University of Vienna, Faculty of Mathematics

Semester Project

Winter 2009-2010

Profinite groups and Galois cohomology

Rosalie Chevalley

Professor:

Dietrich Burde

Assistant:

Wolfgang Moens

Abstract

The purpose of this project is to study the cohomology of groups, in particular the Galois cohomology. Therefore we will study carefully the finite and infinite Galois groups. Those groups are more or less equivalent to profinite groups, i.e. a limit of finite groups endowed with the discrete topology. Consequently a big part of this project consists in studying topological and profinite groups. There will also be some topics in Galois theory, in particular about infinite Galois extensions. At some point we will define the cohomology of groups using homological algebra, but we will mostly use an other equivalent definition, particularly suitable when dealing with profinite groups. The last chapter will give some elementary results about the cohomology of groups and will be an approach to Galois cohomology. In particular we will present different versions of Hilbert's theorem 90.

The most used reference is a book from L.Ribes [**Rib99**], which is an introduction to Galois cohomology.

Contents

CHAPTER 1

Topological groups

In this chapter we introduce the notion of topological groups and their basic properties. They are important to generalize the main theorem of Galois theory in case of infinite extensions. The reader shall find further information in [**Pon66**] and [**Hus66**].

1. Definition and examples

Definition 1.1. A set G of elements is called a *topological group* if

1. G is a group,
2. G is a topological space,
3. the map $G \times G \to G : (a, b) \mapsto ab$ is continuous, where $G \times G$ is equipped with the product topology,
4. the map $g \to G : x \mapsto x^{-1}$ is continuous.

The conditions (3) and (4) formulated in greater details respectively as follows:

- If $a, b \in G$, for every neighborhood W of the element ab there exist neighborhoods U and V of the elements a and b respectively such that $UV \subset W$.
- If $a \in G$, for every neighborhood V of the element a^{-1} there exist a neighborhood U of the element a such that $U^{-1} \subset V$.

Finally the two conditions can be expressed as:

- If $a, b \in G$, for every neighborhood W of the element ab^{-1} there exist neighborhoods U and V of the elements a and b respectively such that $UV^{-1} \subset W$.

Notation 1.2. In this project the neutral element of G will be denoted by 1.

Here are some examples of topological groups.

Examples 1.3. Here are some examples of topological groups.

- If G is a group endowed with the discrete topology (every subset of G is open), then G is a topological group.
- Let us consider the group of the reals numbers $\mathbb{R}$ together with addition: $(\mathbb{R}, +)$. If we append the ordinary topology on $\mathbb{R}$, this is a topological group.
- More generally, the additive group of any topological vector space (for example Banach spaces or Hilbert spaces) is a topological group.
- The linear group $GL_n(\mathbb{R})$ of all invertible $(n \times n)$ matrices with real entries is a topological group if endowed with the topology defined by viewing $GL_n(\mathbb{R})$ as a subset of $\mathbb{R}^{n\times n}$.

Definition 1.4. A *homomorphism of topological groups* is a continuous group-homomorphism. An isomorphism of topological groups is an group-isomorphism and a homeomorphism.

2. Elementary properties

The topological groups are homogeneous, which will later mean that some properties only have to be checked around the neutral element

Proposition 2.1. *Let G be a topological group. Let $a \in G$ and the maps $f, g, \varphi : G \to G$ defined by $f(x) = xa$, $g(x) = ax$, $\varphi(x) = x^{-1}$, then, f,g and φ are homeomorphisms of G.*

Proof. These maps are clearly bijective, and they are continuous because of the axioms of topological groups. □

Proposition 2.2. *Every topological group is homogenous, i.e. $\forall p, q \in G$, there is a homeomorphism f a such that $f(p) = q$.*

Proof. Let $p, q \in G$ and $f : x \mapsto qp^{-1}x$. By proposition 2.1, it is a homeomorphism. □

Proposition 2.3. *Let V be a neighborhood of a. Then there is a neighborhood U of 1 such that $V = aU$.*

Proof. We define $U := a^{-1}V$. As a preimage of V with the continuous map $g : G \to G : x \mapsto ax$ (see 2.1), U is a neighborhood of 1. And we have $V = aU$, hence the result. □

Definition 2.1. Let G be a topological group, a neighborhood V is called *symmetric* if $V = V^{-1}$.

Proposition 2.4. *Let G be a topological group. Then there is a basis consisting in symmetric open sets. In particular, there is a fundamental system of symmetric neighborhoods in each point of G.*

Proof. Let U be an open subset of G, then U^{-1} is open too (because it is a preimage of U under a continuous map) and so is $V := U \cap U^{-1}$. And we clearly have $V \subseteq U$ and $V = V^{-1}$. □

Proposition 2.5. *Let G be a topological group and U be a neighborhood of $x \in G$. Then we have:*

1. *There is a neighborhood V of x such that $V^2 \subseteq U$.*
2. *There is a neighborhood V of x such that $V^{-1} \subseteq U$.*
3. *There is a neighborhood V of x such that $VV^{-1} \subseteq U$.*
4. *There is a neighborhood V of x such that $V^{-1}V \subseteq U$.*

Proof. We only have to prove this proposition for neighborhoods of 1 (because topological groups are homogeneous).
The four statements are a consequence of the continuity of the following operations:

1. Consider the map $f_1 : G \to G : x \mapsto x^2$, which is continuous (because the product is continuous), and define $V = f_1^{-1}(U)$. As $1 = 1^2$, V is a neighborhood of 1, moreover $V^2 = f_1(V) = f_1(f_1^{-1}(U)) \subseteq U$.
2. Idem, using $f_2 : G \to G : x \mapsto x^{-1}$ and $1 = 1^{-1}$.
3. Idem, using $f_3 : G \to G : x \mapsto xx^{-1}$ and $1 = 11^{-1}$.
4. Idem, using $f_4 : G \to G : x \mapsto x^{-1}x$ and $1 = 1^{-1}1$.

□

Notation 2.2. Let X be a topological space and let $A \subseteq X$. We denote by $\bar{A}$ the topological closure of A.

Lemma 2.6. *Let X, Y be to topological spaces and $f : X \to Y$ a continuous map. Then $f(\bar{A}) \subseteq \overline{f(A)}$.*

Proof. Suppose $y \in f(\bar{A})$ and W is a neighborhood of y in Y. There is $x \in \bar{A}$ such that $f(x) = y$. As f is continuous mapping, $U := f^{-1}(W)$ is a neighborhood of x. Then $U \cap A \neq \emptyset$ (because $x \in \bar{A}$). Hence

$$\emptyset \neq f(U \cap A) \subseteq f(U) \cap f(A) \subseteq W \cap f(A).$$

So $y \in \overline{f(A)}$. □

Proposition 2.7. *Let G be a topological group, $\mathcal{V}$ a fundamental system of open neighborhoods of 1, and D a dense subset in G.*
Then $\mathcal{B} := \{Ux \mid x \in D, U \in \mathcal{V}\}$ is a basis of the topology of G.

Proof. Let W be an open subset of G, with $a \in W$. Then Wa^{-1} is open (it is the preimage of W under a continuous map) and $1 \in Wa^{-1}$. There is then $U \in \mathcal{V}$ such that $UU^{-1} \subseteq Wa^{-1}$ (use the fact that $\mathcal{V}$ is a fundamental system and proposition 2.5).
As D is dense, aD^{-1} is dense too. In fact, if we consider the continuous (and bijective) map $f : G \to G : x \mapsto ax^{-1}$ we have $X = f(X) = f(\overline{D}) \subseteq \overline{f(D)}$ (see lemma 2.6).
Then there is $d \in U \cap aD^{-1}$ and hence $m \in D$ such that $d = am^{-1}$, which implies $m = d^{-1}a$. Then $Ud^{-1}a \in \mathcal{B}$.
As $d \in U$, we obtain $Ud^{-1}a \subseteq UU^{-1}a \subseteq Wa^{-1}a = W$; and this is true for all $a \in W$. Thus

$$\bigcup_{a\in W} Ud^{-1}a \subseteq W.$$

Moreover, we have $1 \in Ud^{-1}$ (because $d \in U$), which implies $a \in Ud^{-1}a$ for all $a \in W$. Then

$$W \subseteq \bigcup_{a\in W} Ud^{-1}a.$$

So $W = \cup_{a\in W} Ud^{-1}a$. □

Proposition 2.8. *Let G be a topological group, $\mathcal{V}$ a fundamental system of open neighborhoods of 1. Then $\bigcap_{V\in\mathcal{V}} V = \overline{\{1\}}$.*

Proof. Let us show both inclusions:

- $\subseteq$: Let $x \in \bigcap_{V\in\mathcal{V}} V$ and W a neighborhood of x, combining propositions 2.3 and 2.4, we know there is a symmetric set $V \in \mathcal{V}$ such that $Vx \subseteq W$.
By hypothesis on x, $x \in V = V^{-1}$, which implies $x^{-1} \in V$. Thus, $1 = x^{-1}x \in Vx$. Then $1 \in U$, i.e. $U \cap \{1\} \neq \emptyset$. Hence $x \in \overline{\{1\}}$.
- $\supseteq$: Let $x \in \overline{\{1\}}$ and $V \in \mathcal{V}$ symmetric (we can suppose V symmetric because of proposition 2.4). Hence, because xV is a neighborhood of x, $xV \cap 1 \neq \emptyset$. This implies there is $v \in V$ such that $xv = 1$ and then $x = v^{-1} \in V^{-1} = V$. Thus $x \in \bigcap_{V\in\mathcal{V}} V$

□

Proposition 2.9. *Let G be a topological group and $A, B \subseteq G$. Then*

(1) $\bar{A}\bar{B} = \overline{AB}$.
(2) $\bar{A}^{-1} = \overline{A^{-1}}$.
(3) $x\bar{A}y = \overline{xAy}$ for all $x, y \in G$.

Proof.
(1) Let $x \in \bar{A}$, $x \in \bar{B}$ and U a neighborhood of 1. There is a neighborhood V of 1 such that $xVyV \subseteq xyU$ (because of the continuity of the map $G \to G : a \mapsto ba$ for all $b \in G$).
As xV, respectively yV, is a neighborhood of x, respectively y, there is $a \in A \cap xV$ and $b \in B \cap yV$. Hence $ab \in AB \cap xyU$, which means $xy \in \overline{AB}$.
(2) We will show both inclusions
- $\subseteq$: Use lemma 2.6 with the continuous map $i : G \to G : z \mapsto z^{-1}$.
- $\supseteq$: $A^{-1} \subseteq \overline{A^{-1}} \Rightarrow A \subseteq (\overline{A^{-1}})^{-1} = i(\overline{A^{-1}})$ and this last set is closed because i is homeomorphism.
Hence $\bar{A} \subseteq (\overline{A^{-1}})^{-1} \Rightarrow (\bar{A})^{-1} \subseteq \overline{A^{-1}}$.

(3) Idem with homeomorphism $G \to G : z \mapsto xzy$.

□

3. Characterization of the topology

We can use the fact that topological groups are homogeneous to characterize their topology using a neighborhoods basis of the neutral element of G.

Proposition 3.1. *Let G be a topological group, and let $\mathcal{V}$ be a neighborhood basis for the neutral element 1 of G. Then*

(1) For all $V_1, V_2 \in \mathcal{V}$, there is a $V \in \mathcal{V}$ such that $1 \in V \subseteq V_1 \cap V_2$;
(2) For all $V \in \mathcal{V}$, there is a $W \in \mathcal{V}$ such that $W^2 \subseteq V$;
(3) For all $V \in \mathcal{V}$, there is a $W \in \mathcal{V}$ such that $W^{-1} \subseteq V$;
(4) For all $V \in \mathcal{V}$ and all $g \in G$, there exists a $W \in \mathcal{V}$ such that $W \subseteq gVg^{-1}$;
(5) For all $g \in G$, $\{gV \mid V \in \mathcal{V}\}$ is a neighborhood basis of g.

Conversely, if G is a group and $\mathcal{V}$ is a nonempty set of subsets of G satisfying (1)-(4), then there is a (unique) topology on G for which (5) holds.

Proof. Suppose that $\mathcal{V}$ is a basis of neighborhoods of 1 in a topological group.
Then (1) is a consequence of the definition of a neighborhood basis. And (2), (3) and (4) are consequences of proposition 2.5. Finely (5) holds because the map $f : G \to G : x \mapsto gx$ is a homeomorphism.
Conversely, suppose that G is a group and $\mathcal{V}$ is a nonempty set of subsets of G satisfying (1)-(4). Note that (1) implies that $1 \in V$ for each $V \in \mathcal{V}$.
We define

$$\mathcal{T} = \{U \subseteq G \mid \forall g \in U\ \exists V \in \mathcal{V} \textit{ such that } gV \subseteq U\},$$

and we will show that $\mathcal{T}$ is a topology on G. First note that the empty set and G are clearly in $\mathcal{T}$. Suppose that $(U_i)_{i\in I}$ is a family of elements of $\mathcal{T}$ (for I a set of indexes) and let $g \in \cup_{i\in I} U_i$. Hence there is a $j \in I$ such that $g \in U_j$, by definition there is $V \in \mathcal{V}$ such that $gV \subseteq U_j$, which implies $gV \subseteq \cup_{i\in I} U_i$. Now let $U_1, U_2 \in \mathcal{T}$, and let $g \in U_1 \cap U_2$. By definition there are $V_1, V_2 \in \mathcal{V}$ with $gV_1 \subseteq U_1$ and $gV_2 \subseteq U_2$. We apply then (1) and we obtain a $V \in \mathcal{V}$ such that $V \subseteq V_1 \cap V_2$ and this means $gV \subseteq U_1 \cap U_2$. Hence $U_1 \cap U_2 \in \mathcal{T}$. And thus, we proved that $\mathcal{T}$ defines a topology on G. It is then easy to see that (5) holds.
We will now prove that $G \to G : g \mapsto g^{-1}$ is continuous. Let $g \in G$ and let U be an element of $\mathcal{T}$ (i.e. an open set) such that $g^{-1} \in U$. We have to find a $V \in \mathcal{V}$ such that $gV \subseteq U^{-1}$. By definition of $\mathcal{T}$, there is a $V \in \mathcal{V}$ such that $g^{-1}V \subseteq U$, which implies $V^{-1}g \subseteq U^{-1}$. If we use (3), we obtain a $V' \in \mathcal{V}$ such that $gV' \subseteq U^{-1}$; and now using (4), we have the existence of a $V'' \in \mathcal{V}$ with $gV'' \subseteq g(g^{-1}Vg) \subseteq U^{-1}$.
Let us check that the multiplication $G \times G \to G : (g_1, g_2) \mapsto g_1g_2$ is continuous. Notice that the sets $g_1V_1 \times g_2V_2$ form a neighborhoods basis of $(g_1, g_2) \in G \times G$ for all $V_1, V_2 \in \mathcal{V}$. Let $(g_1, g_2) \in G \times G$ and let U be an open such that $g_1g_2 \in U$. We have to find $V_1, V_2 \in \mathcal{V}$ such that $g_1V_1g_2V_2 \subseteq U$. As U is in $\mathcal{T}$, there is a $V \in \mathcal{V}$ such that $g_1g_2V \subseteq U$. We use (2) to obtain a $V' \in \mathcal{V}$ such that $g_1g_2V'V' \subseteq U$. We now apply (4), to obtain a $V'' \in \mathcal{V}$ such that $V'' \subseteq g_2V'g_2^{-1}$, which implies $g_1V''g_2V' \subseteq g_1(g_2V'g_2^{-1})g_2V' \subseteq U$. This concluded the proof. □

4. Topological subgroups

We briefly discuss some properties of topological groups, in particular some properties of their subgroups.

Proposition 4.1. *Let G be a topological group and H a subgroup. Then H is a topological group.*

Proof. We only have to prove that the product and the inverse map are continuous, but this is obvious because they are only restriction on the one of G. □

Proposition 4.2. *Let G be a topological group and H a subgroup. Then $\overline{H}$ is a subgroup of G. Moreover, if H is normal, than so is $\overline{H}$.*

Proof. It is enough to prove that $\overline{H}$ is closed under addition and inversion. Suppose $a, b \in \overline{H}$ and let us show that ab^{-1} is in $\overline{H}$.
Let W be a neighborhood of ab^{-1}, then there are U and V neighborhoods of a and b respectively such that, $UV^{-1} \subseteq W$ (because the map $G \times G \to G : (x, y) \mapsto xy^{-1}$ is continuous). We have then $U \cap H \neq \emptyset$ and $V \cap H \neq \emptyset$ (recall that $a, b \in \overline{H}$). Which means we can find $x \in U \cap H$ and $y \in V \cap H$ with $xy^{-1} \in UV^{-1} \cap H \subseteq W \cap H$. Hence $W \cap H \neq \emptyset$ and thus $ab^{-1} \in \overline{H}$.

Suppose now that H is normal. Let $a \in \overline{H}$ and $g \in G$, we are going to show that $g^{-1}ag \in \overline{H}$ which will imply the result.
Let V be a neighborhood of $g^{-1}ag$, then there is a neighborhood U of a such that $g^{-1}Ug \subseteq V$. But $a \in \overline{H}$ implies $U \cap H \neq \emptyset$. Hence there is $h \in U \cap H$, and we have $g^{-1}hg \in V$. But as H is normal, we have also that $g^{-1}hg \in H$. Then $V \cap H \neq \emptyset$. □

Definition 4.1. A topological space is *totally disconnected* if its only connected subspaces are one-point sets.

Examples 4.2.

- All discrete spaces are totally disconnected.
- The rational numbers $\mathbb{Q}$ and the irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ are totally disconnected spaces.
- The real numbers $\mathbb{R}$ (with the usual topology) is not a totally disconnected space.

Lemma 4.3. *Let X be a totally disconnected topological space. Then $\{x\}$ is closed in X for every $x \in X$.*

Proof. Let C be the topological closure of $\{x\}$. If we suppose that $A|B$ is a separation of C, with $x \in A$. A is closed in C and therefore in X. Hence we have $A = C$. Thus C is connected, so we must have $C = \{x\}$ because X is totally disconnected. □

Proposition 4.4. *Let G be a topological group*

1. *If H is an open (resp. closed) subgroup of G, then every coset Hg or gH is open (resp. closed).*
2. *Every open subgroup of G is closed. If G is compact, then every open subgroup of G has finite index.*
3. *Every closed subgroup of G of finite index is open.*
4. *If H is a subgroup containing a non-empty open subset U of G, then H is open in G.*
5. *G is Hausdorff if and only if $\{1\}$ is a closed subset of G. And if K is a normal subgroup of G then G/K is Hausdorff if and only if K is closed in G. If G is totally disconnected, then G is Hausdorff.*

Proof. (1) This follows from proposition 2.2.

(2) We will show that if H is open, we have $\overline{H} \subseteq H$. Let $a \in \overline{H}$. As H is open, aH is an open neighborhood of a and hence $aH \cap H \neq \emptyset$. Then, $\exists h_1, h_2 \in H$ such that $ah_1 = h_2$, which means $a = h_2h_1^{-1} \in H$. To prove that H as finite index, note that the gH is open (using (1)), disjoints and their union is G. Thus if G is compact, we must have that H has finite index.

(3) Suppose H is a closed subgroup of G with finite index. Then gH is closed for every $g \in G$. And since we have $G\backslash H = \cup_{g \notin H} gH$, H having finite index implies that $G\backslash H$ is closed (as finite union of closed spaces), and H is open.

(4) Since each set hU is open (using (1)), and since $H = \bigcup_{h \in H} hU$, H is open.

(5) We already know (using elementary topology) that every one-element subset in Hausdorff spaces are closed. Suppose now that $\{1\}$ is closed in G. Let a, b be distinct element of G. Proposition 2.2 implies that the set $\{ab^{-1}\}$ is closed (as image of $\{1\}$ under a homeomorphism). Then there exists an open set U with $1 \in U$ and $U \subseteq G\backslash(\{ab^{-1}\})$. From the continuity of the map $G \to G : (x, y) \mapsto xy^{-1}$ (trivial), the inverse image of U is open. Then, there are open sets V, W in G, containing 1, with $VW^{-1} \subseteq U$. So we have that $a^{-1}b \notin VW^{-1}$, and hence $aV \cap bW = \emptyset$. Since aV and bW are open, we have the result.
The next assertions follows from the first, the definition of the quotient topology and lemma 4.3.

□

5. Quotient groups

We will here present a proposition about quotients of topological groups.

Proposition 5.1. *Let G be a topological group and N a normal subgroup. Then G/N endowed with the quotient topology is a topological group. Moreover the canonical projection $\pi : G \to G/N$ is a continuous open homomorphism.*

Remark 5.1. The quotient topology is given by

$$\mathcal{T} = \{U \subseteq X \mid \pi^{-1}(U) \text{ open in } G\}.$$

Proof. We will first prove that π is an open map. Let U be open subset of G. Then $\pi^{-1}(\pi(U)) = UN$ and UN is open because so is U, hence the result. Moreover π is trivially continuous, by definition of $\mathcal{T}$.

We will now prove that G/N is a topological group. N being normal implies that G/N is an abstract group. Let us prove the continuity of the product and of the inverse maps.

Let W be a neighborhood of $g_1g_2N \in G/N$, then $\pi^{-1}(W)$ is a neighborhood of g_1g_2 because π is continuous. Using the continuity of the product in G, we know there are U_1, U_2 neighborhoods of g_1, g_2 respectively with $U_1U_2 \subseteq \pi^{-1}(W)$. Then $\pi(U_1)$ and $\pi(U_2)$ are neighborhoods of g_1N and g_2N (using the fact that π is open). Moreover we have $\pi(U_1)\pi(U_2) = \pi(U_1U_2) \subseteq W$ because π is a homomorphism. Hence the product is a continuous mapping.

Let W be a neighborhood of $gN \in G/N$, then $\pi^{-1}(W)$ is a neighborhood of g because π is continuous. Using the continuity of the inverse map in G, we know there is U a neighborhood of g, with $U^{-1} \subseteq \pi^{-1}(W)$. Then $\pi(U)$ is a neighborhood of gN. Moreover we have $\pi(U)^{-1} = \pi(U^{-1}) \subseteq W$. Hence the inverse map is continuous. □

6. Lie Groups

We briefly introduce Lie Groups because they provide a lot of examples of topological groups. One can find more information about this subject in **??**.

Definition 6.1. A *Lie group* is a finite dimensional smooth manifold G endowed with a group structure with smooth multiplication. This means that we have a smooth multiplication $\mu_G \times G \to G$, an inversion $i : G \to G$ and a unit element $1 \in G$ such that the group axioms are satisfied.

One can find the definition of a smooth manifold in [**Lan02b**, Chapter 2].

Remark 6.2. Notice that the Lie groups are topological groups. They provide a lot of examples of topological groups.

Examples 6.3.

- $\mathbb{R}$ and $\mathbb{C}$ are Lie groups under addition. Moreover, any finite dimensional real or complex vector space is a Lie group under addition.
- $\mathbb{R}^*(=\mathbb{R}\backslash\{0\})$ and $\mathbb{C}^*$ are Lie group under multiplication. $\mathbb{S} = \{z \in \mathbb{C} \mid |z| = 1\}$ is also a Lie group under multiplication.
- If G and H are Lie groups then the product $G \times H$ is a Lie group (with the usual product structure). Then (1) and (2) imply that the torus $\mathbb{T}_n = \mathbb{S}^n$ is a Lie group.
- The fundamental example of a Lie group is the group $GL(V)$ of invertible linear maps on a finite dimensional real vector space V.
  We will prove that in case $V = \mathbb{R}^n$. Let $f \in L(V, V)$ and consider the canonical basis $\{e_1, \dots, e_n\}$. The element $f(e_i) \in \mathbb{R}^n$ is the ith column of the matrix associated to f. This define a map between $L(V, V)$ and $M_n(\mathbb{R}) = \mathbb{R}^{n^2}$. The determinant defines a smooth function $det : M_n(\mathbb{R}) \to \mathbb{R}$. In particular $GL_n(\mathbb{R}) = det^{-1}(\mathbb{R}_n^*)$ is an open subset of $\mathbb{R}_n^2$ and thus a smooth manifold. Moreover, the entries of the product of two matrices A and B are polynomials in the entries of A and B, which implies that the multiplication defines a smooth map.

- The special linear group $SL_n(\mathbb{R})$ defined to be the kernel of the determinant application $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a Lie group as subgroup of $GL_n(\mathbb{R})$.
- The classical groups $O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$, define with $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid AA^T = A^TA = Id_n\}$ and $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) \mid \det(A) = 1\}$, are also Lie groups.

We give now some examples of topological groups which are not Lie groups.

Examples 6.4.

- Infinite dimensional groups, such as the additive group of an infinite dimensional real vector space. These are not Lie groups as they are not finite dimensional manifolds.
- Some totally disconnected groups, such as the Galois group of an infinite extension of fields, or the additive group of the p-adic numbers. These are not Lie groups because their underlying spaces are not real manifolds.

CHAPTER 2

Finite and infinite Galois Theory

In a first place we give a summary of classical Galois theory, in particular, we present the main theorem of Galois theroy for finite extensions. Next, we endow Galois groups with a specific topology, in order to state and prove the main theorem for infinite extensions.

1. Review of Galois Theory

In this section, $\mathbb{K}$, $\mathbb{L}$ and $\mathbb{E}$ denote always fields.

1.1. Some reminders.

Definition 1.1. Let $\mathbb{L}$ be a field extension of a field $\mathbb{K}$. We say that $\mathbb{L}$ is *algebraic* over $\mathbb{K}$, if every element of $\mathbb{L}$ is algebraic over $\mathbb{K}$.

Example 1.2. Consider the finite field with q elements $\mathbb{F}_q$, where $q = p^k$ with p a prime number. We recall that all finite extensions of $\mathbb{F}_q$ have an order that is a power of q (see [**Lan02a**, Thm 5.1] and [**Lan02a**, Corollary 5.2]).

Definition 1.3. Let $\mathbb{E}$ and $\mathbb{L}$ be two extensions of $\mathbb{K}$. A $\mathbb{K}$-*homomorphism* from $\mathbb{L}$ to $\mathbb{E}$ is a homomorphism $\sigma : \mathbb{L} \to \mathbb{E}$ such that $\sigma|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$.

Definition 1.4. Suppose G is a subgroup of the group of all homomorphisms of a field $\mathbb{L}$. Then we define

$$\mathbb{L}^G = \{\alpha \in \mathbb{L} \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}.$$

This is a subfield of $\mathbb{L}$, called the *fixed field* of G.

1.2. Normal and Separable extensions.

1.2.1. *Normal extension.*

Theorem 1.1. *Let $\mathbb{L}$ be and algebraic extension of $\mathbb{K}$ contained in some algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$.*
The following conditions are equivalent:

1. *$\mathbb{L}$ is the splitting field of a family of non-constant polynomials of $\mathbb{K}[X]$.*
2. *For every $\mathbb{K}$-homomorphism $\sigma : \mathbb{L} \to \overline{\mathbb{K}}$, $\sigma(\mathbb{L}) = \mathbb{L}$.*
3. *Every polynomial of $\mathbb{K}[X]$ having a root in $\mathbb{L}$ has all its roots in $\mathbb{L}$, i.e. it splits into linear factor in $\mathbb{K}$.*

Proof. One can find a proof of the theorem in [**Lan02a**, Chapter 5, §3]. □

Definition 1.5. We say that an algebraic extension $\mathbb{L}$ of $\mathbb{K}$ is *normal* if it satisfies one of the properties of the preceding theorem.

Examples 1.6.

- If $[\mathbb{L} : \mathbb{K}] = 2$, then $\mathbb{L}$ is normal over $\mathbb{K}$. In fact, let $\alpha \in \mathbb{L}\backslash\mathbb{K}$, the minimal polynomial of α over $\mathbb{K}$ can be written $f(X) = X^2 + cX + d$. And so $-c + \alpha \in \mathbb{L}$ is the other roof of f.
- The extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ is normal. But the extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}]$ is not normal ($X^3 - 2$ does not split in $\mathbb{Q}[\sqrt[3]{2}]$).

1.2.2. *Separable extension.*

Definition 1.7. An irreducible polynomial $f \in \mathbb{K}[X]$ is *separable* if it has no multiple roots.

Definition 1.8. Let $\mathbb{L}$ be an extension of $\mathbb{K}$.
We say that $\alpha \in \mathbb{L}$ is *separable* over $\mathbb{K}$ if α is algebraic over $\mathbb{K}$ and if $\min(\alpha, \mathbb{K})$ is separable.
We say that $\mathbb{L}$ is *separable* over $\mathbb{K}$ if every $\alpha \in \mathbb{E}$ is separable over $\mathbb{K}$.

Remark 1.9. Here is an explicit characterization of a separable extension:
$\mathbb{L}$ is algebraic and separable over $\mathbb{K}$ if every irreducible polynomial in $\mathbb{K}[X]$ having a root in $\mathbb{L}$ is separable.

Examples 1.10.

- If $\mathrm{char}(\mathbb{K}) = 0$, every algebraic extension of $\mathbb{K}$ is separable.
- If $\mathbb{K}$ is finite, every algebraic extensions of $\mathbb{K}$ is separable.
- Consider $\mathbb{F}_p$ for a prime number p and α a root of $X^p - t$. Then $\mathbb{F}_p[\alpha] \cong \mathbb{F}_p[X]/(X^p - t)$ is not a separable extension of $\mathbb{F}_p$ because α is not separable (the minimal polynomial of α over $\mathbb{K}$ is $X^p - t = (X - \alpha)^p$).

Definition 1.11. Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. The *separable closure* of $\mathbb{K}$ inside $\overline{\mathbb{K}}$ is the smallest subfield of $\overline{\mathbb{K}}$ containing every finite separable extension of $\mathbb{K}$.
We will denote by $\mathbb{K}_s$ the separable closure of $\mathbb{K}$ in some algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$.

Remark 1.12. In other words the separable closure of $\mathbb{K}$ is the union of all finite separable extensions of $\mathbb{K}$ contained in $\overline{\mathbb{K}}$.

We will next present the separable and inseparable degrees, which we will use later.

Definition 1.13. Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$, and let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. The *separable degree* of $\mathbb{L}$ over $\mathbb{K}$, denoted by $[\mathbb{L} : \mathbb{K}]_s$, is the number of extensions to $\mathbb{L}$ of the inclusion homomorphim $i : \mathbb{K} \to \overline{\mathbb{K}}$.

We have to check that this notion is well-defined, i.e. that $[\mathbb{L} : \mathbb{K}]_s$ is idependent of the choice of $\overline{\mathbb{K}}$. This is done in [**Lan02a**, §4, Chapter V].

Proposition 1.2. *Let $\mathbb{E}$ be a finite extension of $\mathbb{K}$, and $\mathbb{L}$ a finite extension of $\mathbb{E}$. Then*

$$[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{E}]_s \cdot [\mathbb{E} : \mathbb{K}]_s$$

Proof. One can find the proof refering to [**Lan02a**, Theorem 4.1, §1, Chapter V]. □

Proposition 1.3. *Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$. Then the separable degree $[\mathbb{L} : \mathbb{K}]_s$ divides the degree $[\mathbb{L} : \mathbb{K}]$. Moreover the quotient is 1 if the characteristic is 0 and a power of p isf the characteristic is a prime number $p > 0$.*

Definition 1.14. If $\mathbb{L}$ is a finite extension of $\mathbb{K}$, we call the quotient

$$\frac{[\mathbb{L} : \mathbb{K}]}{[\mathbb{L} : \mathbb{K}]_s}$$

the *inseparable degree*, denoted by $[\mathbb{L} : \mathbb{K}]_i$.

1.3. Galois extension.

Definition 1.15. An extension $\mathbb{L}$ of $\mathbb{K}$ is a *Galois extension* if it is an algebraic, normal and separable extension.

Remarks 1.16.

- We can describe a Galois extension more explicitly :
  Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$ and let f be an irreducible polynomial of degree m in $\mathbb{K}[X]$. If f has a root in $\mathbb{L}$, then f has m distinct roots in $\mathbb{L}$. So $\mathbb{L}$ is Galois, if and only if, for each $\alpha \in \mathbb{L}$, the minimal polynomial of α over $\mathbb{K}$ has $[\mathbb{K}[\alpha] : \mathbb{K}]$ distinct roots in $\mathbb{L}$.

- In our definition of Galois extension, we do not require the extension to be of finite degree. Later if there is no particular mention, a Galois extension can be finite or infinite.

Example 1.17. We consider the extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ for any prime number p. By construction $\mathbb{F}_{p^n} \cong \mathbb{F}_p/f_n(X)$, where $f_n(X) = X^{p^n} - X$ is an irreducible polynomial in $\mathbb{F}_p$ (see [**Lan02a**, Theorem 5.1, §5, Chaper V]). Then every element of $\mathbb{F}_{p^n}$ is a root of the polynomial $f_n(X)$, or in other words $\mathbb{F}_{p^n}$ is the splitting field of the polynomial $f_n(X)$. Thus $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$.

Here is a proposition we will often use later.

Proposition 1.4. *If $\mathbb{L}$ is a Galois extension of $\mathbb{K}$ (finite or infinite), then it is a Galois extension of any intermediate field $\mathbb{E}$, i.e. $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$.*

Proof. Let f be an irreducible polynomial in $\mathbb{E}[X]$ having a root α in $\mathbb{L}$. Since the property of being algebraic is transitive, we can find $g = \min(\alpha, \mathbb{K}) \in \mathbb{K}[X]$ the minimal polynomial of α over $\mathbb{K}$. $\mathbb{K}$ being normal implies that g splits in $\mathbb{L}[X]$ and $\mathbb{K}$ being separable implies that g has distinct roots in $\mathbb{L}$ (because g as a root α is $\mathbb{L}$).
As f divides g (in $\mathbb{E}[X]$), f must also be split into distinct factors of degree one in $\mathbb{L}[X]$. □

1.4. Galois group and fundamental theorem of Galois theory.

In this section, we will in particular present the fundamental theorem of Galois theory in the finite case.

Definition 1.18. Let $\mathbb{L}$ be an algebraic extension of $\mathbb{K}$, finite or infinite. The *Galois group* of $\mathbb{L}$ over $\mathbb{K}$, written $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$, is the set of all $\mathbb{K}$-homomorphisms of $\mathbb{L}$.

Definition 1.19. A Galois extension $\mathbb{L}$ of $\mathbb{K}$ is said to be *abelian* (resp. *cyclic*) if its Galois group is abelian (resp. cyclic).

The next example is an example of a Galois extension, moreover it provides us an intuition about the main theorem of the Galois theory.

Example 1.20. Consider the field $\mathbb{Q}$ and its extension $\mathbb{Q}[\sqrt[3]{2}, \omega]$, where $\omega = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt(3)}{2}$. We define

$$\begin{aligned} \sigma : \mathbb{Q}[\sqrt[3]{2}, \omega] &\rightarrow \mathbb{Q}[\sqrt[3]{2}, \omega] \\ \sqrt[3]{2} &\mapsto \omega\sqrt[3]{2} \\ \omega &\mapsto \omega \end{aligned}$$

and

$$\begin{aligned} \tau : \mathbb{Q}[\sqrt[3]{2}, \omega] &\rightarrow \mathbb{Q}[\sqrt[3]{2}, \omega] \\ \sqrt[3]{2} &\mapsto \sqrt[3]{2} \\ \omega &\mapsto \omega^2 = \overline{\omega}. \end{aligned}$$

Then, one can prove that $\{\mathrm{Id}_{\mathbb{Q}[\sqrt[3]{2},\omega]}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} = \mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}, \omega], \mathbb{Q})$. So we have $|\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}, \omega], \mathbb{Q})| = 6 = [\mathbb{Q}[\sqrt[3]{2}, \omega] : \mathbb{Q}]$. (Note that $\mathbb{Q}[\sqrt[3]{2}, \omega]$ is a normal extension of $\mathbb{Q}$.)

Theorem 1.5. *Let $\mathbb{L}$ be a finite Galois extension of $\mathbb{K}$, and let $G = \mathrm{Gal}(\mathbb{L}, \mathbb{K})$. There is a bijective correspondence*

$$\{H \mid H \leq G \ \textit{subgroup}\ \} \leftrightarrow \{\mathbb{E} \mid \mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L} \ \textit{intermediate field}\ \}.$$

More precisely, the maps $H \mapsto \mathbb{L}^H$ and $\mathbb{E} \mapsto \mathrm{Gal}(\mathbb{L}, \mathbb{E})$ are inverse bijections between the set of subgroups of G and the set of intermediate fields between $\mathbb{L}$ and $\mathbb{K}$.
Moreover,

(1) Let $H_1, H_2 \leq G$, then $H_1 \supseteq H_2$ if and only if $\mathbb{L}^{H_1} \subseteq \mathbb{L}^{H_2}$;

(2) Indexes equal degrees: $[H_1 : H_2] = [E^{H_2} : E^{H_1}]$.

(3) If H is a subgroup of G and $\sigma \in G$, then $\mathbb{L}^{\sigma H \sigma^{-1}} = \sigma(\mathbb{L}^H)$.
Conversely, if $\mathbb{E}$ is an intermediate field, $\mathrm{Gal}(\mathbb{L}, \sigma\mathbb{E}) = \sigma \,\mathrm{Gal}(\mathbb{L}, \mathbb{E})\sigma^{-1}$.

(4) Let $\mathbb{E}_1, \mathbb{E}_2$ be intermediate fields, then

$$\mathrm{Gal}(\mathbb{L}, \mathbb{E}_1\mathbb{E}_2) = \mathrm{Gal}(\mathbb{L}, \mathbb{E}_1) \cap \mathrm{Gal}(\mathbb{L}, \mathbb{E}_2).$$

(5) $\mathbb{E}$ is a Galois extension of $\mathbb{K}$ if and only if $\mathrm{Gal}(\mathbb{L}, \mathbb{E})$ *is a normal subgroup of G, and we have*

$$\mathrm{Gal}(\mathbb{E}, \mathbb{K}) \cong G/\,\mathrm{Gal}(\mathbb{L}, \mathbb{E}).$$

Proof. One can find the proof of this theorem in [**Mil08**, Chapter 3] or in [**Lan02a**, §1, Chapter IV] □

Remark 1.21. The theorem is in general false in case of infinite Galois extensions. We will therefore provide the Galois groups with a topology in order to get a theorem valid for both finite and infinite Galois extensions.

2. Krull topology on the Galois group

As previously discuss the main theorem of the Galois theory is not valid for infinite Galois extensions. However endowing Galois groups with a topology, we will obtain a similar result. The Krull topology is the most natural (non trivial) topology for a Galois group and it has many interesting properties.
Notice that in this section, there is no restriction about the degree of the field extensions.

2.1. Preliminary propositions.

The point of this section is to define a topology on the Galois groups. We will use therefore some propositions and lemmas.

Lemma 2.1. *Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$ and let $\mathbb{M}$ be an intermediate field, i.e. $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$. Then every $\mathbb{K}$-homomorphism from $\mathbb{M}$ to $\mathbb{L}$ can be extended to a $\mathbb{K}$-isomorphism from $\mathbb{L}$ to $\mathbb{L}$.*

Proof. See [**Mil08**, Chapter 7]. □

Lemma 2.2. *Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$. For all finite Galois extension $\mathbb{E}$ of $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$, the map*

$$\begin{array}{rcl} \mathrm{Gal}(\mathbb{L}, \mathbb{K}) & \to & \mathrm{Gal}(\mathbb{E}, \mathbb{K}) \\ \sigma & \mapsto & \sigma|_{\mathbb{E}} \end{array}$$

is surjective.

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{E}, \mathbb{K})$, then σ is a $\mathbb{K}$-homomorphism from $\mathbb{L}$ to $\mathbb{E}$. Hence using lemma 2.1, σ can be extended to a $\mathbb{K}$-isomorphism from $\mathbb{L}$ to $\mathbb{L}$ (which is a preimage). □

Notation 2.1. Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$. We denote $\mathcal{F}_{\mathbb{L}}$ the family of all finite Galois extension $\mathbb{E}$ of $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$.

Remark 2.2. Notice that if $\mathbb{L}$ is a Galois extension of $\mathbb{K}$, even infinite, we have that

$$\mathbb{L} = \bigcup_{\mathbb{E} \in \mathcal{F}_{\mathbb{L}}} \mathbb{E}.$$

Lemma 2.3. *Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$ and let $\mathbb{M}$ be an intermediate field. Then* $\mathbb{L}^{\mathrm{Gal}(\mathbb{L},\mathbb{M})} = \mathbb{M}$.

Proof. Clearly $\mathbb{M} \subseteq \mathbb{L}^{\mathrm{Gal}(\mathbb{L},\mathbb{M})}$ because of the definition of the fixed field.
For the other inclusion:
Suppose $\alpha \in \mathbb{L}^{\mathrm{Gal}(\mathbb{L},\mathbb{M})}$. Then the definition of $\mathrm{Gal}(\mathbb{L},\mathbb{M})$ implies $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(\mathbb{L},\mathbb{M})$. Since $\mathbb{L}$ is an union of finite intermediate Galois extensions, there is one such extension $\mathbb{E}$ with $\alpha \in \mathbb{E}$. Then, thanks to lemma 2.2, the map

$$\mathrm{Gal}(\mathbb{L},\mathbb{M}) \to \mathrm{Gal}(\mathbb{E},\mathbb{M}) : \sigma \mapsto \sigma|_{\mathbb{E}}$$

is surjective. And hence $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(\mathbb{E},\mathbb{M})$. Then using the theorem about finite extensions 1.5, we get that $\alpha \in \mathbb{E}^{\mathrm{Gal}(\mathbb{E},\mathbb{M})} = \mathbb{M}$. □

Proposition 2.4. *Let* $\mathbb{L}$ *be a Galois extension of* $\mathbb{K}$. *Suppose* $\mathbb{E}$ *is an intermediate finite Galois extension of* $\mathbb{K}$. *Then* $\mathrm{Gal}(\mathbb{L},\mathbb{E})$ *is normal in* $\mathrm{Gal}(\mathbb{L},\mathbb{K})$ *and* $\mathrm{Gal}(\mathbb{L},\mathbb{K})/\mathrm{Gal}(\mathbb{L},\mathbb{E}) = \mathrm{Gal}(\mathbb{E},\mathbb{K})$.

Proof. Let us take $\mathbb{E}' \in \mathcal{F}_{\mathbb{L}}$ with $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{E}' \subseteq \mathbb{L}$. Using theorem 1.5, we have that $\mathrm{Gal}(\mathbb{E}',\mathbb{E}) \lhd \mathrm{Gal}(\mathbb{E}',\mathbb{K})$, because $\mathbb{E}'$ is a finite extension of $\mathbb{K}$. By remark 2.2, we also have $\mathrm{Gal}(\mathbb{L},\mathbb{E}) \lhd \mathrm{Gal}(\mathbb{L},\mathbb{K})$.
Now suppose there exists a $\xi \in \mathbb{E}$ with $\sigma(\xi) \notin \mathbb{E}$ for a $\sigma \in \mathrm{Gal}(\mathbb{L},\mathbb{K})$. Using lemma 2.3, this implies the existence of $\gamma \in \mathrm{Gal}(\mathbb{L},\mathbb{E})$ such that $\gamma\sigma(\xi) \neq \sigma(\xi)$, which means $\sigma^{-1}\gamma\sigma(\xi) \neq \xi$. We have proven $\mathrm{Gal}(\mathbb{L},\mathbb{E}) \lhd \mathrm{Gal}(\mathbb{L},\mathbb{K})$ and so there is a $\widetilde{\gamma} \in \mathrm{Gal}(\mathbb{L},\mathbb{E})$ with $\widetilde{\gamma} = \sigma^{-1}\gamma\sigma$. But then $\widetilde{\gamma}(\xi) \neq \xi$ which is a contradiction with the fact that $\mathrm{Gal}(\mathbb{L},\mathbb{E})$ fixes $\mathbb{E}$.
This implies that $\sigma(\xi) \in \mathbb{E}$ for all $\xi \in \mathbb{E}$ and for all $\sigma \in \mathrm{Gal}(\mathbb{L},\mathbb{K})$. Thus $\sigma|_{\mathbb{E}}$ is an automorphism of $\mathbb{E}$.
Let $[\tau], [\eta] \in \mathrm{Gal}(\mathbb{L},\mathbb{K})/\mathrm{Gal}(\mathbb{L},\mathbb{E})$, then

$$\begin{aligned}
\tau \equiv \eta \quad &\Leftrightarrow \quad \tau\,\mathrm{Gal}(\mathbb{L},\mathbb{E}) = \eta\,\mathrm{Gal}(\mathbb{L},\mathbb{E}) \\
&\Leftrightarrow \quad \tau = \eta\gamma \textit{ with } \gamma \in \mathrm{Gal}(\mathbb{L},\mathbb{E}) \\
&\Leftrightarrow \quad \eta^{-1}\tau = \gamma \textit{ with } \gamma \in \mathrm{Gal}(\mathbb{L},\mathbb{E}) \\
&\Leftrightarrow \quad \eta^{-1}\tau|_{\mathbb{E}} = id_{\mathbb{E}} \\
&\Leftrightarrow \quad \eta|_{\mathbb{E}} = \tau|_{\mathbb{E}}.
\end{aligned}$$

And this proves that $\mathrm{Gal}(\mathbb{L},\mathbb{K})/\mathrm{Gal}(\mathbb{L},\mathbb{E}) \cong \{\sigma|_{\mathbb{E}} \mid \forall\sigma \in \mathrm{Gal}(\mathbb{L},\mathbb{K})\}$. But the right side is the set of automorphisms of $\mathbb{E}$ fixing $\mathbb{K}$, i.e. $\mathrm{Gal}(\mathbb{E},\mathbb{K})$. □

2.2. Definition. Recall that $\mathcal{F}_{\mathbb{L}}$ the family of all finite Galois extension $\mathbb{E}$ of $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$.

Definition 2.3. Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$ and $G = \mathrm{Gal}(\mathbb{L},\mathbb{K})$. Consider the set of normal subgroups of finite index, $\mathcal{S} = \{\mathrm{Gal}(\mathbb{L},\mathbb{E}) \mid \mathbb{E} \in \mathcal{F}_{\mathbb{L}}\}$. The topology defined by $\mathcal{S}$, as a basis of neighborhoods of the neutral element of G, is called the *Krull topology* of G.

Proposition 2.5. *The Krull topology is well-defined, i.e. if we consider* $\mathcal{S}$ *as in the definition, there is a unique structure of topological group on* G *for which the set* $\mathcal{S}$ *forms a basis of neighborhood of the neutral element. HenceG* $:= \mathrm{Gal}(\mathbb{L},\mathbb{K})$ *with the Krull topology in a topological group. Moreover the elements of* $\mathcal{S}$ *are open normal subgroups.*

Proof. We show that the collection $\mathcal{S}$ satisfies the assertions (1)-(4) of proposition 3.1 in chapter 1.

(1) Let $\mathrm{Gal}(\mathbb{L},\mathbb{E})$ and $\mathrm{Gal}(\mathbb{L},\mathbb{E}')$ be elements of $\mathcal{S}$. Using theorem 1.5, we have
$$\mathrm{Gal}(\mathbb{L},\mathbb{E}\mathbb{E}') = \mathrm{Gal}(\mathbb{L},\mathbb{E}) \cap \mathrm{Gal}(\mathbb{L},\mathbb{E}').$$
And $\mathrm{Gal}(\mathbb{L},\mathbb{E}\mathbb{E}')$ is an element of $\mathcal{S}$ because theorem 1.5 assure that the extension $\mathbb{E}\mathbb{E}'$ is finite and Galois over $\mathbb{K}$.
(2) Let $\mathrm{Gal}(\mathbb{L},\mathbb{E}) \in \mathcal{S}$, then $\mathrm{Gal}(\mathbb{L},\mathbb{E})\,\mathrm{Gal}(\mathbb{L},\mathbb{E}) \subseteq \mathrm{Gal}(\mathbb{L},\mathbb{E})$ because it is a group.
(3) Let $\mathrm{Gal}(\mathbb{L},\mathbb{E}) \in \mathcal{S}$, then $\mathrm{Gal}(\mathbb{L},\mathbb{E})^{-1} \subseteq \mathrm{Gal}(\mathbb{L},\mathbb{E})$ because it is a group.
(4) Let $\mathrm{Gal}(\mathbb{L},\mathbb{E}) \in \mathcal{S}$ and $\sigma \in G$. We proved in proposition 2.4 that $\mathrm{Gal}(\mathbb{L},\mathbb{E}) \lhd G$ and hence $\mathrm{Gal}(\mathbb{L},\mathbb{E}) = \sigma\,\mathrm{Gal}(\mathbb{L},\mathbb{E})\sigma^{-1}$.

□

Remark 2.4. If $\mathbb{L}$ is a finite Galois extension of $\mathbb{K}$, the Krull topology of $\text{Gal}(\mathbb{L}, \mathbb{K})$ is the discrete topology.

Remark 2.5. From now on, when there is no specific mention, we always consider that a Galois group is endowed with the Krull topology.

2.3. Properties.

Theorem 2.6. *Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$ and let $G = \text{Gal}(\mathbb{L}, \mathbb{K})$. The group G endowed with the Krull topology is a*

(1) Hausdorff,
(2) compact,
(3) totally disconnected

topological group.

Proof. (1) We have to show that for every $\sigma, \tau \in G$ with $\sigma \neq \tau$, there are two neighborhoods U and V of σ and τ respectively such that $\sigma \in U$, $\tau \in V$ and $U \cap V = \emptyset$. First, notice that

$$\bigcap_{U \in \mathcal{S}} U = \bigcap_{\mathbb{E} \in \mathcal{F}_{\mathbb{L}}} \text{Gal}(\mathbb{E}, \mathbb{K}) = 1$$

(which is implied by remark 2.2).
Then, if $\sigma, \tau \in G$ with $\sigma \neq \tau$, we have $\sigma^{-1}\tau \neq 1$, and thus (with the above equation) $\exists\ U_0 \in \mathcal{S}$ such that $\sigma^{-1}\tau \notin U_0$. So $\tau \notin \sigma U_0$, which means $\tau U_0 \cap \sigma U_0 = \emptyset$ since G is a group.

(2) We will prove the compactness using the theorem of Tychonoff. We build therefore the homomorphism

$$h : G \to \prod_{\mathbb{E} \in \mathcal{F}_{\mathbb{L}}} \text{Gal}(\mathbb{E}, \mathbb{K}) =: P$$

defined by

$$h(\sigma) = \prod_{\mathbb{E} \in \mathcal{F}_{\mathbb{L}}} \sigma|_{\mathbb{E}}.$$

Notice that P is compact. In fact every $\text{Gal}(\mathbb{E}, \mathbb{K})$ is a discrete finite group and consequently compact, so using the Theorem of Tychonoff (see [**Mun75**, Theorem 37.3]) we obtain that P is compact as product of compact spaces. If we show that h is injective, continuous and an open map into $h(G)$, we will have a homeomorphism between G and $h(G)$ (see [**Mun75**, Theorem 26.6]). Moreover, if we show that $h(G)$ is a closed subset of P (which implies that $h(G)$ is compact), we get that G is compact.

Injectivity: Suppose $\sigma \in G$ is such that $h(\sigma) = 1$. This means $\sigma|_{\mathbb{E}}$ is the identity for every $\mathbb{E} \in \mathcal{F}_{\mathbb{L}}$. But we know that $\mathbb{L} = \bigcup_{\mathbb{E} \in \mathcal{F}_{\mathbb{L}}} \mathbb{E}$, which means $\sigma = 1$.

Continuity: We consider the composition

$$G \xrightarrow{h} P \xrightarrow{\pi_{\mathbb{E}}} \text{Gal}(\mathbb{E}, \mathbb{K}),$$

where $\pi_{\mathbb{E}}$ is the canonical projection. To show that h is continuous, we only need to prove $\pi_{\mathbb{E}} \circ h$ is continuous for all $\mathbb{E} \in \mathcal{F}_{\mathbb{L}}$. As we work with topological groups, we only have to verify this in 1:

$$(\pi_{\mathbb{E}} h)^{-1}(\{1\}) = \text{Gal}(\mathbb{L}, \mathbb{E}) \in \mathcal{S}.$$

Note that $\{1\}$ is open in P because it is open in each $\text{Gal}(\mathbb{E}, \mathbb{K})$ (since $\text{Gal}(\mathbb{E}, \mathbb{K})$ is finite).

Open map: Let be $\mathbb{E} \in \mathcal{F}_{\mathbb{L}}$, then we have

$$h(\mathrm{Gal}(\mathbb{L},\mathbb{E})) = h(G) \cap (\prod_{\substack{\mathbb{E}' \neq \mathbb{E} \\ \mathbb{E}' \in \mathcal{F}_{\mathbb{L}}}} \mathrm{Gal}(\mathbb{E}',\mathbb{K}) \times \{1\} \ ),$$

which is an open set in $h(G)$.

$h(G)$ **closed:** We define $M_{\mathbb{E}_1|\mathbb{E}_2} := \{\Sigma \in P \mid \pi_{\mathbb{E}_1}(\Sigma)|_{\mathbb{E}_2} = \pi_{\mathbb{E}_2}(\Sigma)\}$ for each pair $\mathbb{E}_1, \mathbb{E}_2 \in \mathcal{F}_{\mathbb{L}}$ with $\mathbb{E}_2 \subseteq \mathbb{E}_1$. We will first show that $M_{\mathbb{E}_1|\mathbb{E}_2}$ is closed in P. As $\mathbb{E}_2$ is a finite extension of $\mathbb{K}$, we can consider $\mathrm{Gal}(\mathbb{E}_2,\mathbb{K}) = \{f_1,\dots,f_r\}$. We call S_i the set of extensions of f_i to $\mathbb{E}_1$. Then we have

$$M_{\mathbb{E}_1|\mathbb{E}_2} = \bigcup_{i=1}^{r} (\prod_{\substack{\mathbb{E} \neq \mathbb{E}_1, \mathbb{E}_2 \\ \mathbb{E} \in \mathcal{F}_{\mathbb{L}}}} \mathrm{Gal}(\mathbb{E},\mathbb{K}) \times S_i \times \{f_i\} \ ).$$

As every set in the finite union is a closed set (as product of closed sets), $M_{\mathbb{E}_1|\mathbb{E}_2}$ is closed.

We have

$$h(G) \subseteq \bigcap_{\mathbb{E}_1 \supseteq \mathbb{E}_2} M_{\mathbb{E}_1|\mathbb{E}_2}$$

and if we prove the other inclusion, we will get that $h(G)$ is closed in P. Now, if $\Sigma \in \bigcap_{\mathbb{E}_1 \supseteq \mathbb{E}_2} M_{\mathbb{E}_1|\mathbb{E}_2}$, we can define an automorphism $\sigma : \mathbb{L} \to \mathbb{L}$ with $\sigma(x) = \pi_{\mathbb{E}}(\Sigma)(x)$ if $x \in \mathbb{E}$. This σ is well-defined since $\Sigma \in \cap M_{\mathbb{E}_1|\mathbb{E}_2}$ (and using remark 2.2). We have $h(\sigma) = \prod_{\mathbb{E} \in \mathcal{F}_{\mathbb{L}}} \pi_{\mathbb{E}}(\Sigma)$, which implies

$$h(G) \supseteq \bigcap_{\mathbb{E}_1 \supseteq \mathbb{E}_2} M_{\mathbb{E}_1|\mathbb{E}_2},$$

and so $h(G)$ is closed.

(3) Since we work with topological groups, we only have to show that the connected component H of 1 is $\{1\}$.
For each $U \in \mathcal{S}$ we define $U_H := U \cap H$. As $\{1\} \in U$, $U_H \neq \emptyset$, and as U is open, U_H is open in H. We define now

$$V_H = \bigcup_{x \in H \setminus U_H} xU_H.$$

Then, V_H is open in H, because all the xU_H are open. We also have $U_H \cap V_H = \emptyset$ and $H = U_H \cup V_H$. But as H is supposed to be connected, we get that $V_H = \emptyset$, otherwise, $U_H|V_H$ is a separation of H. This means $U_H = H$, hence $U \cap H = H$ for all $U \in \mathcal{S}$. Therefore

$$H \subseteq \bigcap_{U \in \mathcal{S}} U = \{1\},$$

which means $H = \{1\}$.

□

3. The fundamental theorem of infinite Galois theory

In this section we will generalize the main theorem of Galois theory seen in the case of finite extensions. Therefore we will also generalize some propositions and lemmas.

3.1. Some necessary propositions.

The first proposition is a generalization of the lemma 2.2, but considering we work with topological groups.

Proposition 3.1. *Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$. For all finite Galois extension $\mathbb{E}$ of $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$, the map*

$$\begin{array}{rcl} r : \mathrm{Gal}(\mathbb{L},\mathbb{K}) & \to & \mathrm{Gal}(\mathbb{E},\mathbb{K}) \\ \sigma & \mapsto & \sigma|_{\mathbb{E}} \end{array}$$

is a continuous surjection.

Proof. We already proved that the map is surjective in lemma 2.2.
We will show that the inverse image of $1_{\mathrm{Gal}(\mathbb{E},\mathbb{K})}$ is open in $\mathrm{Gal}(\mathbb{L},\mathbb{K})$ (it is enough since topological groups are homogeneous). But $r^{-1}(\{1_{\mathrm{Gal}(\mathbb{E},\mathbb{K})}\}) = \mathrm{Gal}(\mathbb{L},\mathbb{E})$, which is an open set because of the definition of the Krull topology. □

Proposition 3.2. *Let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$ and write $G := \mathrm{Gal}(\mathbb{L},\mathbb{K})$. Then the following assertions hold.*

(1) The field $\mathbb{L}$ is Galois over every intermediate field $\mathbb{M}$ (i.e. $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$).
Moreover $\mathrm{Gal}(\mathbb{L},\mathbb{M})$ is closed in G and $\mathbb{L}^{\mathrm{Gal}(\mathbb{L},\mathbb{M})} = \mathbb{M}$.

(2) For every subgroup H of G, $\mathrm{Gal}(\mathbb{L},\mathbb{L}^H)$ is the topological closure of H.

Proof. (1) The first assertion is implied by lemma 1.4.
Consider $\mathcal{F}_{\mathbb{M}}$ the family of envery finite and Galois extensions $\mathbb{E}$ of $\mathbb{K}$ such that $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{M}$. Then $\mathbb{M}$ is the union of all the elements of $\mathcal{F}_{\mathbb{M}}$. Which means

$$\mathrm{Gal}(\mathbb{L},\mathbb{M}) = \cap_{\mathbb{E}\in\mathcal{F}_{\mathbb{M}}} \mathrm{Gal}(\mathbb{L},\mathbb{E}).$$

But the groups $\mathrm{Gal}(\mathbb{L},\mathbb{E})$ are all open subgroups of G and therefore they are closed (see proposition 4.4 (2) and theorem 2.6). Then $\mathrm{Gal}(\mathbb{L},\mathbb{M})$ is closed as intersection of closed sets.
Lemma 2.3 implies the final statement.

(2) We have that $H \subseteq \mathrm{Gal}(\mathbb{L},\mathbb{L}^H)$, but because $\mathrm{Gal}(\mathbb{L},\mathbb{L}^H)$ is closed, $\overline{H} \subseteq \mathrm{Gal}(\mathbb{L},\mathbb{L}^H)$.
Now consider $\sigma \in G\backslash\overline{H}$, there is an $\mathbb{E} \in \mathcal{F}_{\mathbb{L}}$ such that $\sigma\,\mathrm{Gal}(\mathbb{L},\mathbb{E}) \cap H = \emptyset$. And so $\sigma \notin H\,\mathrm{Gal}(\mathbb{L},\mathbb{E})$. Since σ can not be writen $\sigma = h\tau$ for some $h \in H$ and $\tau \in \mathrm{Gal}(\mathbb{L},\mathbb{E})$ (which would have implied $\sigma(\alpha) = h(\alpha)$ for all $\alpha \in \mathbb{E}$), we have the existence of an $\alpha \in \mathbb{E}$ such that H fixes α ($\Rightarrow \alpha \in \mathbb{L}^H$) but $\sigma(\alpha) \neq \alpha$. This means $\sigma \notin \mathrm{Gal}(\mathbb{L},\mathbb{L}^H)$. Thus $\mathrm{Gal}(\mathbb{L},\mathbb{L}^H) \subseteq \overline{H}$.

□

3.2. The main theorem.

We will now prove a similar theorem as the main theorem for finite Galois extensions (see 1.5).

Theorem 3.3. *Let $\mathbb{L}$ be Galois over $\mathbb{K}$ with Galois group G. There is a bijection between*

$$\{H \mid H \textit{ closed subgroup of } G\} \leftrightarrow \{\mathbb{M} \textit{ intermediate field} \mid \mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}\}$$

given by the maps $H \mapsto \mathbb{L}^H$ (sending a closed subgroup on its fixed field) and $\mathbb{M} \mapsto \mathrm{Gal}(\mathbb{L},\mathbb{M})$ (sending an intermediate field on its Galois group).
Moreover,

(1) If H_1 and H_2 are two closed subgroups of G, we have $H_1 \supseteq H_2$ if and only if $\mathbb{L}^{H_1} \subseteq \mathbb{L}^{H_2}$.

(2) A closed subgroup H of G is open if and only if $\mathbb{L}^H$ has finite degree over $\mathbb{K}$. In this case, $[G : H] = [\mathbb{L}^H : \mathbb{K}]$, i.e indexes and degrees coincide.

(3) For every element $\sigma \in G$, and every subgroup H of G, $\mathbb{L}^{\sigma H \sigma^{-1}} = \sigma(\mathbb{L}^H)$, and if $\mathbb{M}$ is an intermediate field $\mathrm{Gal}(\mathbb{L},\sigma\mathbb{M}) = \sigma\,\mathrm{Gal}(\mathbb{L},\mathbb{M})\sigma^{-1}$.

(4) If H is a closed subgroup of G, we have the following equivalence:
H is normal if and only if $\mathbb{L}^H$ is Galois over $\mathbb{K}$. In this case we have $\mathrm{Gal}(\mathbb{L}^H,\mathbb{K}) \cong G/H$.

Proof. To prove the first statement we have to show that the maps $H \mapsto \mathbb{L}^H$ and $M \mapsto \mathrm{Gal}(\mathbb{L}, \mathbb{M})$ are inverse maps. First suppose that H is a closed subgroup of G. Then $\mathbb{L}$ is Galois over $\mathbb{L}^H$ and $\mathrm{Gal}(\mathbb{L}, \mathbb{L}^H) = H$ (see proposition 3.2). Conversely if $\mathbb{M}$ is an intermediate field, we have that $\mathrm{Gal}(\mathbb{L}, \mathbb{M})$ is a closed subgroup of G and $\mathbb{L}^{\mathrm{Gal}(\mathbb{L},\mathbb{M})} = \mathbb{M}$ (see proposition 3.2 (1)).

(1) If H_1, H_2 are closed subgroups of G, using the definitions, we have
$$H_2 \subseteq H_1 \Rightarrow \mathbb{L}^{H_1} \subseteq \mathbb{L}^{H_2} \Rightarrow \mathrm{Gal}(\mathbb{L}, \mathbb{L}^{H_1}) \supseteq \mathrm{Gal}(\mathbb{L}, \mathbb{L}^{H_2})$$
Hence $\mathrm{Gal}(\mathbb{L}, \mathbb{L}^{H_i}) = H_i$ implies the result.

(2) Using proposition 4.4, we obtain that H being a closed subgroup of G with finite index implies that H is open. And conversely using the same proposition, if H is an open subgroup of G, H is closed and has finite index (recall that G is compact - see theorem 2.6).
Suppose now that H is closed and has finite index. We consider the continuous map
$$\begin{array}{rcl} r : \mathrm{Gal}(\mathbb{L}, \mathbb{K}) & \rightarrow & \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}^H, \mathbb{K}) \\ \sigma & \mapsto & \sigma|_{\mathbb{L}^H}. \end{array}$$
Clearly $\ker(r) = \mathrm{Gal}(\mathbb{L}, \mathbb{L}^H)$ and $\mathrm{im}(r) = Hom_{\mathbb{K}}(\mathbb{L}^H, \mathbb{K})$ (for the last statement apply lemma 2.1). Then, using the first isomorphism theorem for groups, we have
$$\mathrm{Gal}(\mathbb{L}, \mathbb{K})/\ker(r) \cong Hom_{\mathbb{K}}(\mathbb{L}^H, \mathbb{K}),$$
which is equivalent to
$$G/H \cong Hom_{\mathbb{K}}(\mathbb{L}^H, \mathbb{K}).$$

(3) Let $\mathbb{M}$ be an intermediate field and $H = \mathrm{Gal}(\mathbb{L}, \mathbb{M})$. If $\sigma \in G$, we want to prove that $\sigma H \sigma^{-1} \leftrightarrow \sigma\mathbb{M}$.
Therefore, let $\tau \in G$ and $\alpha \in \mathbb{L}$. We have that $\tau(\alpha) = \alpha$ if and only if $\sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma(\alpha)$. Hence $\mathrm{Gal}(\mathbb{L}, \sigma\mathbb{M}) = \sigma \,\mathrm{Gal}(\mathbb{L}, \mathbb{M})\sigma^{-1}$. And $\sigma(\mathbb{L}^H) = \sigma\mathbb{M} = \mathbb{L}^{\sigma H \sigma^{-1}}$.

(4) Suppose that $\mathbb{M}$ is an intermediate field with $H = \mathrm{Gal}(\mathbb{L}, \mathbb{M})$. Using (3), we have that H is normal in G if and only if $\mathbb{M}$ is stable under the natural action of G. This last statement is equivalent to say that $\mathbb{M}$ is a union of finite extensions of $\mathbb{K}$ stable under G. But this, using the point (3) of theorem 1.5, is the same as expecting that all those finite extensions are Galois over $\mathbb{K}$. And so $\mathbb{M}$ is Galois.
And then the isomorphism follows from (2).

□

Here is an example showing that the main theorem is invalid if we omit the topological conditions.

Example 3.1. We consider the finite field $\mathbb{F}_p$ for a prime number p and its algebraic closure $\overline{\mathbb{F}}_p$. Notice that $\overline{\mathbb{F}}_p$ is a Galois extension of $\mathbb{F}_p$. As $\overline{\mathbb{F}}_p$ must contain the roots of all polynomials of the form $X^{p^n} - X$ for $n \geq 1$, $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_p$. Moreover $\overline{\mathbb{F}}_p$ can be written as union of intermediate finite extensions, we must have $\overline{\mathbb{F}}_p = \cup_{n\geq 1}\mathbb{F}_p^n$.
Now consider $G = \mathrm{Gal}(\overline{\mathbb{F}}_p, \mathbb{F}_p)$. We denote by φ the Frobenius automorphism, i.e.
$$\varphi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p : \alpha \mapsto \alpha^p.$$
As $\mathbb{F}_p^*$ is a cyclic group of order $p - 1$, for each $\alpha \in \mathbb{F}_p$, $\varphi(\alpha) = \alpha$. Hence $\varphi \in G$.
We define $H =< \varphi >$ the subgroup of G generated by all the powers of φ. We will now prove two remarquable statements about H.

(1) $H \neq G$
To prove that, we have to find an element τ of G such that $\tau \notin H$.
We first show that there is an infinite intermediate extension $\mathbb{M}$ of $\mathbb{F}_p$ such that $\mathbb{F}_p \subsetneqq \mathbb{M} \subsetneqq \overline{\mathbb{F}}_p$. Therefore we consider $\mathbb{M} = \cup_{n\geq 0}\mathbb{F}_{p^{2^n}}$, clearly $\mathbb{M}$ is an infinite extension since $\mathbb{F}_{p^{2^n}} \subseteq \mathbb{M}$ for all $n \geq 0$ and $\mathbb{M}$ is Galois over $\mathbb{F}_p$ since it is a union of Galois extensions.

We now show that $\mathbb{M} \neq \overline{\mathbb{F}}_p$. Therefore we consider $\mathbb{F}_{p^3}$, clearly $[\mathbb{F}_{p^3} : \mathbb{F}_p] = 3$ and $\mathbb{F}_{p^3} \subseteq \overline{\mathbb{F}}_p$ but $\mathbb{F}_{p^3} \nsubseteq \mathbb{M}$. In fact if we suppose $\mathbb{F}_{p^3} = \mathbb{F}_p[\alpha]$ and $\alpha \in \mathbb{M}$, we have $\alpha \in \mathbb{F}_{p^{2^n}}$ for some $n \geq 0$, and hence $\mathbb{F}_3 \subseteq \mathbb{F}_{p^{2^n}}$. But then using the degree formula for the extensions, we have:

$$2^n = [\mathbb{F}_{p^{2^n}} : \mathbb{F}_p] = [\mathbb{F}_{p^{2^n}} : \mathbb{F}_{p^3}][\mathbb{F}_{p^3} : \mathbb{F}_p] = [\mathbb{F}_{p^{2^n}} : \mathbb{F}_{p^3}] \cdot 3,$$

which is a contradiction. Thus $\mathbb{F}_p \subsetneqq \mathbb{M} \subsetneqq \overline{\mathbb{F}}_p$.

Now using proposition 1.4, we know that $\overline{\mathbb{F}}_p$ is Galois over $\mathbb{M}$. Then let $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}_p, \mathbb{M}) \backslash \{\mathrm{Id}\} \subseteq G$. If we suppose $H = G$, there is a $n \geq 1$ such that $\tau = \varphi^n$. Hence φ^n fixes $\mathbb{M}$, so $\mathbb{M} \subseteq \mathbb{F}_{p^n}$. But this is a contradiction since $\mathbb{M}$ is infinite.

(2) $\mathbb{F}_p^H = \overline{\mathbb{F}}_p$

By definition $\mathbb{F}_p^H \subseteq \overline{\mathbb{F}}_p$, hence we show the other inclusion. Let $\alpha \in \overline{\mathbb{F}}_p$. Then $\alpha \in \mathbb{F}_{p^n}$ for some $n \geq 1$. This means $\alpha^{p^n} - \alpha = 0$ (see example 1.17). But then $\alpha^{p^n} = \alpha$, and so $\varphi^n(\alpha) = \alpha$. Hence $\alpha \in \mathbb{F}_p^H$.

We conclude that H and G are two different groups but they have the same fixed field, as $\overline{\mathbb{F}}_p = \mathbb{F}_p^G$. This contradicts the theorem, unless G is the topological closure of H.

CHAPTER 3

Profinite Groups

In this chapter we define the notion of profinite groups. Those are defined as limits of particular systems. They are useful to characterize Galois groups, in fact, every Galois group is a profinite group and every profinite group can be realized as a Galois group.

1. Definition and examples

1.1. The notion of inverse limit.

1.1.1. *Definition.*

Definition 1.1. A *directed set* is a nonempty set I together with a reflexive and transitive binary relation $\leq$, with the additional property that every pair of elements has an upper bound.

Definition 1.2. Let I be a directed set. An *inverse system* $(X_i, f_{ij})_I$ of topological spaces indexed by I consists of a family $\{X_i \mid i \in I\}$ of topological spaces and of a family $\{f_{ij} : X_j \to X_i \mid i, j \in I, i \leq j\}$ of continuous maps such that

1. f_{ii} is the identity over X_i for all $i \in I$,
2. $f_{ij} \circ f_{jk} = f_{ik}$ for all $i \leq j \leq k \in I$.

Remark 1.3. The preceding definition is not only available in the category of topological spaces, it can be generalized to an arbitrary category.

Examples 1.4.

1. We consider the directed set $(\mathbb{Z}, >)$, with $m > n$ if and only if n divides m, for each $m, n \in \mathbb{Z}$. We define $G_m = \mathbb{Z}/m\mathbb{Z}$ and consider the natural projections
$$f_{nm} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : k + m\mathbb{Z} \mapsto k + n\mathbb{Z},$$
which are well-defined in case $n|m$. Then $(G_m, f_{nm})_{\mathbb{Z}}$ is an inverse system.
2. Let p be a prime number. We consider now $I = \mathbb{N}$ provide with the usual order. We define $G_n = \mathbb{Z}/p^n\mathbb{Z}$ and consider the natural projections
$$f_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$$
which are well-defined in case $m \leq n$. Then $(G_n, f_{mn})_{\mathbb{N}}$ is an inverse system.
3. Let G be an arbitrary group. Denote $\mathcal{S}$ the set of all its normal subgroups of finite index. We provide $\mathcal{S}$ with the order $U < V$ if and only if $V \subseteq U$ for $U, V \in \mathcal{S}$. Define
$$f_{UV} : G/V \to G/U : gV \mapsto gU,$$
in case $U \leq V$. Then $(G/U, f_{UV})_{\mathcal{S}}$ is an inverse system.

Definition 1.5. If Y is a topological space, we call a family of continuous maps $\{\psi_i : Y \to X_i\}_{i\in I}$ *compatible*, if $f_{ij}\psi_j = \psi_i$ for every $i \leq j \in I$, i.e. if the following diagram commutes:

$$\begin{tikzcd} & Y \arrow[dl, "\psi_j"'] \arrow[dr, "\psi_i"] & \\ X_j \arrow[rr, "f_{ij}"'] & & X_i. \end{tikzcd}$$

Definition 1.6. An *inverse limit* (X, φ_i) of an inverse system $(X_i, f_{ij})_I$ of topological spaces is a topological space X provided with a compatible family $\{\varphi_i : X \to X_i\}_{i \in I}$ satisfying the following universal property:
For every topological space Y and for every compatible family $\{\psi_i : Y \to X_i\}_{i \in I}$, there exists a unique continuous map $\theta : Y \to X$ such that the following diagram commutes for all $i \leq j \in I$.

$$\begin{tikzcd}
 & Y \arrow[d, dotted, "\exists!"', "\theta"] \arrow[ddl, "\psi_j"'] \arrow[ddr, "\psi_i"] & \\
 & X \arrow[dl, "\varphi_j"] \arrow[dr, "\varphi_i"'] & \\
X_j \arrow[rr, "f_{ij}"'] & & X_i.
\end{tikzcd}$$

Remark 1.7. An injective limit is also called a projective limit.

1.1.2. *Existence and uniqueness of the inverse limit.*

Proposition 1.1. *Let $(X_i, f_{ij})_I$ be an inverse system of topological spaces. If $(X, \varphi_i)_I$ and $(Y, \psi_i)_I$ are two inverse limits of $(X_i, f_{ij})_I$, then, there is a homeomorphism $\Phi : X \to Y$ such that $\psi_i \circ \Phi = \varphi_i$ for all $i \in I$.*

Proof. As $(X, \varphi_i)_I$ is an inverse limit and $(Y, \psi_i)_I$ a compatible family, there exists a unique $\Phi : X \to Y$ such that $\psi_i \circ \Phi = \varphi_i$ for all $i \in I$.
As $(Y, \psi_i)_I$ is an inverse limit and $(X, \varphi_i)_I$ a compatible family, there exists a unique $\Psi : Y \to X$ such that $\varphi_i \circ \Psi = \psi_i$ for all $i \in I$.
Then $\Psi \circ \Phi : X \to X$ and $\varphi_i \Psi \Phi = \psi_i \Phi = \varphi_i$ for all $i \in I$, moreover $\varphi_i id_X = \varphi_i$ for all $i \in I$. So $\Psi \circ \Phi = id_X$ by the uniqueness of the morphism in definition 1.6.
One can show in the same way that $\Phi \circ \Psi = id_Y$. □

Proposition 1.2. *Let $(X_i, f_{ij})_I$ be an inverse system of topological spaces. Denote by X the set of elements $x \in \prod_{k \in I} X_k$ which make the diagram commute*

$$\begin{tikzcd}
 & \prod_{k \in I} X_k \arrow[dl, "\pi_j"'] \arrow[dr, "\pi_i"] & \\
X_j \arrow[rr, "f_{ij}"'] & & X_i
\end{tikzcd}$$

That means X is the set of all elements $x \in \prod_{k \in I} X_k$ such that $f_{ij}\pi_j(x) = \pi_i(x)$ for all $i \leq j \in I$. Where the π_i are the canonical projections.
Define $\varphi_i := \pi_i|_X$ for all $i \in I$. Then $(X, \varphi_i)_I$ is an inverse limit of $(X_i, f_{ij})_I$.

Remark 1.8. We endow $\prod_{k \in I} X_k$ with the product topology and X with the subspace topology.

Proof. By definition of the product topology the maps φ_i are continuous, and we have $f_{ij}\varphi_j = \varphi_i$ because of definition of X. This means $\{\varphi_i : X \to X_i | i \in I\}$ is compatible.
Let us consider an other compatible family $\{\psi_i : Y \to X_i | i \in I\}$. We have to show that there exists a unique continuous map $\theta : Y \to X$ with $\varphi_i \theta = \psi_i$ for all $i \in I$. Therefore, we define

$$\begin{aligned} \overline{\theta} : Y &\to \prod_{k \in I} X_k \\ y &\mapsto \{\psi_k(y)\}_{k \in I}. \end{aligned}$$

We have $\pi_i \overline{\theta} = \psi_i$ which is continuous for all $i \in I$, and this implies the continuity of $\overline{\theta}$. Moreover the image of $\overline{\theta}$ is in X, in fact

$$f_{ij} \circ \pi_j(\overline{\theta}(y)) = f_{ij}\psi_j(y) = \psi_i(y) = \pi_i(\overline{\theta}(y)) \quad \forall i \leq j \in I, \forall y \in Y.$$

This means we can define the map

$$\begin{array}{rcl}\theta : Y & \to & X \\ y & \mapsto & \overline{\theta}(y)\end{array}$$

which is continuous. This map satisfies also $\varphi_i \theta = \psi_i$ for all $i \in I$. Note that the uniqueness of θ follows from its construction. □

Notation 1.9. We can now denote by $\varprojlim_I X_i$ the inverse limit of an inverse system $(X_i, f_{ij})_I$. And let $s \varprojlim_I X_i$ denote the particular above construction.

1.1.3. *Properties.*
Here are some properties of the inverse limit we will use later.

Proposition 1.3. *Let $(X_i, f_{ij})_I$ be an inverse system indexed by I, and write $X = \varprojlim X_i$.*

(1) If each X_i is Hausdorff, so is X.
(2) If each X_i is totally disconnected, so is X.
(3) If each X_i is Hausdorff, then $s \varprojlim X_i$ is closed in $P = \prod_{i \in I} X_i$.
(4) If each X_i is compact and Hausdorff, so is X.

Proof. It is enough to prove the result for $X = s \varprojlim X_i$ because of the uniqueness of inverse limit.

(1) Products and subspaces of Hausdorff spaces are always Hausdorff, hence the result.
(2) Idem.
(3) By a topological result, if $f, g : Y \to Z$ are continuous maps and Z is a Hausdorff space, the set $\{y \mid f(y) = g(y)\}$ is closed in Y. Since
$$s \varprojlim X_i = \bigcap_{j \geq i} \{p \in P \mid f_{ij} \pi_j(p) = \pi_i(p)\}$$
(where π_i is the canonical projection form P to X_i), it follows that if each X_i is Hausdorff, then $s \varprojlim X_i$ is an intersection of closed sets, hence $s \varprojlim X_i$ is closed.
(4) This result follows from the fact that each closed subspace of a compact space is compact, and from the fact that a product of compact spaces is compact.

□

1.2. Profinite groups. We will now consider the case of inverse limits of topological groups.

Proposition 1.4. *The inverse limit $\varprojlim G_i$ of an inverse system of topological groups $(G_i, f_{ij})_I$ is a topological group.*

Proof. The cartesian product $\prod_{k \in I} G_k$ is a topological group, this means we only have to show that $G := \varprojlim G_i$ is a subgroup.
Clearly G is not empty ($1_{\prod_{k \in I} G_k} \in G$) and closed under multiplication and taking inverse. In fact $G = \{g \in \prod_{k \in I} G_k \mid f_{ij} \pi_j(g) = \pi_i(g) \ \forall i \leq j\}$ and all the f_{ij} and π_k $(i, j, k \in I)$ are groups homomorphisms. Then G is a subgroup of $\prod_{k \in I} G_k$ and therefore a topological subgroup for the induced topology. □

Definition 1.10. A *profinite group* G is a topological group isomorphic to an inverse limit of an inverse system $(G_i, f_{ij})_I$ of finite groups, all of them provided with the discrete topology.

Examples 1.11.

(1) We denote $\widehat{\mathbb{Z}} := \varprojlim_{m \in \mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ the inverse limit of the inverse system $(\mathbb{Z}/m\mathbb{Z}, f_{nm})_{\mathbb{Z}}$ (see example 1.4 (2)).
$\widehat{\mathbb{Z}}$ is called the *Prüfer group*. Note that $\widehat{\mathbb{Z}}$ is the set of all equivalence classes of sequences (a_m) such that
$$a_m \equiv a_n \mod n \ \forall n | m.$$

(2) We define $\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ the inverse limit of the inverse system $(\mathbb{Z}/p^n\mathbb{Z}, f_{mn})_{\mathbb{N}}$ (see example 1.4 (2)).
$\mathbb{Z}_p$ is the additive group of the *p-adic integers*.

(3) Every finite group G is in particular a profinite group. In fact it is the limit of the trivial inverse system $(G, \mathrm{Id}_G)_{\{1\}}$.

(4) The group of integers $\mathbb{Z}$ is not a profinite group.

Definition 1.12. Let G be an arbitrary group, denote by $\mathcal{S}$ the set of all its normal subgroups of finite index. Then as in example 1.4 $(G/U, f_{UV})_{\mathcal{S}}$ is an inverse system, and we define

$$\widehat{G} := \varprojlim_{U\in\mathcal{S}} G/U$$

to be the *profinite completion* of G.

2. General properties of profinite groups

The goal of this section is to give an particular characterization of the profinite groups, in fact, we will prove that profinite groups are exactly the compact, totally disconnected, Hausdorff groups.

2.1. Some lemmas and propositions.

Proposition 2.1. *Let $(G_i, f_{ij})_I$ be an inverse system of finite groups G_i (endowed with the discrete topology). We construct $G := s\varprojlim_{i\in I} G_i$ and write $\varphi_i : G \to G_i$ the projection homomorphisms. Then $\{\ker(\varphi_i) \mid i \in I\}$ is a fundamental system of open neighborhoods of the identity element 1 in G.*

Proof. Consider the family of neighborhoods of 1 in $\prod_{i\in I} G_i$ of the form

$$(\prod_{i\neq i_1,\ldots i_t} G_i) \times \{1\}_{i_1} \times \ldots \times \{1\}_{i_t}$$

for any finite collection of indexes $i_1, \ldots, i_t \in I$ and where $\{1\}_i$ denotes the subset of G_i containing its identity element. As the G_i are discrete, the above family is a fundamental system of neighborhoods of the identity element of $\prod_{i\in I} G_i$ (see definition of the product topology - [**Mun75**, §19]). As I is a directed set and as the collection is finite, there is $i_0 \in I$ such that $i_0 \geq i_r$ for all $1 \leq r \leq t$. So we have that

$$G \cap [(\prod_{i\neq i_0} G_i) \times \{1\}_{i_0}] = G \cap [(\prod_{i\neq i_1,\ldots i_t} G_i) \times \{1\}_{i_1} \times \ldots \times \{1\}_{i_t}]$$

because $f_{i_r i_0}(1) = 1$ for all $1 \leq r \leq t$.
Then a fundamental system of open neighborhoods of 1 in G is given by all the sets $G \cap [(\prod_{i\neq i_0} G_i) \times \{1\}_{i_0}]$. But we see that $\ker(\varphi_{i_0}) = G \cap [(\prod_{i\neq i_0} G_i) \times \{1\}_{i_0}]$ □

Lemma 2.2. *Let X be a compact, Hausdorff topological space. Let $x \in X$ and let $\{U_i \mid i \in I\}$ be the family of all compact open sets containing x. Then $A = \cap_{i\in I} U_i$ is connected.*

Proof. Note that X being Hausdorff and U_i being compact implies that U_i is closed for all $i \in I$ (see [**Mun75**, Theorem 26.3]).
Suppose there exists a separation of A, i.e. suppose there are U, V closed with $A = U \cup V$ and $U \cap V = \emptyset$. Since X is normal (X is compact Hausdorff - see [**Mun75**, Theorem 32.3]), there are U', V' open such that $U \subseteq U'$, $V \subseteq V'$ and $U' \cap V' = \emptyset$. So we have:

$$U \cup V \subseteq U' \cup V' \Rightarrow X\backslash(U' \cap V') \subseteq X\backslash(U \cap V),$$

which means $[X\backslash(U' \cap V')] \cap A = \emptyset$. But, as $X\backslash(U' \cap V')$ is closed, it is compact too. Having $X\backslash(U' \cap V') \subseteq X\backslash A = \cup_{i\in I} X\backslash U_i$ (with $X\backslash U_i$ open), there is $J \subseteq I$ finite with

$$[X\backslash(U' \cap V')] \cap (\bigcap_{i\in J} U_i) = \emptyset.$$

We consider $B := \cap_{i\in J} U_i$. B is open because $|J| < \infty$ and U_i is open for all $i \in I$, and B is compact because it is a closed subset of X (B is also an intersection of closed spaces). We have $x \in B$ and $B = (B \cap U') \cup (B \cap V')$. Suppose $x \in B \cap U'$. Since $B \cap U'$ is open and compact, $B \cap U' = U_{i_0}$ for a $i_0 \in I$. This means $A \subseteq B \cap U' \subseteq U'$, then

$$A \cap V \subseteq A \cap V' \subseteq U' \cap V' = \emptyset \Rightarrow V = \emptyset,$$

hence the result. □

Lemma 2.3. *Let G be a compact, Hausdorff, totally disconnected topological group. Then every neighborhood of 1 contains an open normal subgroup. Moreover this subgroup has finite index in G.*

Proof. We consider $\{U_i \mid i \in I\}$ the family of all compact open sets containing 1. Like in the preceding lemma, a result of topology implies that U_i is closed for each $i \in I$.
Because of lemma 2.2 and because X is totally disconnected, we have $\{1\} = \cap_{i\in I} U_i$.
Suppose that U is an open neighborhood of $\{1\}$. Then $G\backslash U$ is closed, hence compact. We have

$$(G\backslash U) \cap (\bigcap_{i\in I} U_i) = \emptyset,$$

this means there is a finite set $J \subseteq I$ with

$$(G\backslash U) \cap (\bigcap_{i\in J} U_i) = \emptyset.$$

Let $A := \cap_{i\in J} U_i$, we have that A is open as a finite intersection of open sets and that A is compact because it is a closed subspace of G (note that A is an intersection of closed sets). This means that A is a neighborhood of 1. Moreover we have $A \subseteq U$.
We define $F := (G\backslash A) \cap A^2$. Notice that A^2 is compact because it is the image of $A \times A$ (compact - see [**Mun75**, Theorem 26.7]) under the continuous map $(x, y) \mapsto xy$. Then A^2 is closed, hence so is F.
Let V be a symmetric open neighborhood of 1 such that $AV \cap F = \emptyset$ and $V \subseteq A$ (such a neighborhood exists because of proposition 2.4, chapter 1). Then we have $AV \subseteq A^2 \Rightarrow AV \cap (G\backslash A) \subseteq A^2 \cap (G\backslash A) = F$. Which means $AV \cap (G\backslash A) = \emptyset$ because $AV \cap F = \emptyset$. Hence $AV \subseteq A \Rightarrow AV^n \subseteq A$ for all $n \geq 1$, which implies $V^n \subseteq A$ (because $1 \in A$).
We define $K := \cup_{n\geq 1} V^n \subseteq A$, an open subset of G. As G is compact, K has a finite index by proposition 4.4. Hence we can write $G := \cup_{m=1}^{r} x_m K$. The fact that K as finite index, implies that there is a finite number of conjugacy classes of K ($xK = yK \Rightarrow \exists k \in K$ with $x = yk \Rightarrow xKx^{-1} = ykKk^{-1}y^{-1} = yKy^{-1}$). Hence

$$H := \bigcap_{x\in G} xKx^{-1} = \bigcap_{m=1}^{r} x_m K x_m^{-1}.$$

Because $x_m K x_m^{-1}$ is open for all $1 \leq m \leq r$ (see proposition 4.4), H is an open normal subgroup of G. And this means that H has finite index (propostion 4.4). □

Lemma 2.4. *Let $(X_i, f_{ij})_I$ be an inverse system of topological spaces. Let $(X, \varphi_i)_{i\in I}$ be a compatible family with all the h_i being surjective maps. Then either $\varprojlim X_i$ is empty or the induced map $\theta : X \to \varprojlim X_i$ sends X onto a dense subset of $\varprojlim X_i$.*

Proof. We will prove that for every basic open subset V of $\varprojlim X_i$ we can find $y \in X$ such that $\theta(y) \in V$.
Let us consider

$$V = (\varprojlim X_i) \cap (\prod_{i\in I\backslash\{i_1,\ldots i_n\}} X_i \times U_1 \times \ldots U_n),$$

where U_j are non-empty open subsets of X_{i_j}, for each $1 \leq j \leq n$.
As I is a directed set, we can find $i_0 \in I$ with $i_0 > i_j$ for all $1 \leq j \leq n$. If we take $x = \prod_{i\in I} X_i \in V$; we have $f_{i_j i_0}(x_{i_0}) = x_{i_j}$ for all $1 \leq j \leq n$.

Because φ_{i_0} is surjective, there is $y \in X$ such that $\varphi_{i_0}(y) = x_{i_0}$. This means $\pi_{i_0}(\theta(y)) = x_{i_0}$, so $\pi_{x_j}(\theta(y)) = f_{i_j i_0}(\pi_{x_0}(\theta(y))) = x_{i_j}$, and hence $\theta(y) \in V$. □

2.2. Other characterization of pro-finite groups.

Theorem 2.5. *The profinite groups are exactly the compact, totally disconnected, Hausdorff groups.*

Proof. Assume G is a profinite group.
By definition of a profinite group, there are finite groups $(G_i)_{i\in I}$ and maps $f_{ij} : X_j \to X_i$ for all $i, j \in I, i \leq j$ such that $G = \varprojlim_{i\in I} G_i$. As all the G_i are finite discrete topological groups, they are Hausdorff, compact and totally disconnected groups. Hence, with proposition 1.3, we have that G is an Hausdorff compact totally disconnected group.
Conversely, assume G is a Hausdorff, compact and totally disconnected topological group.
We write $U <_O G$ when U in an open normal subgroup of G.
Consider the family $\mathcal{S} = \{U \mid U <_O G\}$. As G is compact, U being open implies that G/U is finite (proposition 4.4, chapter 1). By lemma 2.3 $\mathcal{S}$ is a basis of open neighborhoods of $1 \in G$.
For each pair $U, V \in \mathcal{S}$ with $U \subseteq V$, consider the natural map:

$$f_{U,V} : G/U \to G/V : gU \mapsto gV.$$

Then it is clear that $(G/U, f_{U,V})_{\mathcal{S}}$ is an inverse system of groups.
If we consider the compatible family of canonical homomorphisms $\varphi_U : G \to G/U$, $U \in \mathcal{S}$, we get a map

$$\varphi : G \to s\varprojlim_{\mathcal{S}} G/U \subseteq \prod_{U\in\mathcal{S}} G/U.$$

We will show that φ is injective, continuous and surjective. And then, because G is compact, we will get that φ is a topological isomorphism (see [**Mun75**, Theorem 26.6]).

- φ **is injective:** Let $\sigma \in G$ with $\varphi(\sigma) = 1$. Then we have $\sigma \in U$ for all $U \in \mathcal{S}$, which implies $\sigma \in \cap_{U\in\mathcal{S}} U = \{1\}$.
- φ **is continuous:** We will prove that the composition

$$G \xrightarrow{\varphi} s\varprojlim_{\mathcal{S}} G/U \xrightarrow{\pi_U} G/U$$

is continuous for each $U \in \mathcal{S}$. In fact, it is enough because $s\varprojlim_{\mathcal{S}} G/U \subseteq \prod_{U\in\mathcal{S}} G/U$ (see [**Mun75**, Theorem 19.6]). But

$$(\pi_U\varphi)^{-1}\{1\} = \varphi^{-1}(\pi_U^{-1}(\{1\})) = U$$

is open in G.
(Notice that $\{1\}$ is a basis of open neighborhood of 1 in G/U for all $U \in \mathcal{S}$ - because $\{1\}$ was already a basis of open neighborhood in G.)
- φ **is surjective:** By lemma 2.4 $\varphi(G)$ is dense in $s\varprojlim_{\mathcal{S}} G/U$. Let us show that $\varphi(G)$ closed, hence $\varphi(G) = s\varprojlim_{\mathcal{S}} G/U$. $\varphi(G)$ is closed because we have $\varphi(G) = \pi_U^{-1}(\varphi_U(G)) = \pi_U^{-1}(G/U)$ (we use that φ_U is surjective) and π_U is continuous.

□

Remark 2.1. Some authors, considering theorem 2.5, define the profinite groups to be the Hausdorff, compact, totally disconnected topological groups.

Corollary 2.6. *Let G be a profinite group. Then if $\mathcal{S} :=$ {open, normal subgroups of G}, we have*

$$G \cong \varprojlim_{U\in\mathcal{S}} G/U.$$

2.3. Consequences of the theorem.

Proposition 2.7. *Let G be a profinite group.*

(1) Let $\{H_i \mid i \in I\}$ be a collection of closed subgroups of G and let $\cap_{i\in I} H_i \leq U \leq G$ where U is an open subgroup of G.
Then there is a finite subset J of I such that $\cap_{j\in J} H_j \leq U$.

(2) Let $\{U_i \mid i \in I\}$ be a collection of open subgroups of G such that $\cap_{i\in I} U_i = 1$. Let $\mathcal{V} = \{\cap_{j\in J} U_j \mid J \subseteq I \ finite\}$
Then $\mathcal{V}$ is a fundamental system of neighborhood of 1 in G.

Proof. (1) Consider the open covering $\{G\backslash H_i \mid i \in I\}$ of the compact space $G\backslash U$ (note that $G\backslash U$ is a closed subset of the compact space G). So there is a finite subcovering $\{G\backslash H_j \mid j \in J\}$ for a finite subset J of I. This means

$$G\backslash U \subseteq \bigcup_{j\in J} G\backslash H_j,$$

and so

$$\bigcap_{j\in J} G\backslash H_j \subseteq U.$$

(2) Follows from (1).

□

Proposition 2.8. *A closed subgroup H of a profinite group G is profinite. Precisely, if $G = \varprojlim_{\mathcal{S}} G/U$ with $\mathcal{S} = \{open,\ normal\ subgroups\ of\ G\}$, then*

$$H \cong \varprojlim_{\mathcal{S}} HU/U \cong \varprojlim_{\mathcal{S}} H/H \cap U.$$

Proof. We use the characterization of theorem 2.5. Clearly H is Hausdorff and totally disconnected because so is G. The theorem [**Mun75**, Theorem 26.2, Chapter 3] implies that H is compact (because H is closed).
The second assertion follows from lemma 2.4. In fact, the canonical maps

$$\varphi_U : H \to HU/U$$
$$\pi_U : H \to H/H \cap U$$

are surjective for all U in $\mathcal{S}$. □

Proposition 2.9. *A quotient group G/H of a profinite group G by a closed subgroup H is a profinite group. In fact, if $\mathcal{S} = \{open,\ normal\ subgroups\ of\ G\}$, then*

$$G/H \cong \varprojlim_{\mathcal{S}} G/HU.$$

Proof. Consider the canonical projection

$$\pi : G \to G/HU,$$

which is a surjective map. As $\pi(H) = 0$, we can define

$$\widetilde{\pi} : G/H \to G/HU$$

and use again lemma 2.4. □

Proposition 2.10. *Let I be a set of index, and let $(G_i)_{i\in I}$ be profinite groups. Then $G := \prod_{i\in I} G_i$ is a profinite group.*

Proof. Clear since the product of Hausdorff, compact and totally disconnected groups is again Hausdorff, compact and totally disconnected. □

Corollary 2.11. *Let $(G_i, f_{ij})_I$ be an inverse system of profinite groups. Then $G = \varprojlim_I G_i$ is profinite.*

Proof. Use proposition 1.3 to see that G is a closed subgroup of $\prod_{i\in I} G_i$, and use corollary 2.11. □

Example 2.2. Let $\mathbb{P}$ be the set of all prime numbers. We will show that

$$\widehat{\mathbb{Z}} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p.$$

We construct the natural projection

$$\alpha_p^m : \mathbb{Z}_p \to \mathbb{Z}/p^{m_p}\mathbb{Z}$$

where $m = \prod_{q\in\mathbb{P}} q^{m_q}$.
Then we have the map

$$\alpha^m : \prod_{p\in\mathbb{P}} \alpha_p^m : \prod_{p\in\mathbb{P}} \mathbb{Z}_p \to \prod_{p\in\mathbb{P}} \mathbb{Z}/p^{m_p}\mathbb{Z},$$

which is onto (one can easily build an inverse image).
Note that, using the Chinese reminder theorem (see [**Lan02a**, Corollary 2.2, §2, Chapter 2]), we have

$$\prod_{p\in\mathbb{P}} \mathbb{Z}/p^{m_p}\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}.$$

Using lemma 2.4, the maps α^m, $m \in \mathbb{Z}$, induce a continuous surjection

$$\alpha : \prod_{p\in\mathbb{P}} \mathbb{Z}_p \to \widehat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}.$$

On the other hand, let $(x_p)_{p\in\mathbb{P}}$ be an element of $\prod_{p\in\mathbb{P}} \mathbb{Z}_p$ such that $\alpha((x_p)_\mathbb{P}) = 0$. This means $\alpha^m((x_p)_\mathbb{P}) = 0$ for each $m \in \mathbb{Z}$ (by definition of $\widehat{\mathbb{Z}}$). Consequently $\alpha_q^m((x_p)_\mathbb{P}) = 0$ for each $m \in \mathbb{Z}$, and each $q \in \mathbb{P}$. So $x_p = 0$ for all $p \in \mathbb{P}$, i.e. $(x_p)_\mathbb{P} = 0$. This implies that α is injective.
Since $\prod_{p\in P} \mathbb{Z}_p$ is compact, we get that α is a topological isomorphism (see [**Mun75**, Theorem 26.6, Chapter 3]).

Proposition 2.12. *$\varprojlim$ is an exact functor from the category of inverse systems, over a directed indexing set I, of profinite groups to the category of profinite groups.*

Proof. Let

$$\begin{tikzcd} 1 \arrow[r] & (H_i, \varphi_{ij}) \arrow[r, "(f_i)_I"] & (G_i, \psi_{ij}) \arrow[r, "(g_i)_I"] & (K_i, \eta_{ij}) \arrow[r] & 1 \end{tikzcd}$$

be an exact sequence of inverse systems (over I) of profinite groups. We have to show that

$$\begin{tikzcd} 1 \arrow[r] & \varprojlim_I H_i \arrow[r, "f"] & \varprojlim_I G_i \arrow[r, "g"] & \varprojlim_I K_i \arrow[r] & 1 \end{tikzcd}$$

is exact.

- We first show that f is injective:
  Let $(x_i)_I \in \varprojlim_I H_i$ with $f((x_i)_I) = 0$. Then $f_i(x_i) = 0$ for each i in I. And as f_i is injective $x_i = 0$, for each $i \in I$. Hence $(x_i)_I = 0$.
- Next, we prove $\ker(g) = \operatorname{im}(f)$:
  Let $(x_i)_I \in \varprojlim_I H_i$,

  $$(g \circ f)((x_i)_I) = g((f_i(x_i))_I) = ((g_i \circ f_i)(x_i))_I = 0$$

  because the sequence of projective systems is exact. This implies $\operatorname{im}(f) \subseteq \ker(g)$.
  Let $(y_i)_I \in \ker(g)$. This is equivalent to $g((y_i)_I) = 0$ and so $(g_i(y_i))_I = 0$. Consequently $y_i \in \ker(g_i)$ for all i in I. And as the sequence of projective systems is exact, there is a $x_i \in H_i$ such that $f_i(x_i) = y_i$ for each $i \in I$. Hence $\ker(g) \subseteq \operatorname{im}(f)$.

- Finally we have to show the surjectivity of g:
  Let $(z_i)_I \in \varprojlim_I K_i$. Consider the set $Y_i = g_i^{-1}(x_i)$ which is compact in G_i as inverse image of a closed subset. Note that $(g_i)_I$ being a morphism in the category of inverse system implies if $i \leq j$
  $$\begin{tikzcd} G_j \arrow[r, "\varphi_{ij}"] \arrow[d, "g_j"'] & G_i \arrow[d, "g_i"] \\ K_j \arrow[r, "\eta_{ij}"'] & K_i \end{tikzcd}$$
  So if $i \leq j$, we have $\psi_{ij}(Y_j) \subseteq Y_i$, in fact
  $$\begin{aligned} g_i(\psi_{ij}(y_j)) &= (g_i \circ \psi_{ij})(y_j) \\ &= (\eta_{ij} \circ g_j)(y_j) \\ &= \eta_{ij}(x_j) = x_i, \end{aligned}$$
  for each $y_j \in Y_j$. Consequently (Y_i, ψ_{ij}) is an inverse system of non-empty compact sets. Hence $\varprojlim_I Y_i \neq \emptyset$ (see [**Bou71**, Proposition 8, §9, Chapter 1]). As for each $(y_i)_I \in \varprojlim_I Y_i$, we have $g((y_i)_I) = (x_i)_I$, hence the result.

□

3. Galois groups and profinite groups

We have already seen in chapter 2 (theorem 2.6) that Galois groups are Hausdorff, compact and totally disconnected. But as seen in theorem 2.5, so are the profinite groups. This section will make that more clear.

Theorem 3.1. *Assume $\mathbb{L}$ is a Galois extension of a field $\mathbb{K}$. We fix $\mathcal{F} = \mathcal{F} = \{\mathbb{E} \mid \mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L},\ \mathbb{E}\ finite\ Galois\ extension\ of\ \mathbb{K}\}$. Then* $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ *is the inverse limit of the finite groups* $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$ *with $\mathbb{E} \in \mathcal{F}$; in particular,* $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ *is a profinite group.*

Proof. From the Galois theory $\mathrm{Gal}(\mathbb{E}, \mathbb{K})$ is a finite group. If $\mathbb{E}_1, \mathbb{E}_2 \in \mathcal{F}$ with $\mathbb{E}_1 \subseteq \mathbb{E}_2$, we define
$$\begin{aligned} \varphi_{\mathbb{E}_1\mathbb{E}_2} : \mathrm{Gal}(\mathbb{E}_2, \mathbb{K}) &\rightarrow \mathrm{Gal}(\mathbb{E}_1, \mathbb{K}) \\ \sigma &\mapsto \sigma|_{\mathbb{E}_1}. \end{aligned}$$
Then $(\mathrm{Gal}(\mathbb{E}, \mathbb{K}), \varphi_{\mathbb{E}_1\mathbb{E}_2})_{\mathcal{F}}$ is an inverse system indexed with $\mathcal{F}$.
Considering the restriction maps $\mathrm{Gal}(\mathbb{L}, \mathbb{K}) \rightarrow \mathrm{Gal}(\mathbb{E}, \mathbb{K})$, we get a group homomorphism $\theta : \mathrm{Gal}(\mathbb{L}, \mathbb{K}) \rightarrow \prod_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K})$. The image of θ in contained in $\varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K})$, because
$$\varphi_{\mathbb{E}_1,\mathbb{E}_2}(\pi_{\mathbb{E}_2}(\theta(\sigma))) = \varphi_{\mathbb{E}_1,\mathbb{E}_2}(\sigma|_{\mathbb{E}_2}) = \sigma|_{\mathbb{E}_1} = \pi_{\mathbb{E}_1}(\theta(\sigma)).$$
Now given $(\sigma_{\mathbb{E}})_{\mathbb{E}\in\mathcal{F}} \in s \varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K})$ and $x \in \mathbb{K}$, we build
$$\psi((\sigma_{\mathbb{E}}))(x) = \sigma_{\mathbb{M}}(x)$$
for $\mathbb{M} \in \mathcal{F}$ an intermediary extension with $x \in \mathbb{M}$ (which always exists). This construction of ψ is independent of the choice of $\mathbb{M}$ because σ is in $\varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K})$. We can easily see that $\psi((\sigma_{\mathbb{E}})) \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ and that ψ is the inverse of θ. Then θ is an isomorphism. And so $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ is isomorphic to $\varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K})$ as abstract groups.
We will now show that there is an isomorphism between the basis of the topology of 1.
recall that the basis of open neighborhood of 1 in $\varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K})$ is given by
$$\{\ker(\pi_{\mathbb{E}}) \mid \mathbb{E} \in \mathcal{F}\}$$
(see proposition 3.3). But for every $\mathbb{F} \in \mathcal{F}$, we have
$$\ker(\pi_{\mathbb{F}}) = \{(\sigma_{\mathbb{E}}) \in s \varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K}) \mid \pi_{\mathbb{F}}((\sigma_{\mathbb{E}})) = \mathrm{Id}_{\mathbb{F}}\}$$

Note that

$$\theta(\mathrm{Gal}(\mathbb{L},\mathbb{F})) = \prod_{\mathbb{E}\in\mathcal{F}\setminus\{\mathbb{F}\}} \mathrm{Gal}(\mathbb{E},\mathbb{K}) \times \{\mathrm{Id}_{\mathbb{F}}\}$$

and as $\mathrm{im}(\theta) \subseteq s\varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E},\mathbb{K})$, we obtain that

$$\ker(\pi_{\mathbb{F}}) = \theta(\mathrm{Gal}(\mathbb{L},\mathbb{F}))$$

for all $\mathbb{F} \in \mathcal{F}$. This proves that we have a homeomorphism, hence

$$\mathrm{Gal}(\mathbb{L},\mathbb{K}) \cong s\varprojlim_{\mathbb{E}\in\mathcal{F}} \mathrm{Gal}(\mathbb{E},\mathbb{K}).$$

□

Proof. You can find a proof of this lemma in [**Wil98**, Chapter 3.3]. □

Theorem 3.2. *Every profinite group G is isomorphic (as a topological group) to a Galois group.*

Proof. Recall that G is a Hausdorff compact totally disconnected topological group (see 2.5).
Let $\mathbb{F}$ be an arbitrary field. We consider S the disjoint union of the sets G/N with N running through the collection of open normal subgroups of G (we write $N <_O G$). Think of the elements of S as indeterminates, and build the field $\mathbb{L} = \mathbb{F}(S)$ (the rationals functions with coefficients in $\mathbb{F}$ with their indeterminates in S).
The group G operates on S in a natural way: if $g \in G$ and $g'N \in G/N$, then $g(g'N) = gg'N$ (for any $N \in S$). And so, this induces an action of G on $\mathbb{L}$.
Define $\mathbb{K} = \mathbb{L}^G$ the subfield of $\mathbb{L}$ consisting of the elements of $\mathbb{K}$ fixed by G.
Our goal is now to show that $\mathbb{L}$ is a Galois extension of $\mathbb{K}$ with Galois group G.
If $\alpha \in \mathbb{L}$, consider the subgroup of G

$$G_\alpha = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}.$$

If the indeterminates that appear in the rational expression of α are $\{t_i \in G/N_i \mid i = 1,\dots,n\}$, then

$$\{1\} \subseteq \bigcap_{i=1}^{n} N_i \subseteq G_\alpha.$$

In fact, if $n \in N_i$ and $gN_i \in G/N_i$, we have

$$n(gN_i) = ngN_i = gg^{-1}ngN_i = gN_i,$$

because $g^{-1}ng \in N_i$ (as N_i is a normal subgroup of G). This means the action of N_i on G/N_i is trivial. As all the N_i are open subgroups of G, $\cap_{i=1}^{n} N_i$ is open. Then using proposition 4.4 part (4) (in Chapter 1) we get that G_α is open. And hence, using the same proposition (part (2)), G_α has finite index.
As the index of the isotropy group of an element is equal to the cardinality of its orbit. Then the orbit of α under the action of G is finite. Suppose that this orbit is $O_\alpha = \{\alpha_1,\dots,\alpha_r\}$ (with all the α_i different) and consider the polynomial

$$f(X) = \prod_{i=1}^{r} (X_{\alpha_i}).$$

As G transforms O_α into itself (because of the definition of an orbit), we have that α_i is in $\mathbb{K}$ for all $1 \leq i \leq r$, which means that $f(X) \in \mathbb{K}[X]$. But as a root of $f(X)$, α is then algebraic over $\mathbb{K}$. Furthermore, notice that all the roots of $f(X)$ are different and this means that α is separable over $\mathbb{K}$. And so $\mathbb{L}$ is a separable extension of $\mathbb{K}$.
Observe that $\mathbb{K}[\alpha_1,\dots,\alpha_r]$ is a normal extension of $\mathbb{K}$ (as splitting field of a non constant polynomial $f(X) \in \mathbb{K}[X]$). And so $\mathbb{L}$ is a union of normal extensions of $\mathbb{K}$, hence $\mathbb{L}$ is normal over $\mathbb{K}$.
So we have proved that $\mathbb{L}$ is a Galois extension of $\mathbb{K}$.

We write $H := \text{Gal}(\mathbb{L}, \mathbb{K})$. Clearly, as G acts on $\mathbb{L}$ and fixes $\mathbb{K} = \mathbb{L}^G$, $G \subseteq H$. We will now prove the equality. Consider $i : G \hookrightarrow H$ the inclusion map. The next step will be to show that this map is continuous.

Let U be a normal open subgroup of H and consider $\mathbb{L}^U$. As U have finite index (see proposition 4.4 in Chapter 1), $\mathbb{L}^U$ is a finite Galois extension of $\mathbb{K}$ (use the theorem 3.3 in Chapter 2). Suppose $\mathbb{L}^U = \mathbb{K}(\alpha'_1, \ldots, \alpha'_s)$ for some $\alpha'_i \in \mathbb{L}$. Then

$$G \cap U \supseteq \bigcap_{i=1}^{s} G_{\alpha'_i}.$$

Which implies that $G \cap U$ is open (because containing an open subgroup - see proposition 4.4 in Chapter 1). Then we have that G is open, and so G is a closed subgroup of H.

To conclude, use the theorem about infinite Galois extensions (theorem 3.3 in Chapter 2) : as $\mathbb{L}^G = \mathbb{L}^H$ and G is closed, $H = G$. □

CHAPTER 4

Group Cohomology

In the following chapter, we define cohomology groups. This notion come from topology, they were later used in group theory in order to provide invariants.
Many proofs in this chapter will be left to the reader.

1. Generalities

1.1. (Co)homology modules.

Definition 1.1. A *left R-module*, where R is a ring, is an abelian group $(M, +)$, having a scalar multiplication $R \times M \to M : (r, m) \mapsto r \cdot m$ such that for all $m, m' \in M$ and all $r, r' \in R$, we have

(1) $r \cdot (m + m') = r \cdot m + r \cdot m'$,
(2) $(r + r') \cdot m = r \cdot m + r' \cdot m$,
(3) $(rr') \cdot m = r \cdot (r' \cdot m)$,
(4) $1 \cdot m = m$.

Definition 1.2. Let M and N be two R-modules, a R-map (or a R-homomorphism) is a group homomorphism $f : M \to N$, such that, for all $m \in M$ and $r \in R$,

$$r \cdot f(m) = f(r \cdot m).$$

We can define similarly a right R-module, but in the case R is commutative they coincide. Therefore, to make it easier, we assume from now on that R is a commutative ring.

Notation 1.3.

(1) Often we write rm instead of $r \circ m$ to denote the action of R on a R-module M.
(2) The class of R-modules and R-maps is an abelian category denoted by $\mathscr{M}_R$.

We present here the most general notion of (co)homology.

Definition 1.4. A *chain complex* C over R is a sequence of R-modules $(C_n)_{n\in\mathbb{Z}}$ and R-maps $(d_n : C_n \to C_{n-1})_{n\in\mathbb{Z}}$, called *differentiations*,

$$C : \ldots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \to \ldots$$

such that $d_n \circ d_{n+1} = 0$ for all $n \in \mathbb{Z}$.

Definition 1.5. A *morphism of chain complexes* $f : C \to C'$ is a collection of morphisms of R-modules $(f_n : C_n \to C'_n)_{n\in\mathbb{Z}}$ such that the following diagram commutes for all n,

$$\begin{tikzcd} C_n \arrow[r, "d_n"] \arrow[d, "f_n"'] & C_{n-1} \arrow[d, "f_{n-1}"] \\ C'_n \arrow[r, "d'_n"'] & C'_{n-1}. \end{tikzcd}$$

Definition 1.6. Let C be a chain complex, we define its *n-th homology module* by

$$H_n(C) := \ker d_n / \operatorname{im} d_{n+1}.$$

If $f : C \to C'$ is a morphism of chain complexes, we define

$$\begin{array}{rcl} H_n(f) : H_n(C) & \to & H_n(C') \\ {[z]} & \to & [f_n(z)]. \end{array}$$

And here is the definition of cohomology.

Definition 1.7. A *cochain complex* C over R is a sequence of R-modules $(D_n)_{n\in\mathbb{Z}}$ and R-maps $(\delta_n : C_n \to C_{n-1})_{n\in\mathbb{Z}}$,

$$D : \ldots \to D^{n-1} \xrightarrow{\delta^{n-1}} D^n \xrightarrow{\delta_n} D^{n+1} \to \ldots$$

such that $\delta^{n+1} \circ \delta^n = 0$ for all $n \in \mathbb{Z}$.

Definition 1.8. Let D be a cochain complex, we define its *n-th cohomology module* by

$$H^n(D) := \ker \delta^n / \operatorname{im} \delta^{n-1}.$$

1.2. Hom Functor.

Definition 1.9. Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A *covariant functor* F from $\mathscr{C}$ to $\mathscr{D}$ is a mapping that associates to each object $C \in \mathscr{C}$ an object $F(C) \in \mathscr{D}$ and associates to each morphism $f : C_1 \to C_2$ in $\mathscr{C}$ a morphism $F(f) : F(C_1) \to F(C_2)$ in $\mathscr{D}$; such that

- $F(id_C) = id_{F(C)}$, for every object $C \in \mathscr{C}$;
- $F(g \circ f) = F(g) \circ F(f)$, for all morphisms $f : C_1 \to C_2$ and $g : C_2 \to C_3$ in $\mathscr{C}$.

A *contravariant functor* F from $\mathscr{C}$ to $\mathscr{D}$ is a mapping that associates to each object $C \in \mathscr{C}$ an object $F(C) \in \mathscr{D}$ and associates to each morphism $f : C_1 \to C_2$ in $\mathscr{C}$ a morphism $F(f) : F(C_2) \to F(C_1)$ in $\mathscr{D}$; such that

- $F(id_C) = id_{F(C)}$, for every object $C \in \mathscr{C}$;
- $F(g \circ f) = F(f) \circ F(g)$, for all morphisms $f : C_1 \to C_2$ and $g : C_2 \to C_3$ in $\mathscr{C}$.

Definition 1.10. Let M be a fixed R-module.
We define the functor $\operatorname{Hom}(\square, M)$ from the category $\mathscr{M}_R$ to the category $\mathscr{A}$, sending each R-module N to the set of all R-maps from N to M : $\operatorname{Hom}_R(N, M)$ and sending each R-map $\varphi : N_1 \to N_2$ to the map

$$\operatorname{Hom}(f, M) : \operatorname{Hom}(N_2, M) \to \operatorname{Hom}(N_1, M) : f \mapsto f \circ \varphi.$$

Next, we define the functor $\operatorname{Hom}(M, \square)$ from the category $\mathscr{M}_R$ to the category $\mathscr{A}$, sending each R-module N to the set of all R-maps from M to N : $\operatorname{Hom}_R(M, N)$ and sending each R-map $\varphi : N_1 \to N_2$ to the map

$$\operatorname{Hom}(f, M) : \operatorname{Hom}(M, N_1) \to \operatorname{Hom}(M, N_2) : f \mapsto \varphi \circ f.$$

Proposition 1.1.

- $\operatorname{Hom}_R(\square, M)$ *is a well-defined contravariant functor from* $\mathscr{M}_R$ *to* $\mathscr{A}$*. Moreover this functor is left-exact.*
- $\operatorname{Hom}_R(M, \square)$ *is a well-defined covariant functor from* $\mathscr{M}_R$ *to* $\mathscr{A}$*. Moreover this functor is left-exact.*

Proof. One can find the proof in [**Rot09**, §2.1]. □

Remark 1.11. There are many ways to obtain a cochain complex from a chain complex C. The most natural is to define $C^n := C_{-n}$ and $\delta_m := d_{-n}$.
But there is another one more interesting: we simply have to apply the functor $Hom(\square, G)$. Precisely, $C^n := \operatorname{Hom}_R(C_n, R)$ and $\delta^n := d^*_{n+1} = \operatorname{Hom}_R(d_{n+1}, R)$. We will denote this cochain complex:

$$\operatorname{Hom}_R(C, R) : \ldots \to \operatorname{Hom}_R(C_{n-1}, R) \xrightarrow{\delta^{n-1}} \operatorname{Hom}_R(C_n, R) \xrightarrow{\delta_n} \operatorname{Hom}_R(C_{n+1}, R) \to \ldots$$

The following theorems are two classical result.

Theorem 1.2. *Let* $0 \to C' \xrightarrow{i} C \xrightarrow{p} C'' \to 0$ *be an exact sequence of chain complexes. Then there is a long exact sequence of modules*

$$\ldots \to H_n(C') \xrightarrow{H_n(i)} H_n(C) \xrightarrow{H_n(p)} H_n(C'') \xrightarrow{\delta_n} H_{n-1}(C') \to \ldots .$$

Proof. One can find a proof of this theorem in [**Rot09**, §6.1]. □

Theorem 1.3. *Let* $0 \to C' \xrightarrow{i} C \xrightarrow{p} C'' \to 0$ *be an exact sequence of cochain complexes. Then there is a long exact sequence of modules*

$$\ldots \to H^n(C') \xrightarrow{H^n(i)} H^n(C) \xrightarrow{H^n(p)} H^n(C'') \xrightarrow{\delta^n} H^{n+1}(C') \to \ldots .$$

2. Projective and injective modules

In this section we will define the notion of projective and injective modules.

Definition 2.1. A R-module P is *projective* if for any epimorphism of R-modules $\beta : M \to N$ and any morphism $\alpha : P \to N$ there exists a morphism $\gamma : P \to M$ such that $\beta \circ \gamma = \alpha$, i.e. such that the following diagram commutes

$$\begin{tikzcd}
 & P \arrow[dl, dotted, "\gamma"'] \arrow[d, "\alpha"] & \\
M \arrow[r, "\beta"] & N \arrow[r] & 0.
\end{tikzcd}$$

We present a theorem which will gives us another characterization of projective modules.

Theorem 2.1. *Let P be a R-module. Then the following assertions are equivalent:*

(1) P is projective,
(2) $\mathrm{Hom}(P, \Box)$ is exact,
(3) every exact sequence of R-modules $0 \to M' \to M \to P \to 0$ splits,
(4) P is a summand of a free module, i.e. there exists a R-module M such that $P \oplus M$ is free.

Proof. The proof is given in [**Rot09**, Proposition 3.2, Proposition 3.3 & Theorem 3.5, Chapter 3]. □

We now define precisely what is a R-module.

Definition 2.2. A R-module M is said to be *free* if there exists a set $X = \{m_i \mid i \in I\}$ (I can be any index set), called a basis of M, such that each $m \in M$ has a unique expression

$$m = \sum_{i \in I} r_i m_i$$

for some $r_i \in R$ with $r_i \neq 0$ only in finite many case.

Proposition 2.2. *Let F be a free R-module and M, N be any R-modules. If $\beta : M \to N$ is an epimorphism, then for every $\alpha : F \to N$, there exists an R-homomorphism $\gamma : F \to M$ making the following diagram commutes*

$$\begin{tikzcd}
 & F \arrow[dl, dotted, "\gamma"'] \arrow[d, "\alpha"] & \\
M \arrow[r, "\beta"] & N \arrow[r] & 0.
\end{tikzcd}$$

Proof. One can find a proof of this proposition in [**Rot09**, Theorem 3.1, Chapter 3]. □

Corollary 2.3. *Every free module is a projective module.*

We define now the dual notion of projective modules, the injective modules.

Definition 2.3. A R-module I is *injective* if for any monomorphism $\beta : M \to N$ and any morphism of R-modules $\alpha : M \to I$ there is a morphism $\gamma : N \to I$ such that $\gamma \circ \beta = \alpha$, i.e. the following diagram commutes

$$\begin{tikzcd} & I & \\ 0 \arrow[r] & M \arrow[u, "\alpha"] \arrow[r, "\beta"'] & N. \arrow[ul, dotted, "\gamma"'] \end{tikzcd}$$

Theorem 2.4. *Let I be a R-module. Then the following assertions are equivalent:*

(1) I is injective,
(2) $\mathrm{Hom}_R(\Box, I)$ is an exact functor,
(3) every exact sequence of R-modules $0 \to I \to M \to M' \to 0$ splits.

Proof. The proof can be found in [**Rot09**, Proposition 3.25 & 3.26, §3.2]. □

3. Resolutions and Cohomology of R-modules

3.1. Resolutions.

We now define a resolutions of modules which will provide the chain complexes used to define cohomology.

Definition 3.1. Let M be a R-module. A *projective* (resp. *free*) *resolution* of M over R is an exact sequence of R-modules

$$\ldots \to P_n \xrightarrow{d_n} P_{n-1} \to \ldots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0,$$

where each P_n s a projective (resp. free) module.

Notation 3.2. Such a projective resolution is sometimes denoted by $P_\bullet \to M$.

Those resolutions are not only useful, we now that one can always find such a resolution for any R-module.

Theorem 3.1. *Every R-module has a free resolution.*

Proof. Refer to [**Rot09**, Proposition 6.2, §6.1]. □

Corollary 3.2. *Every R-module has a projective resolution.*

Definition 3.3. Let M be a R-module. A *injective resolution* of M over R is an exact sequence of R-modules

$$0 \to M \xrightarrow{\varepsilon} I^0 \xrightarrow{\delta^0} I^1 \to \ldots \to I^n \xrightarrow{\delta^n} I^{n+1} \to \ldots,$$

where each I^n is an injective module.

Notation 3.4. Such an injective resolution is sometimes denoted by $M \to I^\bullet$.

Theorem 3.3. *Every R-module has an injective resolution.*

Proof. Refer to [**Rot09**, Proposition 6.4, §6.1]. □

Now we define the deleted (co)complexes because they are easier to deal with.

Definition 3.5. Let M be a R-module. If

$$X : \ldots \to X_n \xrightarrow{d_n} X_{n-1} \to \ldots \to X_1 \to X_0 \to M \to 0$$

is a chain complex, we define the *deleted complex* of X to be the chain complex

$$X_M : \ldots \to X_n \xrightarrow{d_n} X_{n-1} \to \ldots \to X_1 \to X_0 \to 0.$$

Similarly if

$$Y : 0 \to M \to Y^0 \xrightarrow{\delta^0} Y^1 \to \ldots \to Y^n \xrightarrow{\delta^n} Y^{n+1} \to \ldots$$

is a cochain complex, we define the *deleted cocomplex* of Y to be the cochain complex

$$Y_M : 0 \to Y^0 \xrightarrow{\delta^0} Y^1 \to \ldots \to Y^n \xrightarrow{\delta^n} Y^{n+1} \to \ldots$$

3.2. Cohomology of R-modules.

In this section we define the functor Ext, which is a generalisation of the cohomology.

Definition 3.6. Let M, N be R-modules. Let P_M be the deleted complex of a projective resolution of M. Form the complex $\mathrm{Hom}_R(P_M, N)$, i.e.

$$\mathrm{Hom}_R(P_M, N) : 0 \to \mathrm{Hom}_R(P_0, N) \xrightarrow{d_1^*} \ldots \to \mathrm{Hom}_R(P_n, N) \xrightarrow{d_{n+1}^*} \mathrm{Hom}_R(P_{n+1}, N) \to \ldots$$

We define the *n-th cohomology* of M with coefficients in N, $\mathrm{Ext}^n_R(M, N)$, by taking the n-th cohomology of the above cochain complex, i.e.

$$\mathrm{Ext}^n_R(M, N) := H^n(\mathrm{Hom}(P_M, N)).$$

Theorem 3.4. *Let M, N be R-modules, and let P_M and P'_M be to projective resolutions of M. Suppose that $\mathrm{Ext}^n_R(M, N)$, respectively $\mathrm{Ext}'^n_R(M, N)$, is the cohomology module associated to P_M, respectively P'_M. Then*

$$\mathrm{Ext}^n_R(M, N) \cong \mathrm{Ext}'^n_R(M, N).$$

Proof. The proof id given in [**Rot09**, Proposition 6.40, §6.2]. □

Remark 3.7. Some authors define the cohomology of M with coefficients in N using injective resolutions.

Let I_N be the deleted complex of an injective resolution of N. Then form the complex $\mathrm{Hom}_R(M, I_N)$, i.e.

$$\mathrm{Hom}_R(M, I_N) : 0 \to \mathrm{Hom}_R(M, I^0) \to \ldots \to \mathrm{Hom}_R(M, I^n) \xrightarrow{\delta^n_*} \mathrm{Hom}_R(M, E^{n+1}) \to \ldots$$

Then the *n-th cohomology* of M with coefficients in N is

$$H^n(M, N) = H^n(\mathrm{Hom}_R(M, I_N)).$$

There is no ambiguity with the above definition since in [**Rot09**, Theorem 6.67, §6.2], it is proved that

$$H^n(\mathrm{Hom}(M, I_N)) = H^n(\mathrm{Hom}(P_M, N)).$$

4. Cohomology of groups

We will now define precisely the cohomology of groups. R is always a commutative ring with identity 1.

Definition 4.1. Let G be a group, the *group ring* R[G] is the free abelian group with basis G, i.e. the group of all formal linear combinations of elements of G with coefficients in R (and endowed with the multiplication induced by the multiplication of G).

$$R[G] = \{ \sum_{\substack{g \in G \\ finite}} r_g g \mid r_g \in R\}.$$

The *integral group* is the group ring for the ring of integral numbers $\mathbb{Z}$, i.e. $\mathbb{Z}[G]$. This ring is also written $\mathbb{Z}G$.

Definition 4.2. Let $(G, \cdot)$ be a group. A *G-module* is an abelian group $(M, +)$ with a map $G \times M \to M : (g, m) \mapsto g \cdot m$ satisfying:

(1) $(g_1 g_2) \cdot (m) = g_1 \cdot (g_2 \cdot m)$;
(2) $g \cdot (m + n) = g \cdot m + g \cdot n$;

(3) $1_G \cdot m = m$;

for $m, n \in M$ and $g_1, g_2, g \in G$.

Remark 4.3. If M is a G-module, then M becomes a $\mathbb{Z}G$-module if we define

$$(\sum_{\substack{g \in G \\ finite}} n_g g) \cdot m = \sum_{\substack{g \in G \\ finite}} n_g (g \cdot m).$$

Conversely, if M is a $\mathbb{Z}G$-module, then M becomes a G-module if we define $g \cdot m = (1g) \cdot m$.

Definition 4.4. Let G be a group. A G-module M is called *trivial* if every element of G acts as the identity on M, i.e. $g \cdot m = m$.

Definition 4.5. Let G be a group, and M a G-module. Consider the integers $\mathbb{Z}$ as a trivial G-module and define the *n-th cohomology group* of G with coefficients in M to be

$$H^n(G, N) := \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, N).$$

5. Shapiro's Lemma and induced modules

We will present the Lemma of Shapiro and the induced modules. They will be later useful to study the cohomology of Galois groups.

Let G be a group.

Definition 5.1. A $\mathbb{Z}G$-module A is *G-acyclic* if $H^n(G, A) = \{0\}$ for all $n \geq 1$.

Definition 5.2. A group homomorphism $f : G' \to G$ induces a ring homomorphism $\mathbb{Z}G' \to \mathbb{Z}G$, also denoted by f, precisely, $f : \sum n_{g'} g' \mapsto \sum n_{g'} f(g')$. Let A be a $\mathbb{Z}G$-module, it can be considered as a $\mathbb{Z}G'$-module : if $g' \in G'$ and $a \in A$, then $g'a = f(g')a$. Denote a G-module A viewed as a G'-module by UA, and call

$$U_f : \mathscr{M}_{\mathbb{Z}G} \to \mathscr{M}_{\mathbb{Z}G'}$$

a *change of groups functor.*

Lemma 5.1. *Let $f : G' \to G$ be a group homomorphism, and let $U_f : \mathscr{M}_{\mathbb{Z}G} \to \mathscr{M}_{\mathbb{Z}G'}$ be the corresponding change of groups functor.*

(1) If $\boldsymbol{P}$ is a G-cyclic complex, then $U\boldsymbol{P}$ is a G'-cyclic complex.

(2) Let $H \subseteq G$, and let $f : H \to G$ be the inclusion homomorphism. If P is a projective G-module, then UP is a projective H-module. Moreover, if $\boldsymbol{P}$ is a projective resolution of a $\mathbb{Z}G$-module A over $\mathbb{Z}G$, then $U\ \boldsymbol{P}$ is an projective resolution of UA over $\mathbb{Z}S$-

Proof. (1) Using [**Rot09**, Proposition 8.3, §8.2], we now that $U : \mathscr{M}_{\mathbb{Z}G} \to \mathscr{M}_{\mathbb{Z}G'}$ is an exact additive functor. Then $U\boldsymbol{P}$ is a complex, moreover $H^n(G', A) = \{0\}$.

(2) Consider R a set containing an element (and only one) of each coset of G/H. Then G is the disjoint union $\cup_{r \in R} rH$. This implies that for every $g \in G$ there are unique $r \in R$ and $h \in H$ such that $g = rh$. And hence, we can write $\mathbb{Z}G = \bigoplus_{r \in R} r(\mathbb{Z}H)$ (a direct sum is $\mathbb{Z}S$-module), so $\mathbb{Z}G$ is a free $\mathbb{Z}H$-module.

Suppose that P is a projective $\mathbb{Z}G$-module. This is equivalent to the existence of a $\mathbb{Z}G$-module M such that $P \oplus M$ is free. And so UP is a a projective $\mathbb{Z}H$-module.

The second statement follows from (1).

□

Remark 5.3. Suppose H is a subgroup of G and A is an $\mathbb{Z}H$-module. Then $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)$ is a $\mathbb{Z}G$-module if endowed with the action :

$$\begin{array}{rcl} gf : \mathbb{Z}G & \to & A \\ x & \mapsto & gf(g^{-1}x), \end{array}$$

for any $g \in G$ and any $f : \mathbb{Z}G \to A$.

We consider in particular if $H = \{1\}$ (and then $\mathbb{Z}H = \mathbb{Z}$).

Next, we present the Eckman-Shapiro Lemma (known as Shapiro Lemma).

Theorem 5.2. *Let G be a group, H be a subgroup, and A be an $\mathbb{Z}H$-module. Then*

$$H^n(H, A) \cong H^n(G, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A))$$

for all $n \geq 0$.

In this proof, we use the notion of the tensor product, denoted by $\otimes$. For further information about it, see [**Rot09**, §2.2].

Proof. We denote by $U : \mathscr{M}_{\mathbb{Z}G} \to \mathscr{M}_{\mathbb{Z}H}$ the change of groups functor.
Suppose $\mathbf{P} = \ldots \to P_1 \to P_0 \to \mathbb{Z} \to 0$ is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}G$, then

$$H^n(G, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)) = H^n(\operatorname{Hom}_{\mathbb{Z}G}(\mathbf{P}, \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A))),$$

because it is the definition of the cohomology group. Using the adjunction between the tensor product and the functor Hom (precisely see [**Rot09**, Theorem 2.75, §2.2]), we have

$$\operatorname{Hom}_{\mathbb{Z}G}(P_i, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)) \cong \operatorname{Hom}_{\mathbb{Z}H}(P_i \bigotimes_{\mathbb{Z}G} \mathbb{Z}G, A).$$

Next, we use a property of the tensor product (see [**Rot09**, Proposition 2.58, §2.2]), hence $P_i \otimes_{\mathbb{Z}G} \cong P_i$, and we use the fact that $UP_i \cong P_i$. And so we obtain

$$\operatorname{Hom}_{\mathbb{Z}G}(P_i, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)) \cong \operatorname{Hom}_{\mathbb{Z}H}(UP_i, A),$$

for all i.
By lemma 5.1(2), $U\mathbf{P}$ is a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}H$, and hence

$$H^n(H, A) \cong H^n(\operatorname{Hom}_{\mathbb{Z}H}(U\mathbf{P}, A),$$

see theorem 3.4.
Moreover, there is an isomorphism of complex

$$\operatorname{Hom}_{\mathbb{Z}H}(U\mathbf{P}, A) \cong \operatorname{Hom}_{\mathbb{Z}G}(\mathbf{P}, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)). \tag{1}$$

In conclusion we have an isomorphism

$$H^n(H, A) \cong H^n(G, \operatorname{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)).$$

□

Definition 5.4. Suppose G is a group and A an abelian group. We define the *coinduced module* to be the $\mathbb{Z}G$-module $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$.

Remark 5.5. The above construction is the same as in remark 5.3 using $H = \{1\}$, and noticing that every abelian group can be viewed as a trivial $\mathbb{Z}$-module.

Proposition 5.3. *Every coinduced $\mathbb{Z}G$-module A is G-cyclic : $H^n(G, A) = \{0\}$, for all $n \geq 1$.*

Proof. Consider the subgroup $H = \{1\}$ and apply theorem 5.2, then

$$H^n(G, \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)) \cong H^n(H, A).$$

But this cohomology group is trivial (see [**Rot09**, Corollary 9.28, §9.2]). □

CHAPTER 5

Galois Cohomology

We define cohomology groups for profinite groups, note that we will use a slightly different definition as in previous chapter. We will finally state and prove different versions of Hilbert's Theorem 90.

1. Cohomology groups

Working with profinite groups implies we have to consider the topology. We therefore define discrete modules and particular cohomology groups.

1.1. Discrete G-modules.

Definition 1.1. Let $(G, \cdot)$ be a profinite group. A *discrete G-module* (or G-module, if there is no confusion) is an abelian group $(A, +)$ endowed with the discrete topology and on which G operates continuously. This means a G-module is an abelian group A with a continuous map $G \times A \to A : (g, a) \mapsto g \cdot a$ (where $G \times A$ is seen with the product topology) satisfying:

(1) $(g_1 g_2) \cdot (a) = g_1 \cdot (g_2 \cdot a)$;
(2) $g \cdot (a + b) = g \cdot a + g \cdot b$;
(3) $1_G \cdot a = a$;

for $a, b \in A$ and $g_1, g_2, g \in G$.

Remark 1.2. If G is a finite group, then all G-modules are discrete G-modules.

Proposition 1.1. *Let G be a profinite group and A an abelian group. Let $G \times A \to A$ be an action of G on A satisfying the conditions (1), (2) and (3) of definition 1.1. Then, the following are equivalent:*

(1) $G \times A \to A$ is continuous;
(2) For each $a \in A$, the stabilizer of a, $U_a = \{g \in G \mid g \cdot a = a\}$ is an open subgroup of G;
(3) $A = \bigcup_U A^U$ where U runs trough the set of all open subgroups of G, and where

$$A^U = \{a \in A \mid g \cdot a = a \ \forall \ g \in U\}.$$

Proof. We denote $f : G \times A \to A$ the action of G on A.

(1) ⇒ (2): Consider the restriction $f_a : G \times \{a\} \to A$ which is a continuous map because f is continuous. Then $U_a = f_a^{-1}(\{a\})$ is open as a preimage of an open set (recall that A is provided with the discrete topology).

(2) ⇒ (3): Clearly $\bigcup_U A^U \subseteq A$.
Let $a \in A$, then a is in A^{U_a}. And as U_a is an open subgroup of G, we obtain the result.

(3) ⇒ (1): We will show that $f^{-1}(\{a\})$ is a open subgroup of G for each $a \in A$. Hence if $a \in A$, a is in A^U for some open subgroup U of G. Which implies $g \cdot a = a$ for all $g \in U$. And so

$$1_G \times \{a\} \in U \times \{a\} \subseteq f^{-1}(\{a\}).$$

Consequently, $f^{-1}(\{a\})$ is open, because $G \times A$ is a topological group and $U \times \{a\}$ is open (see 4.4 in chapter 1).

□

Here are some examples of discrete G-modules.

Examples 1.3.

- For any profinite group G and any abelian group A we can define the action
$$G \times A \to A : (g, a) \mapsto a.$$
This action is called the *trivial action* on A. And A is a G-module, called a *trivial G-module.*
- Let $\mathbb{L}$ and $\mathbb{K}$ be fields such that $\mathbb{L}$ is a Galois extension of $\mathbb{K}$. Recall that $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ is a profinite group. Consider the abelian group $(\mathbb{L}, +)$ and the action
$$G \times \mathbb{L} \to \mathbb{L} : (\sigma, \alpha) \mapsto \sigma(\alpha).$$
Then $(\mathbb{L}, +)$ (sometimes denoted $\mathbb{L}^+$) is a discrete G-module.
Endowed with the same action $(\mathbb{L}^*, \cdot)$ and the group of all roots of unity in $\mathbb{L}$ (under multiplication) are also discrete G-modules.

Definition 1.4. Let G be a profinite group and A, B be two discrete G-modules. A *G-homomorphism* or a *G-map* $\varphi : A \to B$ is a group homomorphism for which
$$\varphi(g \cdot a) = g \cdot \varphi(a),$$
for all $g \in G$ and all $a \in A$.

Remark 1.5. The class of discrete G-modules and G-maps is an abelian category denoted by $\mathscr{M}_G$.

1.2. Definition of cohomology groups.

Let G be a profinite group. For each $n \in \mathbb{N}$ we denote by G^n the cartesian product of n copies of G.

Consider a discrete G-module A. We set
$$C_c^n(G, A) := \{f : G^n \to A \mid f \textit{ is continuous}\}.$$
Note that $C_c^n(G, A)$ is an abelian group under addition (because A is an abelian group). It is called the group of the *n-cochains.* Moreover $C_c^0(G, A)$ is isomorphic to A (as group of the maps from 0 to A).

For each $n \geq 1$ define a group homomorphism
$$d_{n+1} : C_c^n(G, A) \to C_c^{n+1}(G, A),$$
through
$$\begin{aligned}(d_{n+1}f)(g_1, \dots, g_{n+1}) &= g_1 \cdot f(g_2, \dots, g_{n+1}) \\ &+ \sum_{i=1}^{n}(-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \dots, g_n),\end{aligned}$$
for all $f \in C_c^n(G, A)$ and all $(g_1, \dots g_{n+1}) \in G^{n+1}$. For $n = 0$, we define the homomorphism
$$d_0 : C_c^0(G, A) \to C_c^1(G, A),$$
through
$$(d_0 a)(g) = g \cdot a - a,$$
for all $a \in A$ and all $g \in G$. The maps d_n are called the *coboundary operators.*

Lemma 1.2. *For each $n \geq 0$, d_n is a group homomorphism and moreover $d_{n+1} \circ d_n = 0$.*

Proof. One can find a proof in [**Bur04**, Chapter 2, §2.2]. □

Remark 1.6. This lemma implies that the maps d_n are the differentials of a cochain complex $\overline{C_c}(G, A) := (C_c^n(G, A), d_n)$.

Definition 1.7. Let G be a profinite group and A be a discrete G-module.

- We call the group of the *n-cocycles* of G, the group $Z_c^n := \ker(d_n)$, and we call the group of the *n-coboundaries* of G, the group $B_c^n(G, A) := \operatorname{im} d_{n-1}$.
  The lemma 1.2 implies that $B_c^n(G, A)$ is a subgroup of $Z_c^n(G, A)$.
- We define the *n-th cohomology group of G with coefficients in A* to be the group

$$H_c^n(G, A) := Z_c^n(G, A)/B_c^n(G, A).$$

Remark 1.8. We can built the cohomology in case A is simply a G-module and not expecting the cochains to be continuous. The construction is the same. In that case the cohomology group of G with coefficients in A is denote by $H_c^n(G, A)$. One can prove that this definition of the cohomology groups coincide with the one of chapter 4, i.e. there is no ambiguity with the notations. In case G is a discrete group, the continuity hypothesis is trivially verified. This means $H_c^n(G, A) = H^n(G, A)$. Then we can also use properties presented in chapter 4.

2. Interpretation of cohomology groups in low dimension

Let G be a profinite group and A a discrete G-module. We will study the cohomology groups $H_c^n(G, A)$ for small $n \in \mathbb{N}$.

2.1. Trivial case.

For $n = 0$, we have

$$H_c^0(G, A) \cong Z_c^0(G, A) = \{a \in A \mid d_0(a) = 0\} = \{a \in A \mid g \cdot a - a = 0 \ \forall\ g \in G\}.$$

And hence, $H_c^0(G, A)$ is isomorphic to A^G, the set of the invariant points of A under the action of G.

2.2. First cohomology group.

We consider now $n = 1$. As previously defined $H_c^1(G, A) = Z_c^1(G, A)/B_c^1(G, A)$.
The group of 1-cocycle can be explicitly described as

$$\begin{aligned} Z_c^1(G, A) &= \{f : G \to A \ \textit{continuous} \mid d_1(f) = 0\} \\ &= \{f : G \to A \ \textit{continuous} \mid f(g_1g_2) = g_1 \cdot f(g_2) + f(g_1), \ \forall\ g_1, g_2 \in G\}. \end{aligned}$$

And the group of 1-coboundaries is

$$\begin{aligned} B_c^1(G, A) &= \{f : G \to A \ \textit{continuous} \mid \exists a \in A \ \textit{s.t.}\ d_0(a) = f\} \\ &= \{f : G \to A \ \textit{continuous} \mid \exists a \in A \ \textit{s.t.}\ f(g) = g \cdot a - a, \ \forall\ g \in G\}. \end{aligned}$$

The elements of $Z_c^1(G, A)$ and $B_c^1(G, A)$ are called continuous crossed homomorphisms and principal crossed homomorphisms respectively.

Example 2.1. If G operates trivially on A, $H_c^1(G, A)$ is the group of all continuous group homomorphisms from G to A.

2.3. The second cohomology group.

For $n = 2$, $H_c^2(G, A) = Z_c^2(G, A)/B_c^2(G, A)$, with

$$\begin{aligned} Z_c^2(G, A) &= \{f : G \times G \to A \ \textit{continuous} \mid d_2(f) = 0\} \\ &= \{f : G \times G \to A \ \textit{continuous} \mid g_1 f(g_2, g_3) + f(g_1, g_2g_3) = f(g_1g_2, g_3) + f(g_1, g_2), \\ &\qquad \forall\ g_1, g_2, g_3 \in G\}, \end{aligned}$$

and

$$\begin{aligned} B_c^2(G, A) &= \{f : G \times G \to A \ \textit{continuous} \mid \exists \varphi \in C_c^1(G, A) \ \textit{s.t.}\ f = d_1(\varphi)\} \\ &= \{f : G \times G \to A \ \textit{continuous} \mid \exists \varphi \in C_c^1(G, A) \\ &\qquad \textit{s.t.}\ f(g_1, g_2) = g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1), \ \forall\ g_1, g_2 \in G\}. \end{aligned}$$

The elements of $Z_c^2(G, A)$ are called continuous factor systems.

3. Functorially properties of the cohomology groups

3.1. Compatible maps.

3.1.1. *Definition.*

Definition 3.1. Let G and G' be two profinite groups. Let $A \in \mathscr{M}_G$ and $A' \in \mathscr{M}_{G'}$. Consider $\varphi : G \to G'$ a continuous homomorphism of profinite groups and $\psi : A' \to A$ a group homomorphism. We say that ψ and φ are *compatible maps* if

$$\psi(\varphi(g) \cdot a') = g \cdot f(a'),$$

for all $g \in G$ and all $a' \in A'$.
This is equivalent as asking that ψ is a G-map when A' is considered as a G-module with the action

$$g \cdot a' = \varphi(g) \cdot a',$$

for each $a' \in A'$ and $g \in G$.

Example 3.2. Let $\mathbb{L}$ and $\mathbb{E}$ be Galois extensions of $\mathbb{K}$, with $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$. We consider the restriction

$$\pi : \mathrm{Gal}(\mathbb{L}, \mathbb{K}) \to \mathrm{Gal}(\mathbb{E}, \mathbb{K}),$$

and the injection

$$i : \mathbb{E}^* \hookrightarrow \mathbb{L}^*.$$

Then those mappings are compatible.

Lemma 3.1. *Let φ and ψ be compatible maps as in definition 3.1. They induce a homomorphism on the groups of n-cochains (for $n \geq 0$)*

$$(\varphi, \psi) : C_c^n(G', A') \to C_c^n(G, A)$$

defined by

$$[(\varphi, \psi)(f)](g_1, \dots, g_n) = \psi[f(\varphi(g_1), \dots, \varphi(g_n))].$$

In particular, (φ, ψ) is a map of cochain complexes, i.e. the diagram

$$\begin{tikzcd}
{} \arrow[r, "d_n"] & C_c^n(G', A') \arrow[r, "d_{n+1}"] \arrow[d, "(\varphi,\psi)"] & C_c^{n+1}(G', A') \arrow[r] \arrow[d, "(\varphi,\psi)"] & {} \\
{} \arrow[r, "d_n"] & C_c^n(G, A) \arrow[r, "d_{n+1}"] & C_c^{n+1}(G, A) \arrow[r] & {}
\end{tikzcd}$$

commutes for $n \geq 0$.

Proof. One can easily check this lemma with a straightforward computation. □

Corollary 3.2. *If φ, ψ are compatible maps as in definition 3.1, (φ, ψ) induces a homomorphism of the cohomology groups, written*

$$(\varphi, \psi) : H_c^n(G', A') \to H_c^n(G, A).$$

Proof. Use the commutativity of the above diagram. □

3.1.2. *Functorially properties of compatible maps.*
Let G_i, $i = 1, 2, 3$, be profinite groups and $A_i \in \mathscr{M}_{G_i}$. Consider the continuous group homomorphisms

$$\begin{tikzcd}
G_1 \arrow[r, "\varphi_1"] & G_2 \arrow[r, "\varphi_2"] & G_3
\end{tikzcd}$$

and the group homomorphisms

$$\begin{tikzcd}
A_1 & A_2 \arrow[l, "\psi_1"'] & A_3. \arrow[l, "\psi_2"']
\end{tikzcd}$$

with φ_1, ψ_1 being compatible maps and φ_2, ψ_2 too. They induce two group homomorphisms

$$\begin{aligned}(\varphi_1, \psi_1) : H_c^n(G_2, A_2) &\rightarrow H_c^n(G_1, A_1)\\ (\varphi_2, \psi_2) : H_c^n(G_3, A_3) &\rightarrow H_c^n(G_2, A_2).\end{aligned}$$

Then we have that $\varphi_1 \circ \varphi_2$ is compatible with $\psi_2 \circ \psi_1$ and

$$(\varphi_1, \psi_1) \circ (\varphi_2, \psi_2) = (\varphi_2 \circ \varphi_1, \psi_1 \circ \psi_2).$$

Moreover, if φ is the identity map of G and ψ the identity map of A, then (φ, ψ) is the identity map of $H_c^n(G, A)$.
Consequently, for each profinite group G and for each $n \geq 0$, $H_c^n(G, -)$ is a covariant functor from $\mathscr{M}_G$ to $\mathscr{A}$.

3.2. Direct limit. We define the direct limit in order to consider a direct limit of G-modules. This will be useful to describe limits of cohomology groups.

Definition 3.3. Let I be a directed set. And let $\mathscr{C}$ be a category. A *direct system* $(X_i, f_{ij})_I$ of objects of $\mathscr{C}$ indexed by I consists of a family $\{X_i \mid i \in I\}$ of objects and of a family $\{f_{ij} : X_i \to X_j \mid i, j \in I, i \leq j\}$ of morphisms of $\mathscr{C}$ such that

(1) f_{ii} is the identity over X_i for all $i \in I$,
(2) $f_{jk} \circ f_{ij} = f_{ik}$ for all $i \leq j \leq k \in I$.

Definition 3.4. If Y is an object of $\mathscr{C}$, we call a family of morphisms of $\mathscr{C}$ $\{\psi_i : X_i \to Y\}_{i \in I}$ *compatible*, if $\psi_j \circ f_{ij} = \psi_i$ for every $i \leq j \in I$, i.e. if the following diagram commutes:

$$\begin{tikzcd} & Y & \\ X_i \arrow[ur, "\psi_i"'] \arrow[rr, "f_{ij}"'] & & X_j. \arrow[ul, "\psi_j"] \end{tikzcd}$$

Definition 3.5. An *colimit* (X, φ_i) of a direct system $(X_i, f_{ij})_I$ of objects of $\mathscr{C}$ is an object X provided with a compatible family $\{\varphi_i : X_i \to X\}_{i \in I}$ satisfying the following universal property: For every object Y and for every compatible family $\{\psi_i : X_i \to Y\}_{i \in I}$, there exists a unique morphism of $\mathscr{C}$ $\theta : Y \to X$ such that the following diagram commutes for all $i \leq j \in I$.

$$\begin{tikzcd} & Y & \\ & X \arrow[u, dotted, "\exists!"', "\theta"] & \\ X_i \arrow[uur, "\psi_i"] \arrow[ur, "\varphi_i"'] \arrow[rr, "f_{ij}"'] & & X_j. \arrow[uul, "\psi_j"'] \arrow[ul, "\varphi_j"] \end{tikzcd}$$

Proposition 3.3. *The direct limit is unique up to isomorphism.*

PROOF. Similar as the proof of proposition 1.1 in chapter 3. □

Notation 3.6. As there is no ambiguity anymore, we will denote by $\varinjlim_I X_i$ the direct limit of $(X_i, f_{ij})_I$.

We have seen in chapter 3, that there is a special characterization of a limit (or inverse limit) in case we were in the category of topological spaces. We will now give such a characterization of the direct limit in the category of groups (and group homomorphisms).

Proposition 3.4. *Let $(X_i, f_{ij})_I$ be a direct system of groups. Consider the set $Z = \coprod_I X_i$ (the disjoint union of the X_i) and define an equivalence relation $\sim$, with $(x_i, i) \sim (x_j, j)$ if and only if $i, j \in I$ with $x_i \in X_i$, $x_j \in X_j$ and there is a $k \in I$ with $i, j \leq k$ and $f_{ik}(x_i) = f_{jk}(x_j)$. Then $\varinjlim_I X_i \cong Z/\sim$.*

Proof. It is trivial to see that $\sim$ is an equivalence relation.
We define the morphisms

$$\varphi_i : X_i \to Z/\sim,$$

induced by the inclusion $i : X_i \to Z : x_i \mapsto (x_i, i)$. By construction $\{\varphi_i : X_i \to Z/\sim\}$ is a compatible system.
Consider an other group Y and a compatible family $\{\psi_i : X_i \to Y\}_{i \in I}$. We define

$$\theta : Z \to Y : (x_i, i) \to \psi_i(x_i).$$

Let $(x_i, i), (x_j, j)$ be in Z with $(x_i, i) \sim (x_j, j)$. We want to show that $\theta((x_i, i)) = \theta((x_j, j))$. But $(x_i, i) \sim (x_j, j)$ implies there is a $k \in I$ with $i, j \leq k$ and $f_{ik}(x_i) = f_{jk}(x_j)$. Then

$$\begin{aligned} \theta((x_i, i)) &= \psi_i(x_i) \\ &= \psi_k(f_{ik}(x_i)) \\ &= \psi_k(f_{jk}(x_j)) \\ &= \psi_j(x_j) = \theta((x_j, j)). \end{aligned}$$

Hence, we can define $\widetilde{\theta} : Z/\sim \to Y$. Moreover we have trivially that $\widetilde{\theta} \circ \varphi_i = \psi_i$ for each $i \in I$, and also that $\widetilde{\theta}$ is unique. And so $Z/\sim$ is a direct limit of $(X_i, f_{ij})_I$. □

3.3. Properties of the cohomology group of a limit.

We consider now a directed index set $(I, \leq)$ and two systems; a inverse system of profinite groups $(G_i, \varphi_{ij})_I$ and a direct system of abelian groups (A_i, λ_{ij}) (for definition see section 3.2), such that $A_i \in \mathscr{M}_{G_i}$ for each $i \in I$ and such that φ_{ij} and λ_{ij} are compatible maps for $i \leq j$.
This induces a direct system $(H^n_c(G_i, A_i), (\varphi_{ij}, \lambda_{ij}))_I$.
We denote $G := \varprojlim_I G_i$ and $A := \varinjlim_I G_i$, and the canonical morphisms

$$\begin{aligned} \pi_i : G &\to G_i \\ \lambda_i : A_i &\to A. \end{aligned}$$

Lemma 3.5. *A can be viewed as a G-module with the following action:
For $a \in A$ and $g \in G$, choose $i \in I$ and $a_i \in A_i$ such that $\lambda_i(a_i) = a$. Then define*

$$g \cdot a = \lambda_i((\pi_i(g)) \cdot a_i).$$

This action is well-defined and continuous.

Proof. We will first show that the action is independent of the choice of $i \in I$. recall that

$$A \cong \coprod_I A_i/\sim,$$

with $\alpha_i \sim \alpha_j \Leftrightarrow \alpha_i \in A_i$, $\alpha_j \in A_j$ and there is a $k \in I$ with $i, j \leq k$ and $\lambda_{ik}(\alpha_i) = \lambda_{jk}(\alpha_j)$.
Therefore let i, j be in I and a_i, a_j be in A_i, A_j respectively, such that $\lambda_j(a_j) = a$ and $\lambda_i(a_i) = a$. As I is a directed set, there is a $k \in I$ with $i, j \leq k$. Then, using the property of the inverse limit and the compatibility of π_{ik} and λ_{ik},

$$\begin{aligned} \lambda_{ik}[(\pi_i(g)) \cdot a_i] &= \lambda_{ik}[(\pi_{ik}(\pi_k(g))) \cdot a_i] \\ &= \pi_k(g) \cdot \lambda_{ik}(a_i). \end{aligned}$$

In the same way $\lambda_{jk}[(\pi_j(g)) \cdot a_j] = \pi_k(g) \cdot \lambda_{jk}(a_j)$. But one as (because of the definition of an direct limit)

$$\lambda_k(\lambda_{ik}(a_i)) = \lambda_i(a_i) = a = \lambda_j(a_j) = \lambda_k(\lambda_{jk}(a_j)).$$

As λ_k is injective, $\lambda_{ik}(a_i) = \lambda_{jk}(a_j)$. Which implies

$$\lambda_{ik}[(\pi_i(g)) \cdot a_i] = \lambda_{jk}[(\pi_j(g)) \cdot a_j].$$

And hence

$$\lambda_i[(\pi_i(g)) \cdot a_i] = \lambda_j[(\pi_j(g)) \cdot a_j].$$

Now it is easy to see that the action is continuous as composition of continuous maps. □

Theorem 3.6. *If the G_i and the A_i are as above, for each $n \geq 0$,*

$$H_c^n(G, A) \cong \varinjlim_I H_c^n(G_i, A_i).$$

Proof. One can prove that $\varinjlim$ is an exact functor in the category of abelian groups $\mathscr{A}$ (as in proposition 2.12 - chapter 3). This implies

$$\varinjlim_I H_c^n(G_i, A_i) \cong H_c^n(\varinjlim_I \overline{C}(G_i, A_i))$$

where the cochain complexes $\overline{C}(G_i, A_i)$ form a direct system with the induced maps

$$\overline{\lambda}_{ij} = (\pi_{ij}, \lambda_{ij}) : \overline{C}(G_i, A_i) \to \overline{C}(G_j, A_j)$$

for each $i \leq j$ (see part 3.1). Then, to prove the proposition, we only have to find an isomorphism from $\varinjlim_I C_c^n(G_i, A_i)$ to $C_c^n(G, A)$ commuting with the d_n.
Define

$$\begin{array}{rcl} \varphi_i : C_c^n(G_i, A_i) & \to & C_c^n(G, A) \\ f & \mapsto & \varphi_i(f) := \lambda_i \circ f \circ \pi_i. \end{array}$$

Notice that $\varphi_j \circ \overline{\lambda}_{ij} = \varphi_i$ for each $i, j \in I$ with $i \leq j$, in fact

$$\begin{array}{rcl} \varphi_j \circ \overline{\lambda}_{ij}(f) & = & \varphi_j(\lambda_{ij} \circ f \circ \pi_{ij}) \\ & = & \lambda_j \circ \lambda_{ij} \circ f \circ \pi_{ij} \circ \pi_j \\ & = & \lambda_i \circ f \circ \pi_i \\ & = & \varphi_i(f), \end{array}$$

for each $f \in C_c^n(G_i, A_i)$. Then φ_i induces a morphism

$$\varphi : \varinjlim_I C_c^n(G_i, A_i) \to C_c^n(G, A),$$

because $\{\varphi_i : C_c^n(G_i, A_i) \to C_c^n(G, A)\}_I$ is a compatible family (see definition of the direct limit in section 3.2).
It is easy to see that φ commutes with the coboundary operators d_k, $k \geq 0$.

φ **is injective:** Let f be in $\varinjlim_I C_c^n(G_i, A_i)$ such that $\varphi(f) = 0$. Consider a $i_0 \in I$ and a $f_{i_0} \in C_c^n(G_i, A_i)$ such that $\overline{\lambda}_{i_0}(f_{i_0}) = f$. Now denote

$$f_j := \overline{\lambda}_{i_0 j}(f_{i_0}), \tag{2}$$

for all $j \leq i_0$, this implies in particular

$$\overline{\lambda}_j(f_j) = f, \tag{3}$$

and one can deduce $0 = \varphi(f) = \lambda_j \circ f_j \circ \pi_j$, for all $j \leq i_0$. We define

$$X_j := \{g_j = (g_{j_1}, \ldots, g_{j_n}) \in G_j^n \mid f_j(g_j) \neq 0\}.$$

Yet, we only need to show that $X_j = \emptyset$ for some $j \geq i_0$ ($\Rightarrow f_j = 0$) and this will imply $f = 0$ (because of 2 and 3 - see section 3.2).
Clearly one has

$$G_j^n \subseteq \bigcup_{a \in A_j} f_j^{-1}(\{a\}),$$

but as f_j is a continuous map, A_j a discrete G-module and G_j^n a compact group (as product of compact), f_j takes only a finite number of values. Then X_j is closed (as a finite union of closed space) and hence compact (as subgroup of G_j^n).
Consider $i_0 \leq i \leq j$ and let $g_j \in X_j$, then

$$\begin{aligned} 0 &\neq f_j(g_j) \\ &= (\overline{\lambda}_{ij}(f_i))(g_j) \\ &= \lambda_{ij} \circ f_i \circ \pi_{ij}(g_j), \end{aligned}$$

and we have $f_i \circ \pi_{ij}(g_j) \neq 0$. Which means $\pi_{ij}(g_j) \in X_i$. Consequently $\pi_{ij}(X_j) \subseteq X_i$ for each $i_0 \leq i \leq j$, furthermore, $\{X_i, \pi_{ij}\}_{i \leq i_0}$ is an inverse system of compact spaces. Clearly for $g = (g_1 \ldots, g_n) \in \varprojlim_{i \leq i_0} X_i \subseteq G^n$, one has $\varphi(f)(g) \neq 0$. So $\varprojlim_{i \leq i_0} X_i = \emptyset$. Now using [**Bou71**, Proposition 8, §9, Chapter 1], we obtain $X_i = \emptyset$ for some $i \geq i_0$.

φ **is surjective:** Let $f \in C_c^n(G, A)$. We have to find a continuous map $f_i : G_i^n$ such that $f = \varphi_i(f_i) = \lambda_i \circ f_i \circ \pi_i$ for a $i \in I$. As previously, f being continuous, A being discrete and G^n being compact implies that f takes only a finite number of values. Suppose $f(G^n) = \{a_1, \ldots, a_q\} \subseteq A$. Hence there is a $i_0 \in I$ such that $\lambda_{i_0} A_{i_0} \supseteq f(G^n)$.
Consider U_1 a normal subgroup of G such that f is constant on the cosets of U_1^n in G^n. Since $\{\pi_l^{-1}(U_l) \mid U_l \textit{ normal subgroup of } G\}$ is a basis of open neighborhood of 1 in G (see proposition and corollary 2.6 in chapter 3), there is a normal subgroup U_i of G_i such that $U_1 \supseteq U := \pi_i^{-1}(U_i)$ for some $i \geq i_0$. Note that $i \geq i_0$ implies

$$f(G^n) \subseteq \lambda_{i_0}(A_{i_0}) = \lambda_i \circ \lambda_{i_0 i}(A_{i_0}) \subseteq \lambda_i(A_i). \tag{4}$$

Then

$$f = \overline{f} \circ p,$$

where $p : G^n \to G^n/U^n$ is the natural projection, and $\overline{f} : G^n/U^n \to A$ is defined by $f(gU^n) = f(g)$ (well-defined thanks to the construction of U). Note that

$$\operatorname{im}(\overline{f}) \subseteq \operatorname{im}(f). \tag{5}$$

Conversely π_i induces an injective map $\pi_i' : G^n/U^n \to G_i^n/U_i^n$, (the injectivity comes from $\pi_i(U^n) \subseteq U_i^n$). Precisely for each $\tilde{g} \in G^n$, $\pi_i'(\tilde{g}U^n) = p_i \circ \pi_i(\tilde{g})$, and this implies $\pi_i' \circ p = p_i \circ \pi_i$.
Let $\overline{f}_i : G_i^n/U_i^n \to A_i$ be any map such that $\lambda_i \circ \overline{f}_i \circ \pi_i' = \overline{f}$, i.e. such that the following diagram commutes

$$\begin{tikzcd} G^n/U^n \arrow[r, "\overline{f}"] \arrow[d, "\pi_i'"'] & A \\ G_i^n/U_i^n \arrow[r, dotted, "\overline{f}_i"'] & A_i. \arrow[u, "\lambda_i"'] \end{tikzcd}$$

Such a map always exists because of 4, 5 and the definition of the inverse limit. Moreover $\overline{f}_i$ is continuous because A is discrete, $\overline{f}$ is continuous and π_i' is an open map.
Now define $f_i = \overline{f}_i \circ p_i$, where $p_i : G_i^n \to G_i^n/U_i^n$ is the natural projection. f_i is clearly continuous as composition of continuous maps and moreover

$$\begin{aligned} \lambda_i \circ f_i \circ \pi_i &= \lambda_i \circ \overline{f}_i \circ p_i \circ \pi_i \\ &= \lambda_i \circ \overline{f}_i \circ \pi_i' \circ p \\ &= \overline{f} \circ p = f. \end{aligned}$$

□

Example 3.7. Consider $\mathbb{L}$ a Galois extension of $\mathbb{K}$. And recall that $\mathcal{F}$ is the set of all intermediate fields $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$, with $\mathbb{E}$ being a finite Galois extension of $\mathbb{K}$. Recall that

$$\mathrm{Gal}(\mathbb{L}, \mathbb{K}) = \varprojlim_{\mathcal{F}} \mathrm{Gal}(\mathbb{E}, \mathbb{K}).$$

We define a direct system $(\mathbb{E}, f)_{\mathcal{F}}$, by endowing $\mathcal{F}$ with the partial order of inclusion and considering the trivial inclusions

$$f_{ij} : \mathbb{E}_i^+ \hookrightarrow \mathbb{E}_j^+$$

for $\mathbb{E}_i^+ \subseteq \mathbb{E}_j^+$. Then we have to show that $\mathbb{L}^+ \cong \varinjlim_{\mathcal{F}} \mathbb{E}^+ \cong \coprod_{\mathbb{E}\in\mathcal{F}} \mathbb{E}^+/\sim$ (see section 3.2). We define

$$\begin{array}{rcl} \varphi : \coprod\limits_{\mathbb{E}\in\mathcal{F}} \mathbb{E}^+ & \to & \mathbb{L}^+ \\ \overline{(\alpha, \mathbb{E})} & \mapsto & \alpha, \end{array}$$

where $\overline{(\alpha, \mathbb{E})}$ denote the equivalence class of $(\alpha, \mathbb{E})$ for the relation $\sim$. It is trivial to check that this map is well-define, injective and surjective (use $\mathbb{L} = \cup_{\mathcal{F}}\mathbb{E}$).
Then, using the preceding theorem (3.6), we have

$$H_c^n(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^+) \cong \varinjlim_{\mathcal{F}} H_c^n(\mathrm{Gal}(\mathbb{E}, \mathbb{K}), \mathbb{E}^+).$$

One can prove the same statement for the multiplicative group $\mathbb{L}^*$ instead of $\mathbb{L}^+$.

4. Hilbert's Theorem 90

Hilbert's Theorem 90 was originally a theorem about cyclic extensions of number fields, but there are many generalization of it. The theorem has its name because it is the 90th theorem of a famous book of David Hilbert: "Zahlbericht", published in 1897, although the theorem is sometimes attribute to Kummer. It was later generalized by Andreas Speiser in 1919. However the result is also know to be from Emmy Noether. We will discuss the different versions of this theorem. Our reference will be [**Lor98**].
In this section we write $H^n(G, A)$ instead of $H_c^n(G, A)$ to simplify the notations.

4.1. Original Hilbert's Theorem 90.

To present Hilbert's Theorem, we have to define the norm of a field extension. This is discussed in detail in [**Lan02a**, §5, Chapter VI].

Definition 4.1. Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$. Suppose $[\mathbb{L} : \mathbb{K}]_s = r$, and that $[\mathbb{L} : \mathbb{K}]_i = p^\mu$ if the characteristic is a prime number $p > 0$, and 1 otherwise.
Let $\sigma_1, \dots \sigma_r$ be the distinct embeddings of $\mathbb{L}$ in an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$.
If α is an element of $\mathbb{L}$, we define its *norm* from $\mathbb{E}$ to $\mathbb{K}$ to be

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = N_{\mathbb{K}}^{\mathbb{L}}(\alpha) = \prod_{n=1}^{r} \sigma_n(\alpha^{p^\mu}) = (\prod_{n=1}^{r} \sigma_n(\alpha))^{[\mathbb{L}:\mathbb{K}]_i}.$$

We present some properties without proving them.

Proposition 4.1. *If $\mathbb{L}$ is separable over $\mathbb{K}$, we have*

$$N_{\mathbb{K}}^{\mathbb{L}}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

where the product is taken over the distinct embeddings of $\mathbb{L}$ in $\overline{\mathbb{K}}$ over $\mathbb{K}$.

Proposition 4.2. *Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$. Then the norm is a multiplicative homomorphism of $\mathbb{L}^*$ into $\mathbb{K}^*$.*

Theorem 4.3. *Let $\mathbb{L}$ be a cyclic Galois extension of $\mathbb{K}$, with Galois group $G = \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ and with $[\mathbb{L} : \mathbb{K}] = n$. Suppose σ is a generator of G, i.e. $G =< \sigma >$. Let $\beta \in \mathbb{L}$. The norm $N_{\mathbb{K}}^{\mathbb{L}}(\beta) = N(\beta)$ is equal to 1, if and only if, there is a $\alpha \in \mathbb{L}^*$ such that*

$$\beta = \frac{\alpha}{\sigma(\alpha)}.$$

Proof. Suppose first that such such an α exists. Then $N(\beta) = \frac{N(\alpha)}{N(\sigma(\alpha))}$. But as $N(.)$ is a product over all automorphisms in G, applying σ simply permutes those. Hence $N(\sigma(\alpha)) = N(\alpha)$, i.e. $N(\beta) = 1$.
Next suppose $N(\beta) = 1$. We consider the map

$$id + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \ldots + \beta\sigma(\beta)\ldots\sigma^{n-2}(\beta)\sigma^{n-1}.$$

Each terms are distinct and so we can apply Artin's theorem (see [**Lan02a**, Theorem 4.1, §4, Chapter VI]). Hence the above map is not identical null on $\mathbb{L}$, i.e. there is a $\theta \in \mathbb{L}$ and a $\alpha \in \mathbb{L}^*$ such that

$$\alpha = \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta)\ldots\sigma^{n-2}(\beta)\sigma^{n-1}(\theta).$$

Then

$$\beta\sigma(\alpha) = \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)\sigma^{n}(\theta),$$

but as $1 = N(\beta) = \beta\sigma(\beta)\ldots\sigma^{n-1}(\beta)$, and $\sigma^n(\theta) = \theta$, we have

$$\beta\sigma(\alpha) = \alpha.$$

And this concludes the proof. □

This is the "Theorem 90" of Hilbert. However Hilbert had some restrictions: The field $\mathbb{K}$ was supposed to be a number field and the degree of the extension was a prime number.

4.2. Other formulation.

Let us consider $\mathbb{L}$ a Galois extension of a field $\mathbb{K}$ and its Galois group G. We use the notation $\alpha^\sigma = \sigma(\alpha)$ for $\alpha \in \mathbb{L}$ and $\sigma \in G$, and also the power notation, i.e. $\alpha^{\tau+\sigma} = \tau(\alpha) \circ \sigma(\alpha)$ for $\alpha \in \mathbb{L}$ and $\tau, \sigma \in G$.
Let A be the G-module $\mathbb{L}^*$. We denote by A^{1-G} the subgroup of A generated by the element of the form $\alpha^{1-\sigma}$ (or $\alpha/\sigma(\alpha)$) for $\alpha \in A$ and $\sigma \in G$. And we write ${}_NA$ the kernel of the norm map $N : \mathbb{L}^* \to \mathbb{L}^*$. We have then

$$A^{1-G} \subseteq {}_NA,$$

because $N(\alpha^\sigma) = N(\alpha)$ (see the definition of the norm). Next we can define the quotient

$$H^{-1}(G, A) = {}_NA/A^{1-G}.$$

For any $\sigma, \tau \in A$ and each $\alpha \in A$, we have

$$a^{1-\sigma\tau} = a^{1-\sigma+\sigma-\sigma\tau} = a^{1-\sigma}(a^\sigma)^{1-\tau} \in A^{1-\sigma}A^{1-\tau}.$$

And hence, in case G is a cyclic group with generator σ, we have

$$A^{1-G} = A^{1-\sigma}.$$

And so the Hilbert's Theorem 90 can be formulated as

Theorem 4.4. *Let $\mathbb{L}$ be a cyclic finite extension of $\mathbb{K}$, with Galois group G.
Then $H^{-1}(G, \mathbb{K}^*) = 1$.*

We will now look for a similitude between this formulation and the cohomology groups presented earlier. Recall that the group of 1-cycles $Z^1(G, \mathbb{K}^*)$ can be explicitly described as the set of the maps $f : G \to \mathbb{K}^*$ satisfying

$$f(\tau\sigma) = \tau(f(\sigma))f(\tau) = f(\sigma)^\tau f(\tau).$$

If we suppose that G is cyclic with generator σ, f can be defined by the image of σ. In fact, write $\xi = f(\sigma)$, then

$$f(\sigma^i) = f(\sigma)^{\sigma^{i-1}} f(\sigma^{i-1}) = \xi^{1+\sigma+\sigma^2+\ldots\sigma^{i-1}}, \tag{6}$$

for each $i \in \mathbb{N}$. In addition, $N(\xi) = \xi^{1+\sigma+\ldots\sigma^{n-1}} = f(\sigma^n) = 1$. Notice that the morphisms $f : G \to A$ with $f(\sigma) = \alpha^{1-\sigma}$ are precisely the elements of $B^1(G, A)$. And so, if we consider the map

$$\varphi : H^1(G, A) \to H^{-1}(G, A) : f \mapsto \xi = f(\sigma),$$

we get an injective group homomorphism (first theorem of isomorphism for groups).
Now suppose $\xi \in A$ with $N(\xi) = 1$, we construct an map $f : G \to A$ using the equation 6. Then this map is well-defined and belongs to $Z^1(G, A)$. This means we have the isomorphism

$$H^1(G, A) \cong H^{-1}(G, A),$$

in case G is cyclic.
Hence the above theorem is equivalent to

Theorem 4.5. *Let $\mathbb{L}$ be a cyclic finite extension of $\mathbb{K}$, with Galois group G.
Then $H^1(G, \mathbb{K}^*) = 1$.*

4.3. Generalizations of Hilbert's theorem 90.

We present here one of the most general versions of the Hilbert's Theorem 90. However, there are some other versions of this theorem, one can find one of them in [**Sch02**]. We do not present this version in this project because we need a lot of new notions.

Theorem 4.6. *Let $\mathbb{L}$ be a Galois extension of a field $\mathbb{K}$, then $H^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*) = 0$.*

Proof. Using theorem 3.6, it is enough to prove the theorem in case that $\mathbb{L}$ is a finite extension of $\mathbb{K}$. In this case $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ is a discrete group, hence there is no ambiguity about the cohomology groups.
Recall that $H^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*) = Z^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*)/B^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*)$, and this implies we only have to show

$$Z^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*) \subseteq B^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*).$$

Note that for each $f \in B^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*)$ there is $\alpha \in \mathbb{L}^*$ such that $f = d_0(\alpha)$. And so f is a morphism between $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ and $\mathbb{L}^*$ such that

$$f(\sigma) = \sigma(\alpha)\alpha^{-1}$$

for each $\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ (notice that is equivalent to the expression in section 2.2 but with the multiplicative notation).
Let g be in $Z^1(\mathrm{Gal}(\mathbb{L}, \mathbb{K}), \mathbb{L}^*)$. This means $d_1(g) = 0$, then for each $\sigma, \tau \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$

$$1_{\mathbb{L}} = d_1(g)(\sigma, \tau) = \sigma g(\tau) \cdot g(\sigma\tau)^{-1} \cdot g(\sigma),$$

and hence

$$g(\sigma\tau) = \sigma g(\tau) \cdot g(\sigma). \tag{7}$$

For $\alpha \in \mathbb{L}^*$ define

$$A(\alpha) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})} g(\sigma)\sigma(\alpha).$$

As all he automorphisms of $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ are distinct, they are independent (result of the Galois theory). And so there is a $\alpha \in \mathbb{L}^*$ such that $A(\alpha) \neq 0$, denote $A(\alpha) = \beta$.
For each $\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ we have

$$\sigma(\beta) = \sum_{\tau \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})} \sigma(g(\tau))\sigma\tau(\alpha)$$

and multiplying by $g(\sigma) \in \mathbb{L}^*$:

$$\begin{aligned} g(\sigma) \cdot \sigma(\beta) &= \sum_{\tau \in \mathrm{Gal}(\mathbb{L},\mathbb{K})} g(\sigma)\sigma(g(\tau))\sigma\tau(\alpha) \\ &\overset{7}{=} \sum_{\tau \in \mathrm{Gal}(\mathbb{L},\mathbb{K})} g(\sigma\tau)\sigma\tau(\alpha) \end{aligned}$$

Now this last sum is equal to β because $\sigma\tau$ runs through $\mathrm{Gal}(\mathbb{L},\mathbb{K})$. Rewriting the above equation, we have

$$g(\sigma) = \sigma(\beta^{-1})(\beta^{-1})^{-1}$$

for each $\sigma \in \mathrm{Gal}(\mathbb{L},\mathbb{K})$. And hence $g \in B^1(\mathrm{Gal}(\mathbb{L},\mathbb{K}),\mathbb{L}^*)$. □

Next, a theorem linked to the above one.

Theorem 4.7. *Let $\mathbb{L}$ be a Galois extension of a field $\mathbb{K}$, then $H^n(\mathrm{Gal}(\mathbb{L},\mathbb{K}),\mathbb{L}^+) = 0$ for each $n \geq 1$.*

Proof. Using theorem 3.6, it is enough to prove the theorem in case $\mathbb{L}$ is a finite extension of $\mathbb{K}$. Next, we recall the normal basis theorem (see [**Lan02a**, Theorem 13.1, §13, Chapter VI]), i.e. there is a $\theta \in \mathbb{L}$ such that

$$\{\sigma(\theta) \mid \sigma \in \mathrm{Gal}(\mathbb{L},\mathbb{K})\}$$

is a basis of the $\mathbb{L}^+$ as a $\mathbb{K}$ vector space. This is equivalent to

$$\mathbb{L}^+ = \bigoplus_{\sigma \in G} \mathbb{K}^+\sigma(\theta).$$

But this direct sum is isomorphic to $K[G] \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G,\mathbb{K}^+)$, i.e. $\mathbb{L}^+$ is an induced $\mathbb{Z}G$-module. Thus $H^n(G,\mathbb{L}^+) = \{0\}$, for all $n \geq 0$, by proposition 5.3 in chapter 4. □

Bibliography

[Bou71] N. Bourbaki, *Éléments de mathématique. Topologie générale. Chapitres 1 à 4*, Hermann, Paris, 1971. MR MR0358652 (50 #11111)

[Bur04] Dietrich Burde, *Cohomology of groups with applications to number theory*, 2004, Available at http://homepage.univie.ac.at/Dietrich.Burde/.

[Hus66] Taqdir Husain, *Introduction to topological groups*, W. B. Saunders Co., Philadelphia, Pa., 1966. MR MR0200383 (34 #278)

[Lan02a] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR MR1878556 (2003e:00003)

[Lan02b] ———, *Introduction to differentiable manifolds*, second ed., Universitext, Springer-Verlag, New York, 2002. MR MR1931083 (2003h:58002)

[Lor98] F. Lorenz, *Ein Scholion zum Satz 90 von Hilbert*, Abh. Math. Sem. Univ. Hamburg **68** (1998), 347–362. MR MR1658433 (99i:12004)

[Mil08] James S. Milne, *Fields and galois theory (v4.21)*, 2008, Available at www.jmilne.org/math/, pp. 107+iv.

[Mun75] James R. Munkres, *Topology: a first course*, Prentice-Hall Inc., Englewood Cliffs, N.J., 1975. MR MR0464128 (57 #4063)

[Pon66] L. S. Pontryagin, *Topological groups*, Translated from the second Russian edition by Arlen Brown, Gordon and Breach Science Publishers, Inc., New York, 1966. MR MR0201557 (34 #1439)

[Rib99] Luis Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Applied Mathematics, vol. 24, Queen's University, Kingston, ON, 1999, Reprint of the 1970 original, with errata. MR MR1705274 (2000c:20047)

[Rot09] Joseph J. Rotman, *An introduction to homological algebra*, second ed., Universitext, Springer, New York, 2009. MR MR2455920 (2009i:18011)

[Sch02] Stefan Schröer, *Hilbert's Theorem 90 and algebraic spaces*, J. Pure Appl. Algebra **173** (2002), no. 3, 339–345. MR MR1916484 (2003d:14003)

[Wil98] John S. Wilson, *Profinite groups*, London Mathematical Society Monographs. New Series, vol. 19, The Clarendon Press Oxford University Press, New York, 1998. MR MR1691054 (2000j:20048)