\,\big(\mathsf{Gal}\,[L : K]\big).$$

Proof If $l \notin K$, let $p(X) \in K[X]$ be its minimal polynomial, with roots $l_1, \dots, l_n$ in L. Moreover $K \subseteq K(l_1, \dots, l_n)$ is a Galois extension by proposition 3.1.1. Since $l \notin K$, $p(X)$ does not have degree 1 so that we can fix $l_i \neq l$. By proposition 1.3.4, there exists

$$f\colon K(l_1, \dots, l_n) \longrightarrow K(l_1, \dots, l_n)$$

such that $f(l) = l_i \neq l$. It remains to extend f to $g\colon L \longrightarrow L$ by proposition 3.1.2, which yields $g \in \mathsf{Gal}\,[L : K]$ such that $g(l) \neq l$. □

Proposition 3.1.4 *Let $K \subseteq L$ be a Galois extension of fields. The field L is the set-theoretical filtered union of the subextensions $K \subseteq M \subseteq L$ where $K \subseteq M$ is a finite dimensional Galois extension.*

Proof If $l \in L$ has minimal polynomial $p(X) \in K[X]$ with roots $l_1, \ldots, l_n$ in L, then by proposition 3.1.1,

$$l \in K(l_1, \ldots, l_n) \subseteq L$$

where $K \subseteq K(l_1, \ldots, l_n)$ is a finite dimensional Galois extension. The field L is thus indeed the set theoretical union of the finite dimensional Galois subextensions.

It remains to prove that this union is filtered. For this choose

$$K \subseteq M_1 \subseteq L, \quad K \subseteq M_2 \subseteq L$$

with $K \subseteq M_1$ and $K \subseteq M_2$ finite dimensional Galois extensions. The K-subalgebra $M_3 \subseteq L$ generated by M_1 and M_2 remains finite dimensional over K. Since $K \subseteq M_1$ is a Galois extension, the minimal polynomial of $l \in M_1$ factors in M_1, thus also in M_3, into distinct factors of degree 1; the same argument holds for M_2. This proves that M_3 splits both M_1 and M_2, thus M_3 splits M_3 by lemma 2.3.5. By proposition 2.3.2, this proves that $K \subset M_3$ is a Galois extension. □

Proposition 3.1.5 *Let $K \subseteq L$ be a Galois extension of fields. Suppose that L splits the K-algebra A. For every finite dimensional K-subalgebra $B \subseteq A$, there exists a finite dimensional Galois subextension $K \subseteq M \subseteq L$ which splits B.*

Proof The subalgebra B is generated over K by a finite number $b_1, \ldots, b_n$ of elements. Each of these elements b_i has a minimal polynomial $p_i(X) \in K[X]$, admitting in L the roots $l_1^i, \ldots, l_{m_i}^i$. The extension

$$M_i = K(l_1^i, \ldots, l_{m_i}^i)$$

is a finite dimensional Galois extension by proposition 3.1.1. By proposition 3.1.4, there exists a finite dimensional Galois extension M containing $M_1, \ldots, M_n$. By theorem 2.3.3 this extension M splits each $K(b_i) \subseteq B$, since

$$\begin{aligned} \#\mathsf{Hom}_K\big(K(b_i), M\big) &= \#\mathsf{Hom}_K\left(\frac{K[X]}{\langle p_i(X)\rangle}, M\right) \\ &= \text{number of roots of } p_i(X) \text{ in } M \end{aligned}$$

$$\begin{aligned} &= \text{degree of } p_i(X) \\ &= \dim_K K(b_i) \end{aligned}$$

by proposition 2.2.5. By lemma 2.3.5, M splits $K(b_1) \cup \cdots \cup K(b_n) = B$. □

3.2 Infinitary Galois groups

The Galois group of an arbitrary Galois extension $K \subseteq L$ will be a topological group, which will turn out to be discrete when the extension is finite dimensional.

Proposition 3.2.1 *Let $K \subseteq L$ be a Galois extension of fields. In the category of groups,*

$$\mathsf{Gal}\,[L:K] = \lim_M \mathsf{Gal}\,[M:K]$$

where M runs through the poset of finite dimensional Galois extensions $K \subseteq M \subseteq L$ and, for $M \subseteq M'$, the corresponding morphism

$$\mathsf{Gal}\,[M':K] \longrightarrow \mathsf{Gal}\,[M:K], \quad f \mapsto f|_M$$

is the restriction.

Proof Let us recall that given a K-homomorphism $f\colon M' \longrightarrow M'$ and an element $l \in M$, for $M \subseteq M'$, this element l has a minimal polynomial $p(X) \in K[X]$ and

$$p\big(f(l)\big) = f\big(p(l)\big) = f(0) = 0$$

since f fixes the coefficients of $p(X)$. Thus $f(l)$ is a root of $p(X)$ and therefore $f(l) \in M$ since $K \subseteq M$ is a Galois extension. This proves that f indeed restricts to a K-automorphism of M. The same argument holds replacing M' by L, which provides the projections

$$p_M\colon \mathsf{Gal}\,[L:K] \longrightarrow \mathsf{Gal}\,[M:K]$$

which are thus the restrictions to M. They clearly form a cone, since all morphisms involved are restrictions.

To prove that this cone is a limit one, it remains to choose a compatible family $f_M \in \mathsf{Gal}\,[M:K]$ and show it glues uniquely as an element $f \in \mathsf{Gal}\,[L:K]$. This follows at once from proposition 3.1.4.

Another way of writing the same proof is to consider the isomorphisms

$$\mathsf{Gal}\,[L:K] \;=\; \mathsf{Hom}_K(L,L)$$

$$\begin{aligned} &= \mathsf{Hom}_K(\mathsf{colim}_M M, L) \\ &\cong \mathsf{lim}_M \mathsf{Hom}_K(M, L) \\ &\cong \mathsf{lim}_M \mathsf{Hom}_K(M, M) \\ &= \mathsf{lim}_M \mathsf{Gal}\,[M : K], \end{aligned}$$

using once more the argument that a homomorphisms $M \longrightarrow L$ factors through M, by the Galois property of the extension. □

Definition 3.2.2 Let $K \subseteq L$ be a Galois field extension. The topological Galois group of this extension is the group $\mathsf{Gal}\,[L : K]$ provided with the initial topology for all the projections

$$\mathsf{Gal}\,[L : K] \cong \mathsf{lim}_M \mathsf{Gal}\,[M : K] \longrightarrow \mathsf{Gal}\,[M : K], \quad f \mapsto f|_M,$$

where M runs through the finite dimensional Galois subextensions $K \subseteq M \subseteq L$ and each $\mathsf{Gal}\,[M : K]$ is provided with the discrete topology.

By theorem 1.4.5, all the groups $\mathsf{Gal}\,[M : K]$ in the above definition are finite; by proposition 3.1.4, the diagram constituted by these $\mathsf{Gal}\,[M : K]$ is cofiltered. The topological Galois group is thus a cofiltered projective limit, in the category of topological groups, of a diagram constituted of discrete finite groups: such a group is called a *profinite* group. We shall first study its topology further.

Lemma 3.2.3 *Let $K \subseteq L$ be a Galois field extension. The subgroups $\mathsf{Gal}\,[L : M] \subseteq \mathsf{Gal}\,[L : K]$, for $K \subseteq M \subseteq L$ a finite dimensional Galois subextension, constitute a fundamental system of open and closed neighbourhoods of id_L.*

Proof A fundamental open subset of $\mathsf{Gal}\,[L : K]$ has the form

$$U = p_{M_1}^{-1}(X_1) \cap \cdots \cap p_{M_n}^{-1}(X_n)$$

where $X_i \subseteq \mathsf{Gal}\,[M_i : K]$ is an arbitrary (open) subset and p_{M_i} is the corresponding projection. Notice that U is both open and closed since so is each X_i. An arbitrary open subset of $\mathsf{Gal}\,[L : K]$ is a union of such fundamental open subsets. For U being a fundamental neighbourhood of id_L, we must have $1_{M_i} = p_{M_i}(1_L) \in X_i$ for all $i = 1, \ldots, n$. In that case U contains

$$V = p_{M_1}^{-1}\left(\{1_{M_1}\}\right) \cap \cdots \cap p_{M_n}^{-1}\left(\{1_{M_n}\}\right)$$

which is still an open and closed neighbourhood of id_L. Observe that

$$\begin{aligned} f \in V &\Leftrightarrow \forall i = 1, \dots, n \quad f|_{M_i} = \mathsf{id}_{M_i} \\ &\Leftrightarrow f|_M = \mathsf{id}_M \end{aligned}$$

where M is the subfield of L generated by $M_1, \dots, M_n$. Then $K \subseteq M$ is again a finite dimensional Galois extension, as observed in the proof of proposition 3.1.4. We have thus proved that $V = \mathsf{Gal}\,[L : M]$. □

Lemma 3.2.4 *Let $K \subseteq L$ be a Galois extension of fields. The topology of the Galois group $\mathsf{Gal}\,[L : K]$ is the initial topology for all the maps*

$$\mathsf{ev}_l \colon \mathsf{Gal}\,[L : K] \longrightarrow L, \quad f \mapsto f(l)$$

where l runs through L and the codomain L of ev_l is provided with the discrete topology.

Proof The topology described in this lemma is also called the topology of pointwise convergence on $\mathsf{Gal}\,[L : K]$.

Let us prove first that each map ev_l is continuous. Since L is provided with the discrete topology, it suffices to prove that the inverse image of each point is open. For this, let us fix $l, l_0 \in L$.

$$\mathsf{ev}_l^{-1}\big(\{l_0\}\big) = \big\{f \in \mathsf{Gal}\,[L : K] \big| f(l) = l_0\big\}.$$

If this set is empty, it is open. Otherwise, by proposition 3.1.4, we choose a finite dimensional Galois subextension $K \subseteq M \subseteq L$ containing l and l_0. Let us write $p(X) \in K[X]$ for the minimal polynomial of l. Choosing $f \in \mathsf{ev}_l^{-1}\big(\{l_0\}\big)$,

$$p(l_0) = p\big(f(l)\big) = f\big(p(l)\big) = f(0) = 0$$

and thus l_0 is a root of $p(X)$. By proposition 1.3.4, there exists a K-automorphism $g \colon M \longrightarrow M$ such that $g(l) = l_0$. Therefore

$$\begin{aligned} \mathsf{ev}_l^{-1}\big(\{l_0\}\big) &= \big\{f \in \mathsf{Gal}\,[L : K] \big| f(l) = l_0\big\} \\ &= \big\{f \in \mathsf{Gal}\,[L : K] \big| f(l) = g(l)\big\} \\ &= \big\{f \in \mathsf{Gal}\,[L : K] \big| (g^{-1} \circ f|_M)(l) = l\big\}. \end{aligned}$$

Consider the pullback

$$\begin{array}{ccc} P & \longrightarrow & \mathsf{Gal}\,[M : K(l)] \\ \downarrow & & \downarrow \\ \mathsf{Gal}\,[L : K] & \xrightarrow[p_M]{} & \mathsf{Gal}\,[M : K] \end{array}$$

One has

$$P = \big\{h \in \mathsf{Gal}\,[L : K] \big| h|_M(l) = l\big\}$$

and therefore

$$\begin{aligned} \mathsf{ev}_l^{-1}\big(\{l_0\}\big) &= \big\{f \in \mathsf{Gal}\,[L : K] \big| g^{-1} \circ f \in P\big\} \\ &= \big\{g \circ h \big| h \in P\big\} \end{aligned}$$

which is the image of the subset $P \subseteq \mathsf{Gal}\,[L : K]$ by the homeomorphism

$$\mathsf{Gal}\,[L : K] \longrightarrow \mathsf{Gal}\,[L : K], \quad h \mapsto g \circ h$$

inherited from the topological group structure. Since $\mathsf{Gal}\,[M : K]$ is provided with the discrete topology, $\mathsf{Gal}\,[M : K(l)]$ is both open and closed in $\mathsf{Gal}\,[M : K]$. Since p_M is continuous, P too is open and closed in $\mathsf{Gal}\,[L : K]$. Via the homeomorphism we have exhibited, this implies that $\mathsf{ev}_l^{-1}\big(\{l_0\}\big)$ is open and closed as well.

The topology of lemma 3.2.4 is thus contained in that of lemma 3.2.3. Conversely, it suffices to prove that the fundamental open neighbourhoods $\mathsf{Gal}\,[L : M]$ of id_L in lemma 3.2.3 contain a neighbourhood of id_L for the topology of lemma 3.2.4. Indeed, M is generated by finitely many elements $l_1, \ldots, l_n$. Given $f \in \mathsf{Gal}\,[L : K]$, the condition $f \in \mathsf{Gal}\,[L : M]$ reduces to $f(l_1) = l_1, \ldots, f(l_n) = l_n$. This is equivalent to

$$f \in \mathsf{ev}_{l_1}^{-1}(l_1) \cap \cdots \cap \mathsf{ev}_{l_n}^{-1}(l_n)$$

which is a neighbourhood of id_L for the topology of lemma 3.2.4, since so is each $\mathsf{ev}_{l_i}^{-1}(l_i)$. □

Corollary 3.2.5 *Let $K \subseteq L$ be a Galois extension of fields. For every $f \in \mathsf{Gal}\,[L : K]$, the subsets*

$$V_M(f) = \big\{g \in \mathsf{Gal}\,[L : K] \big| g|_M = f|_M\big\} \subseteq \mathsf{Gal}\,[L : K]$$

for $K \subseteq M \subseteq L$ running through the arbitrary finite dimensional subextensions constitute a fundamental system of neighbourhoods of f.

Proof If M is generated by $l_1, \dots, l_n$,

$$\begin{aligned} V_M(f) &= \{g \in \mathsf{Gal}[L:K] | g(l_1) = f(l_1), \cdots, g(l_n) = f(l_n)\} \\ &= \mathsf{ev}_{l_1}^{-1}(f(l_1)) \cap \cdots \cap \mathsf{ev}_{l_n}^{-1}(f(l_n)) \end{aligned}$$

which is a neighbourhod of f for the topology of lemma 3.2.4.

Conversely, every neighbourhood V of f contains by lemma 3.2.4 a neighbourhood of the form

$$f \in \mathsf{ev}_{a_1}^{-1}(b_1) \cap \cdots \cap \mathsf{ev}_{a_m}^{-1}(b_m)$$

where $a_i, b_i \in L$. One has $f(a_i) = b_i$ and therefore

$$\begin{aligned} &\mathsf{ev}_{a_1}^{-1}(b_1) \cap \cdots \cap \mathsf{ev}_{a_m}^{-1}(b_m) \\ &\quad = \{g \in \mathsf{Gal}[L:K] | g(a_1) = b_1, \dots, g(a_m) = b_m\} \\ &\quad = \{g \in \mathsf{Gal}[L:K] | g(a_1) = f(a_1), \dots, g(a_m) = f(a_m)\} \\ &\quad = V_{K(l_1,\dots,l_n)}(f) \end{aligned}$$

which concludes the proof. □

Corollary 3.2.6 *Let $K \subseteq L$ be a Galois extension of fields. Given a subset $U \subseteq \mathsf{Gal}[L:K]$, its closure is given by*

$$\overline{U} = \left\{ f \in \mathsf{Gal}[L:K] \;\middle|\; \begin{array}{l} \forall M \quad K \subseteq M \subseteq L \text{ with } K \subseteq M \\ \quad \text{finite dimensional Galois extension} \\ \exists g \in U \quad g|_M = f|_M \end{array} \right\}.$$

Proof With shortened notation,

$$\begin{aligned} \overline{U} &= \{f | \forall M \;\; \dim_K(M) \text{ finite}, \;\; V_M(f) \cap U \neq \emptyset\} \\ &= \{f | \forall M \;\; \dim_K(M) \text{ finite}, \;\; \exists g \in U \;\; g|_M = f|_M\} \\ &= \{f | \forall M \;\; K \subseteq M \text{ Galois extension}, \;\; \dim_K(M) \text{ finite}, \\ &\qquad \exists g \in U \;\; g|_M = f|_M\}. \end{aligned}$$

The first equality follows from corollary 3.2.5, the second one from the definition of $V_M(f)$ and the third one, via proposition 3.1.4, from the fact that every finite dimensional subextension is contained in a finite dimensional Galois subextension. □

3.3 Classical infinitary Galois theory

We shall now generalize theorem 1.4.5 to the case of an arbitrary Galois extension $K \subseteq L$. The Galois group $\mathsf{Gal}[L:K]$ is always considered as provided with its topology described in section 3.2.

Proposition 3.3.1 *Let $K \subseteq L$ be a Galois extension of fields. Let $K \subseteq M \subseteq L$ be a finite dimensional intermediate Galois extension. The canonical restriction morphism of definition 3.2.2*

$$p_M : \mathsf{Gal}[L:K] \longrightarrow \mathsf{Gal}[M:K]; f \mapsto f|_M$$

is a topological quotient for the equivalence relation determined by the subgroup $\mathsf{Gal}[L:M] \subseteq \mathsf{Gal}[L:K]$.

Proof By proposition 3.1.2, the restriction map is surjective. One observes at once that

$$\begin{aligned} p_M(f) = p_M(g) &\Leftrightarrow f|_M = g|_M \\ &\Leftrightarrow \forall m \in M \quad f(m) = g(m) \\ &\Leftrightarrow \forall m \in M \quad m = (f^{-1} \circ g)(m) \\ &\Leftrightarrow f^{-1} \circ g \in \mathsf{Gal}[L:M] \end{aligned}$$

which proves that the set theoretical quotient is induced by the subgroup $\mathsf{Gal}[L:K]$.

The quotient toplogy on $\mathsf{Gal}[M:K]$ is the finest one making continuous the surjection p_M. Since the discrete topology makes p_M continuous, it is necessarily the finest one with that property. □

Proposition 3.3.2 *Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every finite dimensional intermediate extension $K \subseteq M \subseteq L$,*

$$\mathsf{Gal}[L:M] = \left\{ f \in \mathsf{Gal}[L:K] \middle| \forall m \in M \quad f(m) = m \right\}$$

is an open and closed subgroup of $\mathsf{Gal}[L:K]$.

Proof We refer to proposition 3.1.4 and consider

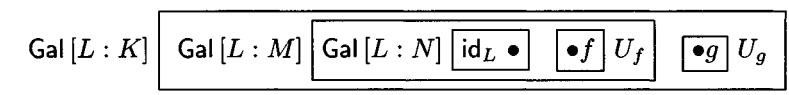
$$K \subseteq M \subseteq N \subseteq L, \quad \dim_K N \text{ finite}, \quad K \subseteq N \text{ Galois extension.}$$

It follows at once that

$$\mathsf{id}_L \in \mathsf{Gal}[L:N] \subseteq \mathsf{Gal}[L:M]$$

and by lemma 3.2.3, we know that $\mathsf{Gal}[L : N]$ is an open and closed neighbourhood of id_L. This forces the conclusion, by elementary properties of topological groups, namely: every subgroup of a topological group containing an open subgroup is itself open, and every open subgroup is closed.

Indeed, in the special case we are handling here, for every $f \in \mathsf{Gal}[L : M]$, multiplication by f is a homeomorphism mapping id_L onto f. This homeomorphism also maps $\mathsf{Gal}[L : N]$ onto some open and closed subset $U_f \subseteq \mathsf{Gal}[L : M]$, because $\mathsf{Gal}[L : M]$ is a subgroup. Thus $\mathsf{Gal}[L : M]$ is a join of open subsets and therefore is open. Now if $g \notin \mathsf{Gal}[L : M]$, one must have $U_g \cap \mathsf{Gal}[L : M] = \emptyset$; otherwise, choosing h in this intersection, one would have $h = g \circ h'$ with $h, h' \in \mathsf{Gal}[L : M]$, thus $g \in \mathsf{Gal}[L : M]$. This proves that the set theoretical complement of $\mathsf{Gal}[L : M]$ is open.



□

Corollary 3.3.3 *Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every arbitrary intermediate extension $K \subseteq M \subseteq L$,*

$$\mathsf{Gal}[L : M] = \left\{ f \in \mathsf{Gal}[L : K] \middle| \forall m \in M \quad f(m) = m \right\}$$

is a closed subgroup of $\mathsf{Gal}[L : K]$.

Proof One has

$$\begin{aligned} \mathsf{Gal}[L : M] &= \left\{ f \in \mathsf{Gal}[L : K] \middle| \forall m \in M \quad f(m) = m \right\} \\ &= \left\{ f \in \mathsf{Gal}[L : K] \middle| \forall m \in M \quad f \in \mathsf{Gal}[L : K(m)] \right\} \\ &= \bigcap_{m \in M} \mathsf{Gal}[L : K(m)]. \end{aligned}$$

We recall that $K(m)$ is finite dimensional over K (see proposition 1.1.4). This forces the conclusion by proposition 3.3.2 and the fact that an intersection of closed subsets is closed. □

Lemma 3.3.4 *Let $K \subseteq L$ be an arbitrary Galois extension of fields and $G \subseteq \mathsf{Gal}[L : K]$ a closed subgroup. Moreover, let us suppose that*

$$K = \mathsf{Fix}(G) = \left\{ l \in L \middle| \forall g \in G \quad g(l) = l \right\}.$$

In these conditions, $G = \mathsf{Gal}[L : K]$.

Proof Let us first consider the subgroup

$$H_M = \{f|_M | f \in G\} \subseteq \mathsf{Gal}\,[M : K]$$

for every finite dimensional Galois extension $K \subseteq M \subseteq L$. By assumption,

$$\begin{aligned} \mathsf{Fix}\,(H_M) &= \{m \in M | \forall h \in H_M \quad h(m) = m\} \\ &= \{m \in M | \forall f \in G \quad f(m) = m\} \\ &= K. \end{aligned}$$

Applying the classical Galois theorem (see 1.4.5)

$$H_M = \mathsf{Gal}\,\big[M : \mathsf{Fix}\,(H_M)\big] = \mathsf{Gal}\,[M : K].$$

In other terms

$$\forall f \in \mathsf{Gal}\,[L : K] \quad \forall M \; K \subseteq M \subseteq L \text{ Galois extension}, \quad \dim_K M \text{ finite}, \quad f|_M \in H_M$$

or also, with shortened notation,

$$\forall f \in \mathsf{Gal}\,[L : K] \quad \forall M \quad \exists g \in G \quad g|_M = f|_M.$$

By corollary 3.2.6, this reduces to

$$\forall f \in \mathsf{Gal}\,[L : K] \quad f \in \overline{G},$$

that is, finally, $\mathsf{Gal}\,[L : K] = \overline{G}$. Thus $G = \mathsf{Gal}\,[L : K]$ since G is closed. □

Theorem 3.3.5 (Galois theorem) *Let $K \subseteq L$ be an arbitrary Galois extension of fields. The correspondences*

$$\begin{aligned} K \subseteq M \subseteq L &\mapsto \mathsf{Gal}\,[L : M], \\ G \subseteq \mathsf{Gal}\,[L : K] &\mapsto \mathsf{Fix}\,(G) \end{aligned}$$

induce a contravariant isomorphism between the lattice of arbitrary extensions $K \subseteq M \subseteq L$ and the lattice of closed subgroups $G \subseteq \mathsf{Gal}\,[L : K]$.

Proof By corollary 3.3.3, $\mathsf{Gal}\,[L : M]$ is a closed subgroup. On the other hand since the elements of G are field homomorphisms, it follows at once that $\mathsf{Fix}\,(G)$ is a field.

Let us consider a closed subgroup $G \subseteq \mathsf{Gal}[L : K]$. Since $K \subseteq L$ is a Galois extension, $\mathsf{Fix}(G) \subseteq L$ is a Galois extension as well (see 1.4.2). On the other hand one has trivially

$$G \subseteq \mathsf{Gal}[L : \mathsf{Fix}(G)] \subseteq \mathsf{Gal}[L : K]$$

with again G closed by assumption. Lemma 3.3.4 applies with $\mathsf{Fix}(G)$ instead of K, proving that $G = \mathsf{Gal}[L : \mathsf{Fix}(G)]$.

Conversely, consider an intermediate extension $K \subseteq M \subseteq L$. Trivially,

$$M \subseteq \mathsf{Fix}\big(\mathsf{Gal}[L : M]\big) \subseteq L$$

and $M \subseteq L$ is a Galois extension, since so is $K \subseteq L$ (see 1.4.2). Given $l \in \mathsf{Fix}\big(\mathsf{Gal}[L : M]\big)$, consider by proposition 3.1.4 a finite dimensional Galois extension $M \subseteq M'$, with

$$M \subseteq M' \subseteq L, \quad l \in M'.$$

By proposition 3.1.2, every M-automorphism of M' is the restriction of an M-automorphism of L. Since l is fixed by all elements of $\mathsf{Gal}[L : M]$, it is thus also fixed by all elements of $\mathsf{Gal}[M' : M]$. Again the classical Galois theorem (see 1.4.5) implies

$$l \in \mathsf{Fix}\big(\mathsf{Gal}[M' : M]\big) = M. \qquad \square$$

3.4 Profinite topological spaces

To treat Grothendieck infinitary Galois theory for fields, it is useful to study more extensively the profinite topological spaces, already mentioned after definition 3.2.2, in the special case of profinite groups.

Definition 3.4.1 A topological space is profinite when it is the projective limit, indexed by a cofiltered poset, of finite discrete topological spaces.

In fact, the requirement that the limit is indexed by a cofiltered poset can equivalently be omitted in definition 3.4.1, as shown by corollary 3.4.8.

Definition 3.4.2 A topological space is totally disconnected when two distinct points admit disjoint neighbourhoods which are both open and closed. Equivalently,

$$x \neq y \Rightarrow \exists U \subseteq X, \quad U \text{ open and closed}, \quad x \in U, \quad y \notin U.$$

In particular, a totally disconnected space is a Hausdorff space. The terminology "totally disconnected" is justified by corollary 5.7.10.

Lemma 3.4.3 *In the category of topological spaces and continuous mappings, a projective limit of totally disconnected spaces is again totally disconnected.*

Proof We recall that given a diagram $\mathcal{D}$ of topological spaces, its projective limit L is the space

$$L = \left\{ (x_X)_{X\in\mathcal{D}} \in \prod_{X\in\mathcal{D}} X \;\middle|\; \forall f \in \mathcal{D},\quad f\colon X \longrightarrow Y,\quad f(x_X) = x_Y \right\}$$

where the topology of the product induces that of L. In other words, the limit is given by the pullback below, where as above f is a morphism $f\colon X \longrightarrow Y$. This diagram presents the limit as an inverse image of a diagonal:

$$\begin{array}{ccc} L & \longrightarrow & \prod_{f\in\mathcal{D}} Y \\ \downarrow & & \downarrow \Delta \\ \prod_{X\in\mathcal{D}} X & \xrightarrow[\alpha]{} & \left(\prod_{f\in\mathcal{D}} Y\right) \times \left(\prod_{f\in\mathcal{D}} Y\right) \cong \prod_{f\in\mathcal{D}} (Y \times Y) \end{array}$$

where α is defined by

$$\alpha\big((x_X)_{X\in\mathcal{D}}\big) = \big(f(x_X), x_Y\big)_{f\in\mathcal{D}}.$$

First, a topological product $\prod_{i\in I} X_i$ of totally disconnected spaces is totally disconnected. Indeed, if $(x_i)_{i\in I} \neq (y_i)_{i\in I}$, there exists an index i_0 with $x_{i_0} \neq y_{i_0}$. In X_{i_0} one can find disjoint open and closed neighbourhoods $x_{i_0} \in U_{i_0}$, $y_{i_0} \in V_{i_0}$. Putting $U_i = X_i = V_i$ for $i \neq i_0$, we get two disjoint open and closed neighbourhoods

$$(x_i)_{i\in I} \in \prod_{i\in I} U_i, \quad (y_i)_{i\in I} \in \prod_{i\in I} V_i,$$

which proves the total disconnectedness of $\prod_{i\in I} X_i$. On the other hand it is immediate that a subspace of a totally disconnected space is itself totally disconnected. □

The following corollary is interesting, even if not useful in this chapter.

Corollary 3.4.4 *The category of totally disconnected spaces is reflective both in the category of topological spaces and in the category of Hausdorff spaces.*

Proof The proof of lemma 3.4.3 applies to show that a projective limit of Hausdorff spaces is again Hausdorff: it suffices to work with arbitrary neighbourhoods instead of open and closed ones. Thus the category of totally disconnected spaces is closed under projective limits both in the category of topological and in that of Hausdorff spaces. In particular, monomorphisms of totally disconnected spaces are continuous injections and therefore the category is well-powered.

On the other hand the discrete two point space is trivially totally disconnected; it is in fact a cogenerator. Indeed given $x \neq y$ in X, we can choose an open and closed subset $U \subseteq X$, with $x \in U$ and $y \notin U$. We consider the equivalence relation $u \sim v$ when $u, v \in U$ or $u, v \notin U$. The topological quotient $q\colon X \twoheadrightarrow X/\sim$ is homeomorphic to the discrete two point space and $q(x) \neq q(y)$. We conclude the proof by the special adjoint functor theorem (see [29]). □

Lemma 3.4.5 *A projective limit of compact and totally disconnected spaces is again compact and totally disconnected.*

Proof By lemma 3.4.3, it suffices to prove that a projective limit of compact Hausdorff spaces is compact Hausdorff. By the Tychonoff theorem, a product of compact Hausdorff spaces is compact. Now in the diagram of lemma 3.4.3, the diagonal is closed because the spaces are Hausdorff, thus the limit L is closed in the product, which is compact Hausdorff; thus L is compact Hausdorff.

A more direct argument is the fact that the category of compact Hausdorff spaces is reflective in that of all topological spaces: the reflection is the Stone–Cĕch compactification. □

Again the following corollary is interesting, even if not immediately useful for our purpose. Part of it will be studied more intensively in section 5.7 and in particular in proposition 5.7.12.

Corollary 3.4.6 *The category of compact and totally disconnected spaces is reflective in the categories of compact Hausdorff spaces, totally disconnected spaces, Hausdorff spaces and topological spaces.*

Proof The discrete two point space is compact and totally disconnected. So the proof of corollary 3.4.4 applies. □

Theorem 3.4.7 *A topological space is profinite if and only if it is compact and totally disconnected.*

Proof Every finite discrete space is compact and totally disconnected, thus every projective limit of finite discrete spaces is still compact and totally disconnected by lemma 3.4.5.

Conversely, let X be compact and totally disconnected. We consider the poset $\mathcal{R}$ of all equivalence relations R on X such that the topological quotient X/R is discrete and finite; the ordering is inclusion. We write $[x]_R$ for the R-equivalence class of $x \in X$. We prove first the cofilteredness of $\mathcal{R}$. Let $R, S \in \mathcal{R}$ correspond respectively to the partitions $X = V_1 \cup \cdots \cup V_n$ and $X = W_1 \cup \cdots \cup W_m$. Let T be the equivalence relation corresponding to the partition

$$X = \bigcup_{1 \leq i \leq n,\ 1 \leq j \leq m} V_i \cap W_j.$$

Trivially $T \subseteq R$ and $T \subseteq S$ and the quotient X/T is finite. Since X/R and X/S are discrete, all V_i and W_j are both open and closed in X. Therefore each $V_i \cap W_j$ is open and closed in X and X/T is discrete as well. This proves the cofilteredness of $\mathcal{R}$.

When $R \subseteq S$ in $\mathcal{R}$, we get a factorization $X/R \longrightarrow X/S$ between the corresponding quotients and we shall prove that $X \cong \mathsf{lim}_{R \in \mathcal{R}} X/R$. To achieve this, we consider the canonical factorization

$$\lambda \colon X \longrightarrow \lim_{R \in \mathcal{R}} X/R, \quad x \mapsto \left([x]_R\right)_{R \in \mathcal{R}};$$

we must prove this is a homeomorphism. But X is compact Hausdorff and totally disconnected by assumption, and the same holds for $\mathsf{lim}_{R \in \mathcal{R}}$ by lemma 3.4.5. Since the spaces are compact Hausdorff, it suffices to prove that λ is bijective. But again by compactness and Hausdorffness, $\lambda(X)$ is compact, thus closed in $\mathsf{lim}_{R \in \mathcal{R}}$. It suffices therefore to prove that λ is injective and $\lambda(X)$ is dense.

To prove the injectivity, consider $x \neq y$ in X and $U \subseteq X$ open and closed, with $x \in U$ and $y \notin U$. The topological quotient X/U is the discrete two point space, thus the corresponding equivalence relation R is in $\mathcal{R}$ and, of course, $[x]_R \neq [y]_R$ since $x \in U$ and $y \notin U$. Therefore $\lambda(x) \neq \lambda(y)$.

To prove the density of $\lambda(X)$, let us fix an element $\left([x_R]_R\right)_{R \in \mathcal{R}}$ in $\mathsf{lim}_{R \in \mathcal{R}} X/R$. For every finite choice $R_1, \ldots, R_n$ in $\mathcal{R}$,

$$U_{R_1, \ldots, R_n} = \left\{ \left([y_R]_R\right)_{R \in \mathcal{R}} \middle| \forall i = 1, \ldots, n \quad \left[x_{R_i}\right]_{R_i} = \left[y_{R_i}\right]_{R_i} \right\}$$

is a neighbourhood of $\left([x_R]_R\right)_{R\in\mathcal{R}}$ in $\lim_{R\in\mathcal{R}} X/R$ since it can be written

$$U_{R_1,\dots,R_n} = p_{R_1}^{-1}\left([x_{R_1}]_{R_1}\right) \cap \cdots \cap p_{R_n}^{-1}\left([x_{R_n}]_{R_n}\right)$$

where the p_{R_i} are the canonical projections of the limit. The subsets $U_{R_1,\dots,R_n}$ even constitute a fundamental system of neighbourhoods of $\left([x_R]_R\right)_{R\in\mathcal{R}}$, since every elementary neighbourhood of this point has the form

$$V = p_{R_1}^{-1}(V_1) \cap \cdots \cap p_{R_n}^{-1}(V_n)$$

for some finite family $R_1,\dots,R_n$ in $\mathcal{R}$ and subsets $V_i \subseteq X/R_i$ such that $[x_{R_i}]_{R_i} \in V_i$. Thus such a V indeed contains $U_{R_1,\dots,R_n}$. Now for each choice $R_1,\dots,R_n$ in $\mathcal{R}$, we can choose $R_0 \in \mathcal{R}$ with $R_0 \subseteq R_i$ for each $i = 1,\dots,n$, by cofilteredness of $\mathcal{R}$. For each index i, the relation $R_0 \subseteq R_i$ and the compatibility of the family $\left([x_R]_R\right)_{R\in\mathcal{R}}$ imply $\left[x_{R_i}\right]_{R_i} = [x_{R_0}]_{R_i}$. This proves that

$$\lambda(x_{R_0}) = \left(\left[x_{R_0}\right]_R\right)_{R\in\mathcal{R}} \in U_{R_1,\dots,R_n}.$$

Every fundamental neighbourhood $U_{R_1,\dots,R_n}$ of $\left([x_R]_R\right)_{R\in\mathcal{R}}$ thus meets $\lambda(X)$, proving that $\lambda(X)$ is dense. □

Corollary 3.4.8 *A topological space is profinite when it is homeomorphic to a projective limit of finite discrete spaces.*

Proof Finite discrete spaces are compact and totally disconnected; thus a projective limit of finite discrete spaces is compact and totally disconnected (see 3.4.5) and therefore profinite (see 3.4.7). □

Corollary 3.4.9 *For a compact Hausdorff space X, the following conditions are equivalent:*

(i) *X is profinite;*
(ii) *the topology of X has a basis constituted of clopens (= simultaneously closed and open subsets);*
(iii) *X is totally disconnected.*

Proof (i) $\Leftrightarrow$ (iii) is part of theorem 3.4.7 and (ii) $\Rightarrow$ (iii) is obvious. Now assume (iii). The set of clopens in X is closed under finite intersections, and it suffices to prove that an open subset $U \subseteq X$ is a union of clopens. Choosing $x \in U$, we shall prove the existence of a clopen V such that $x \in V \subseteq U$, which will yield the result. For each $y \notin U$, choose a clopen

V_y such that $x \in V_y$ and $y \notin V_y$, thus $y \in \mathsf{C}V_y$, where C indicates the set-theoretical complement. The clopens $\mathsf{C}V_y$ cover the compact subset $\mathsf{C}U$, thus a finite number of them already covers $\mathsf{C}U$. But

$$\mathsf{C}U \subseteq \mathsf{C}V_{y_1} \cup \cdots \cup \mathsf{C}V_{y_n}$$

implies

$$x \in V_{y_1} \cap \cdots \cap V_{y_n} \subseteq U$$

with $V = V_{y_1} \cap \cdots \cap V_{y_n}$ a clopen. □

Lemma 3.4.10 *Let $X = \lim_{i\in I} X_i$ be a profinite space, presented as cofiltered limit of finite discrete spaces X_i. The following conditions are equivalent:*

(i) *X is not empty;*
(ii) *for each index $i \in I$, X_i is not empty.*

Proof The existence of the canonical projection $p_i : X \longrightarrow X_i$ of the limit forces (i) ⇒ (ii).

Conversely, consider the product $\prod_{i\in I} X_i$ which is a non empty compact Hausdorff space by the Tychonoff theorem. For each fixed index $k \in I$,

$$C_k = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \,\middle|\, \forall i \geq k \;\; x_i = f_{ki}(x_k) \right\}$$

where $f_{ki} : X_k \longrightarrow X_i$ is the morphism of the diagram corresponding to $k \leq i$. Each subset C_k is closed as intersection of the subsets

$$C_{k,j} = \left\{ (x_i)_{i\in I} \middle| x_j = f_{kj}(x_k) \right\}, \quad j \geq k,$$

which are themselves closed, as inverse images of the diagonal by the continuous maps

$$X \xrightarrow{\begin{pmatrix} p_j \\ f_{kj} \circ p_k \end{pmatrix}} X_j \times X_j, \quad x \mapsto \big(x_j, f_{kj}(x_k)\big).$$

Each C_k is non empty; indeed choosing an arbitrary $x \in X_k$, it suffices to put $x_i = f_{ki}(x)$ for $i \geq k$ and $x_i \in X_i$ arbitrary for the other indices; it follows at once that this family $(x_i)_{i\in I}$ is in C_k. If $k \leq l$, one has $C_k \subseteq C_l$ and therefore the family $(C_k)_{k\in I}$ is cofiltered, because so is I.

Since in the compact Hausdorff space $\prod_{i\in I} X_i$, a cofiltered intersection of non empty closed subsets is again non empty, we deduce that

$$X = \lim_{i\in I} X_i = \bigcap_{k\in I} C_k$$

is non empty. □

Lemma 3.4.11 *Let $X = \lim_{i\in I} X_i$ be a profinite space, presented as cofiltered limit of finite discrete spaces. Let us write $p_i\colon X \longrightarrow X_i$ for the projections of this limit and $f_{ji}\colon X_j \longrightarrow X_i$ for the morphism of the diagram corresponding to $j \leq i$. For every index $i \in I$, there exists an index $j \leq i$ such that $\mathsf{Im}\, f_{ji} = \mathsf{Im}\, p_i$, where Im stands for the image.*

Proof We fix the index $i \in I$. Since the limit is cofiltered, it is equivalent to compute it on the indices $j \leq i$. In other terms, we can assume that i is the terminal object of the poset I.

Given $x \in X_i$ and an index $j \leq i$, let us put $Y_j(x) = f_{ji}^{-1}(\{x\}) \subseteq X_j$. Applying lemma 3.4.10 and the obvious equality $p_i^{-1}(x) = \lim_{j\in I} Y_j(x)$, we get

$$\begin{aligned} x \in \bigcap_{j\in I} \mathsf{Im}\, f_{ji} &\Leftrightarrow \forall j \leq i \;\; Y_j(x) \neq \emptyset \\ &\Leftrightarrow \lim_{j\in I} Y_j(x) \neq \emptyset \\ &\Leftrightarrow p_i^{-1}(x) \neq \emptyset \\ &\Leftrightarrow x \in \mathsf{Im}\, p_i. \end{aligned}$$

This proves that

$$\mathsf{Im}\, p_i = \bigcap_{j\in I} \mathsf{Im}\, f_{ji}.$$

The right hand side of this equality is a cofiltered intersection of finite subsets of X_i, thus by finiteness, is one of these subsets. In other words

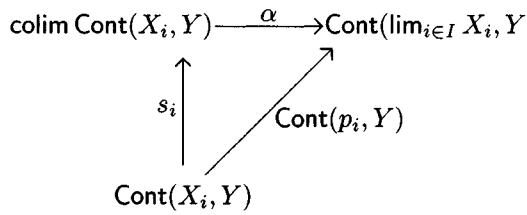
$$\exists j \in I \;\; \mathsf{Im}\, p_i = \mathsf{Im}\, f_{ji}.$$ □

Lemma 3.4.12 *Let $X = \lim_{i\in I} X_i$ be a profinite space, presented as a cofiltered limit of finite discrete spaces X_i. For every finite discrete space Y, the canonical comparison morphism*

$$\alpha\colon \operatorname{colim} \mathsf{Cont}(X_i, Y) \xrightarrow{\cong} \mathsf{Cont}\left(\lim_{i\in I} X_i, Y\right)$$

is a bijection, with Cont *denoting the set of continuous maps.*

Proof Observe first that since X_i is discrete, $\mathsf{Cont}(X_i, Y)$ is the set of all maps from X_i to Y. To fix notation, we recall that α is the unique factorization making the following diagrams commutative:



with s_i the canonical morphisms of the colimit and p_i the canonical morphisms of the limit. We must prove that α is bijective. Since the limit is cofiltered, the colimit is filtered. We recall that this filtered colimit is the quotient of the disjoint union $\coprod_{i\in I} \mathsf{Cont}(X_i, Y)$ by the equivalence relation $\approx$ given by

$$\begin{aligned}\big(u \in \mathsf{Cont}(X_i, Y)\big) &\approx \big(v \in \mathsf{Cont}(X_j, Y)\big)\\ &\Leftrightarrow \exists k \in I,\ k \leq i,\ k \leq j,\ \mathsf{Cont}(f_{ki}, Y)(u) = \mathsf{Cont}(f_{kj}, Y)(v).\end{aligned}$$

In other words

$$\begin{aligned}\big(u \in \mathsf{Cont}(X_i, Y)\big) &\approx \big(v \in \mathsf{Cont}(X_j, Y)\big)\\ &\Leftrightarrow \exists k \in I,\ k \leq i,\ k \leq j,\ u \circ f_{ki} = v \circ f_{kj}.\end{aligned}$$

We first prove the injectivity of α. Two elements of the colimit are thus equivalences classes $[u]$, $[v]$ of elements which, by filteredness, we can choose in the same factor; let us say, $u, v \in \mathsf{Cont}(X_i, Y)$. We assume that $\alpha\big([u]\big) = \alpha\big([v]\big)$. This implies at once

$$\begin{aligned}u \circ p_i &= \mathsf{Cont}(p_i, Y)(u) = (\alpha \circ s_i)(u) = \alpha\big([u]\big)\\ &= \alpha\big([v]\big) = (\alpha \circ s_i)(v) = \mathsf{Cont}(p_i, Y)(v) = v \circ p_i.\end{aligned}$$

But by lemma 3.4.11, we know the existence of an index $j \leq i$ with corresponding morphism $f_{ji} \colon X_j \longrightarrow X_i$ in the diagram and such that $\mathsf{Im}\, f_{ji} = \mathsf{Im}\, p_i$. The previous equalities show that u and v coincide on $\mathsf{Im}\, p_i$, thus on $\mathsf{Im}\, f_{ji}$. But then $u \circ f_{ji} = v \circ f_{ji}$, that is both elements u, v are identified in the factor $\mathsf{Cont}(X_j, Y)$ of the colimit. Thus u, v are identified in the colimit and $[u] = [v]$.

The surjectivity of α is harder to prove. Let us thus consider a continuous map $f \colon \mathsf{lim}_{i\in I} X_i \longrightarrow Y$. We consider first its kernel pair in the

category of topological spaces

$$R \underset{r_2}{\overset{r_1}{\rightrightarrows}} X = \lim_{i\in I} X_i \xrightarrow{f} Y, \quad R = \{(x,x') | f(x) = f(x')\}$$

and the kernel pair of each projection

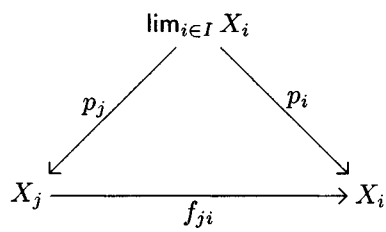
$$R_i \underset{r_2^i}{\overset{r_1^i}{\rightrightarrows}} X = \lim_{i\in I} X_i \xrightarrow{p_i} Y, \quad R_i = \{(x,x') | p_i(x) = p_i(x')\}.$$

These spaces R and R_i are thus obtained as inverse images of the diagonals of Y or X_i.

$$\begin{array}{ccc} R & \longrightarrow & Y \\ \downarrow & & \downarrow \Delta \\ X \times X & \xrightarrow[f\times f]{} & Y \times Y \end{array} \qquad \begin{array}{ccc} R_i & \longrightarrow & X_i \\ \downarrow & & \downarrow \Delta \\ X \times X & \xrightarrow[p_i \times p_i]{} & X_i \times X_i \end{array}$$

Since Y and X_i are discrete, their diagonal is both open and closed and therefore R and R_i are open and closed subspaces of $X \times X$.

Moreover if $j \leq i$, the commutativity of the triangle



implies $R_j \subseteq R_i$. Since I is a cofiltered poset, the poset $(R_i)_{i\in I}$ of equivalence relations, ordered by inclusion, is cofiltered as well.

We observe also that the diagonal $\Delta_X \subseteq X \times X$ of X is closed, because X is a Hausdorff space.

Since R is an equivalence relation, $\Delta_X \subseteq R$. On the other hand, by definition of R_i, one has $\Delta_X = \bigcap_{i\in I} R_i$. Therefore

$$\emptyset = \Delta_X \cap \complement\Delta_X = \left(\bigcap_{i\in I} R_i\right) \cap \complement\Delta_X \supseteq \left(\bigcap_{i\in I} R_i\right) \cap \complement R = \bigcap_{i\in I} (R_i \cap \complement R),$$

which proves that $\bigcap_{i\in I} (R_i \cap \complement R) = \emptyset$. Since the $(R_i)_{i\in I}$ constitute a cofiltered poset, so do the $R_i \cap \complement R$. We have thus a cofiltered family of

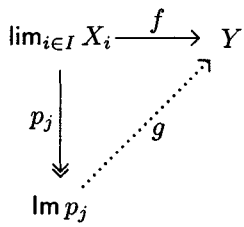
closed subsets of the compact Hausdorff space $X \times X$, whose intersection is empty; by compactness, one of these subsets is already empty. Thus

$$\exists j \in I \quad R_j \cap \complement R = \emptyset, \quad \text{that is,} \quad \exists j \in I \quad R_j \subseteq R.$$

In other words

$$\exists j \in I \quad \forall x, x' \in X \quad p_j(x) = p_j(x') \Rightarrow f(x) = f(x').$$

This shows precisely the existence of a factorization g in the following diagram:



This factorization is continuous since $\mathsf{Im}\, p_j$ is discrete, as a subspace of X_j.

Applying once more lemma 3.4.10, let us choose $k \leq j$ such that $\mathsf{Im}\, p_j = \mathsf{Im}\, f_{kj}$. This yields the composite

$$X_k \xrightarrow{f_{kj}} \mathsf{Im}\, f_{kj} = \mathsf{Im}\, p_j \xrightarrow{g} Y$$

which is such that $g \circ f_{kj} \circ p_k = f$, that is $\mathsf{Cont}(p_k, Y)(g \circ f_{kj}) = f$. By definition of α, this implies $\alpha([g \circ f_{kj}]) = f$. □

3.5 Infinitary extension of the Galois theory of Grothendieck

Definition 3.5.1 Let G be a topological group. A topological G-space is a topological space provided with a continuous action of G; a morphism of topological G-spaces is a continuous morphism of G-sets. A topological G-space is profinite when it is a projective limit, indexed by a cofiltered poset, of finite discrete topological G-spaces.

It is immediate to observe that projective limits of topological G-spaces are computed as in the category of topological spaces, with the corresponding componentwise action of G. Given a topological group G, we shall write G-Prof for the category of profinite G-spaces and their continuous homomorphisms.

Notice that given a topological group, a discrete G-set X, even finite, has no reason to be a topological G-space, since the action $G \times X \longrightarrow X$ is no longer defined on a discrete space. In fact a G-set X equipped with the discrete topology is a topological G-space if and only if the stabilizer $G_x = \{g \in G \mid gx = x\}$ is open for every $x \in X$.

Lemma 3.5.2 *Let K be a field. Every algebraic K-algebra A is the set-theoretical filtered union of its finite dimensional subalgebras.*

Proof Every element $a \in A$ is algebraic, thus the subalgebra $K(a) \subseteq A$ is finite dimensional (see proposition 2.1.10). This implies immediately that $A = \bigcup_B B$, for $B \subseteq A$ running through its finite dimensional subalgebras.

This union is filtered. Indeed given two such B and B', they have the form $B = K(a_1, \ldots, a_n)$, $B' = K(c_1, \ldots, c_m)$, for finite sets of generators. It suffices to observe that $K(a_1, \ldots, a_n, c_1, \ldots, c_m)$ is still finite dimensional. Trivially, $K(a_1, \ldots, a_n, c_1, \ldots, c_m)$ can be described as

$$\{p(a_1, \ldots, a_n, c_1, \ldots, c_m) \mid p(X_1, \ldots, X_n, Y_1, \ldots, Y_m) \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]\}.$$

But if $a_i \in A$ has a minimal polynomial $p(X) \in K[X]$ of degree n_i,

$$p(X) = X^{n_i} + k_{n_i-1}X^{n_i-1} + \cdots + k_0,$$

every occurrence of $a_i^{n_i}$ can be replaced by

$$a_i^{n_i} = -k_{n_i-1}a_i^{n_i-1} - \cdots - k_0.$$

An analogous argument holds for all a_i and c_j. Thus in the description of $K(a_1, \ldots, a_n, c_1, \ldots, c_m)$, there is no restriction in bounding the degree of the polynomial p in each variable, specifically, forcing this degree to be stricly less than the degree of the corresponding minimal polynomial. But these polynomials with bounded degrees have only a bounded number of coefficients, thus the space is finite dimensional. □

Lemma 3.5.3 *Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every K-algebra A which is split by L, there is a bijection*

$$\mathsf{Hom}_K(A, L) \cong \lim_B \mathsf{Hom}_K(B, L)$$

where the limit is cofiltered and indexed by the finite dimensional subalgebras $B \subseteq A$. Moreover, each $\mathsf{Hom}_K(B, L)$ is finite; in particular

the above limit formula provides $\mathsf{Hom}_K(A, L)$ *with the structure of a profinite space.*

Proof By lemma 3.5.2, A is the filtered union, or equivalently, the filtered colimit, of its finite dimensional subalgebras. This yields

$$\mathsf{Hom}_K(A, L) \cong \mathsf{Hom}_K\left(\operatorname*{colim}_B B, L\right) \cong \lim_B \mathsf{Hom}_K(B, L).$$

It remains to prove that $\mathsf{Hom}_K(B, L)$ is finite, for each finite dimensional $B \subseteq A$. By proposition 3.1.5, there exists a finite dimensional Galois extension $K \subseteq M \subseteq L$ which splits B. Every K-homomorphism $f\colon B \longrightarrow L$ is such that, for every element $b \in B$ with minimal polynomial $p(X) \in K[X]$,

$$p\big(f(b)\big) = f\big(p(b)\big) = f(0) = 0,$$

thus $f(b)$ is a root of $p(X)$ in L and therefore $f(b) \in M$. This proves the isomorphism $\mathsf{Hom}_K(B, L) \cong \mathsf{Hom}_K(B, M)$, and this last set is finite by theorem 2.3.3. □

Lemma 3.5.4 *Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every K-algebra A which is split by L, the map*

$$\mu\colon \mathsf{Gal}\,[L : K] \times \mathsf{Hom}_K(A, L) \longrightarrow \mathsf{Hom}_K(A, L), \quad (g, f) \mapsto g \circ f$$

is a continuous action of the topological group $\mathsf{Gal}\,[L : K]$ *on the topological space* $\mathsf{Hom}_K(A, L)$*, when these are provided with the profinite topologies inherited from definition 3.2.2 and lemma 3.5.3.*

Proof By associativity of the composition, μ is a group action. Proving its continuity reduces to proving that for every finite dimensional subalgebra $B \subseteq A$, the composite $p_B \circ \mu$ is continuous, where p_B is the canonical projection of the limit:

$$p_B\colon \mathsf{Hom}_K(A, L) \cong \lim_B \mathsf{Hom}_K(B, L) \longrightarrow \mathsf{Hom}_K(B, L).$$

By proposition 3.1.5, we choose a finite dimensional Galois extension $K \subseteq M \subseteq L$ which splits B. As observed in the proof of lemma 3.5.3, $\mathsf{Hom}_K(B, L) \cong \mathsf{Hom}_K(B, M)$ and is a finite discrete space. This allows consideration of diagram 3.1. Since p_M and p_B are continuous by definition, the left vertical composite is continuous. The bottom arrow is the composition, that is maps (f, g) onto $f \circ g$; it is of course continuous, since it is defined between finite discrete spaces. □

$$\begin{array}{ccc}
\mathsf{Gal}\,[L:K]\times \mathsf{Hom}_K(A,L) & \xrightarrow{\ \mu\ } & \mathsf{Hom}_K(A,L) \\
\Big\downarrow{\scriptstyle p_M\times \mathsf{id}} & & \\
\mathsf{Gal}\,[M:K]\times \mathsf{Hom}_K(A,L) & & \Big\downarrow{\scriptstyle p_B} \\
\Big\downarrow{\scriptstyle \mathsf{id}\times p_B} & & \\
\mathsf{Gal}\,[M:K]\times \mathsf{Hom}_K(B,M) & \longrightarrow & \mathsf{Hom}_K(B,M)
\end{array}$$

Diagram 3.1

Lemma 3.5.5 *Let $K \subseteq L$ be an arbitrary Galois extension of fields. Consider a homomorphism $f\colon A \longrightarrow B$ of K-algebras, where A and B are split by L. The map*

$$\Gamma(f)\colon \mathsf{Hom}_K(B,L) \longrightarrow \mathsf{Hom}_K(A,L), \quad h \mapsto h \circ f$$

is a continuous homomorphism of $\mathsf{Gal}\,[L:K]$-sets, when $\mathsf{Hom}_K(A,L)$ and $\mathsf{Hom}_K(B,L)$ are provided with the profinite topology of lemma 3.5.3.

Proof For every finite dimensional subalgebra $C \subseteq A$, we must prove that the composite

$$\mathsf{Hom}_K(B,L) \xrightarrow{\Gamma(f)} \mathsf{Hom}_K(A,L) = \lim_C \mathsf{Hom}_K(C,L) \xrightarrow{p_C} \mathsf{Hom}_K(C,L)$$

is continuous. Since C is finite dimensional, $f(C) \subseteq B$ is a finite dimensional K-algebra. The following diagram is commutative:

$$\begin{array}{ccc}
\mathsf{Hom}_K(B,L) & \xrightarrow{\ \Gamma(f)\ } & \mathsf{Hom}_K(A,L) \\
\Big\downarrow{\scriptstyle p_C} & & \Big\downarrow{\scriptstyle p_C} \\
\mathsf{Hom}_K\big(f(C),L\big) & \xrightarrow[\ \gamma(f)\ ]{} & \mathsf{Hom}_K(C,L)
\end{array}$$

where $\big(\gamma(f)(h)\big)(c) = h\big(f(c)\big)$ for all $c \in C$. The morphisms p_C are continuous by definition and $\gamma(f)$ is continuous since it is defined between finite discrete spaces. □

Lemma 3.5.6 *Let K be a field and A an algebraic K-algebra. As in lemma 3.5.2, let us write $A = \mathsf{colim}\, B$ where B runs through the finite dimensional subalgebras of A. For every finite dimensional K-algebra C, the canonical morphism*

$$\rho\colon \operatorname*{colim}_B \mathsf{Hom}_K(C,B) \xrightarrow{\cong} \mathsf{Hom}_K(C,A)$$

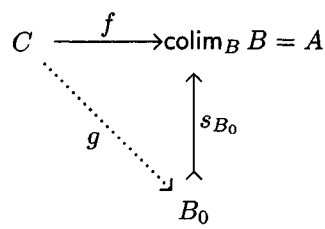
is bijective.

Proof The canonical morphism ρ of the statement is that induced by the canonical inclusions $\mathsf{Hom}_K(C,B) \subseteq \mathsf{Hom}_K(C,A)$.

Let $c_1, \ldots, c_n$ be a basis of C as K-vector space. A morphism of K-algebras $f\colon C \longrightarrow A \cong \mathsf{colim}_B B$ is such that

$$\forall i = 1, \ldots, n \quad f(c_i) = b_i \quad \text{with} \quad b_i \in B_i.$$

By filteredness, there is no restriction in choosing all elements b_i in the same factor B_0 of the colimit. This implies the existence of a K-linear factorization



where

$$g\left(\sum_{i=1,\ldots,n} k_i c_i\right) = \sum_{i=1,\ldots,n} k_i b_i.$$

Since s_{B_0} is injective and f is an algebra homomorphism, it follows at once that g is an algebra homomorphism. The above diagram shows that $f = \rho([g])$, proving the surjectivity of ρ.

To prove the injectivity of ρ, consider a homomorphism $g'\colon C \longrightarrow B_1$ such that $f = \rho([g'])$. By filteredness, we can view g and g' as having values in the same B_2, from which $g = g'$ as maps with values in B_2, since s_{B_2} is injective. This means $[g] = [g']$ in the colimit. □

Lemma 3.5.7 *Let $G = \mathsf{lim}_{i\in I} G_i$ be a profinite group, expressed as a cofiltered projective limit of finite discrete groups. Let us assume that the projections $p_i\colon G \longrightarrow G_i$ are surjective. We write G_i-Set_f for the*

category of finite G_i-sets and G-Top_f for the category of discrete finite topological G-spaces. For every index $i \in I$, there is a functor

$$\gamma_i \colon G_i\text{-}\mathsf{Set}_f \longrightarrow G\text{-}\mathsf{Top}_f, \quad X \mapsto X$$

where the G-set action on X is given by $g \cdot x = p_i(g) \cdot x$. This functor γ_i identifies G_i-Set_f with a full subcategory of G-Top_f. Moreover the category G-Top_f is the set theoretical filtered union of the full subcategories G_i-Set_f.

Proof For $X \in G_i\text{-}\mathsf{Set}_f$, the action of $\gamma_i(X)$ is continuous since it is the composite

$$G \times X \xrightarrow{p_i \times \mathsf{id}} G_i \times X \xrightarrow{\mu_i} X$$

where G_i and X are discrete, μ_i is the group action and p_i is continuous by definition.

To prove the full- and faithfulness, consider $f \colon X \longrightarrow Y$, an arbitrary map between finite G_i-sets. Observe that in the diagram

$$\begin{array}{ccccc} G \times X & \xrightarrow{p_i \times \mathsf{id}} & G_i \times X & \xrightarrow{\mu_i} & X \\ \downarrow{\scriptstyle \mathsf{id} \times f} & & \downarrow{\scriptstyle \mathsf{id} \times f} & & \downarrow{\scriptstyle f} \\ G \times Y & \xrightarrow[p_i \times \mathsf{id}]{} & G_i \times Y & \xrightarrow[\mu_i]{} & Y \end{array}$$

the left hand square is commutative. Since p_i is surjective, the commutativity of the outer diagram is equivalent to that of the right hand square. In other words, f is a morphism of G-sets if and only if it is a morphism of G_i-sets.

To prove the last assertion, consider a finite G-space X. The canonical comparison morphism

$$\left(\lim_{i \in I} G_i\right) \times X \xrightarrow{\cong} \lim_{i \in I}(G_i \times X)$$

is a homeomorphism. Indeed, products commute with limits in every category; moreover $X = \lim_{i \in I} X$ because I is connected. Therefore

$$\lim_{i \in I}(G_i \times X) \cong \left(\lim_{i \in I} G_i\right) \times \left(\lim_{i \in I} X\right) \cong \left(\lim_{i \in I} G_i\right) \times X.$$

By lemma 3.4.12, the composite

$$\lim_i (G_i \times X) \xrightarrow{\cong} \left(\lim_i G_i\right) \times X \xrightarrow{\cong} G \times X \xrightarrow{\mu} X$$

factors as

$$\lim_{i\in I}(G_i \times X) \xrightarrow{p_i \times \mathsf{id}} G_{i_0} \times X \xrightarrow{\mu_{i_0}} X.$$

By surjectivity of $p_i \times \mathsf{id}$, this presents X as a G_{i_0}-set. □

Theorem 3.5.8 (Galois theorem) *Let $K \subseteq L$ be an arbitrary Galois extension of fields. We write $\mathsf{Split}_K(L)$ for the category of K-algebras split by L and $\mathsf{Gal}[L:K]$-Prof for the category of profinite $\mathsf{Gal}[L:K]$-spaces. The functor*

$$\Gamma\colon \mathsf{Split}_K(L) \longrightarrow \mathsf{Gal}[L:K]\text{-}\mathsf{Prof}, \quad A \mapsto \mathsf{Hom}_K(A, L)$$

described in lemmas 3.5.3, 3.5.4, 3.5.5 is a contravariant equivalence of categories.

Proof We prove first that Γ is full and faithful. For this consider $A, B \in \mathsf{Split}_K(L)$. By definition 2.3.1 and lemma 3.5.2, let us write

$$A = \mathsf{colim}\, C, \quad C \subseteq A; \quad B = \mathsf{colim}\, D, \quad D \subseteq B$$

where the colimits are filtered and C, D run respectively through the finite dimensional subalgebras of A and B. For each pair C, D, we can by proposition 3.1.5 choose finite dimensional Galois extensions M_C, M_D which split respectively C and D. By proposition 3.1.4, we can even choose a finite dimensional Galois extension M_{CD} which splits both C and D and yields

$$K \subseteq M_C \subseteq M_{CD} \subseteq L, \quad K \subseteq M_D \subseteq M_{CD} \subseteq L.$$

As observed in the proof of lemma 3.5.3

$$\mathsf{Hom}_K(C, L) \cong \mathsf{Hom}_K(C, M_{CD}), \quad \mathsf{Hom}_K(D, L) \cong \mathsf{Hom}_K(D, M_{CD}).$$

We have then, using 3.4.12,

$$\begin{aligned}
&\mathsf{Hom}\big(\Gamma(A), \Gamma(B)\big) \\
&\quad \cong \mathsf{Hom}\big(\mathsf{Hom}_K(A, L), \mathsf{Hom}_K(B, L)\big) \\
&\quad \cong \mathsf{Hom}\big(\mathsf{Hom}_K(\mathsf{colim}_C\, C, L), \mathsf{Hom}_K(\mathsf{colim}_D\, D, L)\big) \\
&\quad \cong \mathsf{Hom}\big(\lim_C \mathsf{Hom}_K(C, L), \lim_D \mathsf{Hom}_K(D, L)\big) \\
&\quad \cong \lim_D \mathsf{Hom}\big(\lim_C \mathsf{Hom}_K(C, L), \mathsf{Hom}_K(D, L)\big) \\
&\quad \cong \lim_D \mathsf{colim}_C\, \mathsf{Hom}\big(\mathsf{Hom}_K(C, L), \mathsf{Hom}_K(D, L)\big) \\
&\quad \cong \lim_D \mathsf{colim}_C\, \mathsf{Hom}\big(\mathsf{Hom}_K(C, M_{CD}), \mathsf{Hom}_K(D, M_{CD})\big) \\
&\quad \cong \lim_D \mathsf{colim}_C\, \mathsf{Hom}(D, C) \quad \text{by 2.4.3}
\end{aligned}$$

$$\cong \lim_D \mathsf{Hom}(D, \mathsf{colim}\, C) \quad \text{by 3.5.6}$$
$$\cong \mathsf{Hom}(\mathsf{colim}\, D, \mathsf{colim}\, C)$$
$$\cong \mathsf{Hom}(B, A).$$

This proves the full- and faithfulness of Γ.

Observe next that for every finite dimensional Galois extension $K \subseteq M \subseteq L$, the projection, acting by restriction,

$$\mathsf{Gal}\,[L:K] = \lim_M \mathsf{Gal}\,[M:K] \longrightarrow \mathsf{Gal}\,[M:K]$$

is surjective, by definition 3.2.2 and proposition 3.1.2. Thus lemma 3.5.7 applies.

It remains to prove that Γ is essentially surjective on the objects. A profinite $\mathsf{Gal}\,[L:K]$-space is a cofiltered projective limit $X \cong \lim_{i\in I} X_i$ of finite discrete topological $\mathsf{Gal}\,[L:K]$-spaces. By lemma 3.5.7, each X_i is a finite $\mathsf{Gal}\,[M_i:K]$-set for some finite dimensional Galois extension $K \subseteq M_i \subseteq L$. By theorem 2.4.3, $X_i = \mathsf{Hom}_K(C_i, M_i)$ for some finite dimensional K-algebra C_i which is split by M_i. As already observed in lemma 3.5.3

$$X_i = \mathsf{Hom}_K(C_i, M_i) \cong \mathsf{Hom}_K(C_i, L).$$

We observe moreover that given $f_{ij}\colon X_i \longrightarrow X_j$ in the diagram defining X, the space X_i is a finite discrete $\mathsf{Gal}\,[M_i : K]$-space and the space X_j is a finite discrete $\mathsf{Gal}\,[M_j : K]$-space. By proposition 3.1.4, we choose a finite dimensional Galois extension $K \subseteq M \subseteq L$ such that $M_i \subseteq M$ and $M_j \subseteq M$. As above, this yields $X_i = \mathsf{Hom}_K(C_i, M)$ and $X_j = \mathsf{Hom}_K(C_j, M)$, where C_i and C_j are finite dimensional K-algebras split by M. Again by theorem 2.4.3

$$f_{ij}\colon \mathsf{Hom}_K(C_i, M) = X_i \longrightarrow X_j = \mathsf{Hom}_K(C_j, M)$$

is induced by a morphism $h_{ij}\colon C_j \longrightarrow C_i$ of K-algebras. In conclusion, from the cofiltered diagram constituted by the X_i, we have constructed a corresponding filtered diagram constituted by the C_i. We put $A = \mathsf{colim}_{i\in I} C_i$; since this colimit of algebras is filtered, it is computed as in the category of sets.

Each element $a \in A$ has the form $[a_i]$ for some index $i \in I$ and some element $a_i \in C_i$. The minimal polynomial $p(X)$ of a_i factors in $L[X]$ into factors of degree 1 (see definition 2.3.1). But from $p(a_i) = 0$ in C_i we deduce $p(a) = 0$ in A, thus a admits a minimal polynomial $q(X)$ which is a factor of $p(X)$ (see proposition 2.1.7). Therefore $q(X)$ factors in $L[X]$ into factors of degree 1. This proves that L splits A.

Finally one has

$$\mathsf{Hom}_K(A, L) \cong \mathsf{Hom}_K\left(\operatorname*{colim}_{i\in I} C_i, L\right) \cong \lim_{i\in I} \mathsf{Hom}_K(C_i, L) \cong \lim_{i\in I} X_i \cong X.$$

□